

CRANFIELD UNIVERSITY

ABDULMOHSAN ALOSEEL

CYBERSECURITY OF EMBEDDED SYSTEMS
A NOVEL APPROACH FOR DETECTING CYBERATTACKS
BASED ON ANOMALOUS PATTERNS OF RESOURCE
UTILISATION

School of Aerospace, Transport and Manufacturing
SATM
PhD in Aerospace - Cybersecurity of Embedded Systems

This thesis is submitted in partial fulfilment of the requirements for the
degree of Doctor of Philosophy
Academic Year: 2019 - 2022

Supervisor: Dr. Saba Al-Rubaye
Associate Supervisor: Dr. Argyrios Zolotas
Jan 2022

CRANFIELD UNIVERSITY

SCHOOL OF AEROSPACE, TRANSPORT AND MANUFACTURING
PhD in Aerospace - Cybersecurity of Embedded Systems

This thesis is submitted in partial fulfilment of the requirements for the
degree of Doctor of Philosophy

Academic Year 2019 - 2022

ABULMOHSAN ALOSEEL

CYBERSECURITY OF EMBEDDED SYSTEMS
A NOVEL APPROACH FOR DETECTING CYBERATTACKS BASED
ON ANOMALOUS PATTERNS OF RESOURCE UTILISATION

Supervisor: Dr. Saba Al-Rubaye
Associate Supervisor: Dr. Argyrios Zolotas
Jan 2022

This thesis is submitted in partial fulfilment of the requirements for the
degree of Doctor of Philosophy

© Cranfield University 2022. All rights reserved. No part of this
publication may be reproduced without the written permission of the
copyright owner.

Abstract

An embedded system (ES) is a processing unit that has been embedded into a larger cyber-physical system (CPS) to steer its functions. The ES has played an essential role in modern life, where it has been used widely in sensing, controlling and computing for countless applications in different domains, such as the internet of things (IoT), smart cities, healthcare, transportation, communication, military, transportation, gas distribution, avionics and national infrastructures. Due to its widespread application in different domains and its evolution in conjunction with many key technologies, it is crucial that these systems are secured against cyberattacks as the ES has the same generic security goals – confidentiality, integrity and availability – as conventional computer systems.

Although the ES is exposed to the numerous and unpredicted security threats that are experienced by conventional computer systems, it is significantly limited in its ability to manage the advanced security solutions that are implemented on conventional computer systems. The limitations in resources of the ES, due to its identity or characteristics, impose tight constraints on both its communication and computing capacity, thereby hindering the implementation of advanced security solutions. Thus, the cybersecurity of an ES is limited by constraints on its resources rather than by the absence of advanced security solutions. There is an urgent need, therefore, to develop security solutions that are compatible with the capabilities of the ES.

This study tried to bridge the gap by addressing both theoretical and empirical aspects of ES cybersecurity. The study can be divided into three main blocks. The first block identifies the key factors, involved parties or entities, and creates the cybersecurity landscape for embedded systems (CSES), while considering the conflict between the requirements for cybersecurity and the computing capabilities of an ESs. Additionally, twelve factors influencing CSES have been extracted and identified based on the direction of the research. These factors have been used to shape a multiple layers feedback framework of embedded system cybersecurity (MuLFESC), with nine layers of protection. It has been developed in line with an expanded model of risk assessment metrics, which will enable cybersecurity practitioners to evaluate the security

countermeasures of their systems and assist in the development of more comprehensive solutions for CSES.

A novel security approach, called anomalous resource consumption detection (ARCD), was developed in the second block of this study. This involved the design of a testbed to provide a realistic hardware-software environment to analyse an example application of an ES. A Smart PiCar was run repeatedly under different operational conditions – typical conditions and under attack. The data of seven designated parameters based on seven statistical criteria was analysed to measure the range, pattern of performance and resource utilisation. The results from this statistical analysis demonstrated the potential for defining a standard pattern for the resource utilisation and performance of the embedded system due to a significant similarity with the values of the parameters at normal states. In contrast, the results from the attacked cases showed a definite and detectable impact on the consumption and performance of the resources of the ES, which presented anomalous patterns. The ARCD method can be implemented as an additional layer of protection to detect cyber-attacks in an ES, where a septenary tuple model, consisting of seven parameters, is the core of the detection mechanism.

In the final block, the ARCD approach has been placed within an architectural framework, which may pave the way for software engineers to build secure operating systems in line with the capabilities of the ES. The architectural framework was developed after the efficiency of the approach was computationally validated by machine learning. This involved the design of a classifier and predictor model to find the predictive accuracy percentage in terms of separating patterns of anomalous performance and resource utilisation from the typical pattern. Based on the confusion matrix, the prediction accuracy for classifying anomalous patterns compared with default patterns revealed promising results, thus proving the effectiveness of the ARCD approach. The results confirmed very high prediction accuracies as regards distinguishing anomalous patterns from the typical patterns.

Keywords: Anomalous detection, Anomalous Resource Consumption Detection, ARCD approach, Brute-force attack, Cybersecurity of embedded system, Denial-of-service attack, Embedded system, Machine learning, Risk assessment, Security framework.

Acknowledgements

The journey of life carries with it many happy and painful events. Studying for a PhD was one of the most enriching experiences in my life. It has had a huge impact on me, not only on the level of cognitive development, but also regarding life experience. Therefore, as a believer, I thank almighty Allah who gave me life and the ability to complete my PhD thesis.

At the beginning of the PhD journey, I thought I could not make a valuable scientific contribution. However, the days were full of many pleasant surprises, as the entire contribution of my PhD thesis was published in one of the best scientific journals in the cybersecurity field (IEEE Access). Therefore, I have to offer my thanks and gratitude to the wonderful people who were around me or whom I met on my PhD trip. First, I thank my mother. This great woman has showered me with kindness and love since my birth and still sees me as her little child, even though I am almost 40 years old. Also, I pay homage to the soul of my father, who passed away during my studies and left behind him great sadness and sorrow. I also extend my thanks to my beautiful wife, who has been a calming influence when the winds of suffering blew. I do not forget to thank my wonderful children, who have always added joy and happiness to my life.

I realised during my PhD experiences that 'as a man thinks, so he is'. Therefore, positive thinking and optimism to achieve my ambitions are some of the most important skills I have learned. My academic achievement, which I am proud of, would not have been completed and seen the light of day had it not been for the wonderful and experienced people who did not hesitate to provide all the necessary support. So, I would like to thank all my wonderful and experienced supervisors, Dr Saba Al-Rubaye, Dr Argyrios Zolotas, Dr Hongmei He, and Dr Muhammad Khan. I also extend a special thanks to Dr Carl Shaw, co-founder of Cerberus Security Laboratories Ltd, for his rich support through his deep experience in the field of cybersecurity.

In conclusion, I realised that the field of scientific research is vast and has no limits, and every researcher can look at things from a different angle. Therefore, I hope that I have succeeded in providing a scientific contribution of high added value to the main body of knowledge in the field of cybersecurity that can be beneficial and be part of the development of science that serves humanity.

Table of Contents

Abstract	I
Acknowledgements	IV
Table of Contents.....	V
List of Figures	X
List of Tables.....	XIV
List of Abbreviations.....	XVI
1. Chapter 1: Introduction	2
1.1. Background.....	2
1.2. Aim and Objectives.	4
1.3. Thesis Structure	5
1.4. List of Publications	9
1.5. References:	10
2. Chapter 2: Cybersecurity for Embedded Systems: Requirements and Challenges.....	13
2.1. Abstract.....	13
2.2. Introduction.....	13
2.3. Embedded Systems	15
2.3.1. Architecture of An Embedded System	15
2.3.2. The Role of Embedded Systems.....	16
2.3.3. Characteristics and Limitations of Embedded Systems	19
2.4. Security Risks of Embedded Systems	23
2.4.1. Security Problems.....	23
2.4.2. Classic Attacks and Impact on ESs	25
2.4.3. Challenges of Implementing CSES	28

2.5. Cybersecurity of Embedded Systems	34
2.5.1. Security Objectives.....	34
2.5.2. Security Countermeasures of ESs	35
2.5.3. Risk Management and Security Incident Response	41
2.6. Conclusion	46
2.7. References:	47
 3. Chapter 3: Assessment Framework for Embedded Systems Security: A Multiple Layers Feedback Framework of Embedded System Cybersecurity (MuLFESC)	61
3.1. Abstract.....	61
3.2. Introduction.....	61
3.3. Analytical Results of CSES	62
3.3.1. Security Risk Metrics	62
3.3.2. Key Factors of the MuLFESC Framework.....	65
3.3.3. Multiple Layers Feedback Framework of Embedded System Cybersecurity (MuLFESC)	70
3.4. Conclusion	76
3.5. References:	77
 4. Chapter 4: A Novel Approach for Detecting Cyberattacks in Embedded Systems Based on Anomalous Patterns of Resource Utilisation.....	83
4.1. Abstract.....	83
4.2. Introduction.....	84
4.3. The Hypothesis and Testbed Configuration	88
4.3.1. The Hypothesis	88
4.3.2. The Testbed	89
4.4. Hardware and software of the testbed	94

4.5. Methodology	95
4.5.1. Configuration of the Experiment Environment	95
4.5.2. Experiment Conduction and Analysis Method.....	97
4.6. Results and Analysis of Normal Cases	99
4.6.1. CPU Utilisation	99
4.6.2. Memory Load	100
4.6.3. Tasks and Threads	101
4.6.4. CPU Temperature	103
4.6.5. Power Consumption Measuring	104
4.6.6. Data Traffic Rate	106
4.7. Attacked Cases Results	109
4.7.1. Denial-of-Service Attack (DoS)	109
4.7.2. Password Attack (Brute-Force Attack)	116
4.7.3. Remote Code Execution Attack (RCE)	121
4.7.4. Man-in-the-Middle Attack (MITM) Remote Command Execution.....	127
4.8. Detection Latency	134
4.9. Conclusion	135
4.10. References:	137
 5. Chapter 5: Attack-Detection Architectural Framework Based on Anomalous Patterns of System Performance and Resource Utilisation	 144
5.1. Abstract.....	144
5.2. Introduction.....	145
5.2.1. Embedded Systems and Cybersecurity Challenges.....	145
5.2.2. Machine Learning for ES Cybersecurity	147
5.3. Applying The Machine Learning Method for ARCD Approach Validation....	151
5.3.1. Approach Hypothesis	151

5.3.2. Machine Learning Algorithm Selection	152
5.4. Case Study Design	153
5.4.1. Normal Conditions	153
5.4.2. Attacked Case Scenarios	154
5.5. Statistical Classification Method Results	155
5.5.1. Machine Learning: Data Normalisation, Modelling Requirements and Attack Prediction	161
5.5.2. Data Preparation and Testing	161
5.5.3. Machine Learning Modelling	162
5.6. Classification Results: Analysis and Validation	164
5.6.1. Confusion Matrix Results	164
5.6.2. Effect of Predictors	165
5.7. Architectural Framework of The Anomalous Resource Consumption Detection (ARCD) Approach	177
5.7.1. Determining The Components:	177
5.7.2. Determining The Functions:	178
5.7.3. Identifying The Typical Pattern:	178
5.7.4. Generating A Standard Model as A Reference Pattern:	180
5.7.5. Designing and Applying the Detection Mechanism:	181
5.7.6. Monitoring The System Performance Pattern:	181
5.7.7. Responding To Anomalous Patterns:	183
5.8. Conclusion	184
5.9. References:	185
6. Chapter 6: Discussion	192
6.1 How can the Security Risk Metrics Model be leveraged in parallel with the MuLFESC framework?	192

6.2. What is the main purpose of developing the MuLFESC framework?.....	192
6.3. Based on what, the detection mechanism of the ARCD approach derived its rationale to be effective and applicable within an OS of an ES?.....	193
6.3.1. CPU utilisation parameter	193
6.3.2. Memory usage parameter	195
6.3.3. Tasks and Threads parameters.....	197
6.3.4. CPU Temperature	200
6.3.5. The voltage and Current parameter	201
6.3.6. Received and Transmitted packets parameters.....	203
6.4. How the ARCD approach can be implemented in line with an ES's resources and capabilities and what are its benefits and flexibility extent?	205
6.5. The mechanism of the detection method has been explained, but how effective is the proposed approach in terms of detection latency?	206
6.6. References.....	209
7. Chapter 7: Conclusions and future work	211
7.1. Conclusions.....	211
7.2. Future Work.....	214
7.3. References.....	215
Appendices: A, B, and C	217
A. Appendix A: Python Functions	217
B. Appendix B: Statistical Results	220
C. Appendix C: Row Data.....	224

List of Figures

Figure 1-1. Conflict between Cybersecurity Requirements and ESs' capabilities	3
Figure 1-2. Thesis chapters content	8
Figure 2-1. Typical architecture of embedded system.....	15
Figure 2-2. Relationship between ESs and cyber-physical systems.....	17
Figure 2-3. The relations between all relevant concepts.	18
Figure 2-4. TCP/IP layers and attacks [4].	27
Figure 2-5. The 27 different angles [84].....	39
Figure 2-6. NIST Security Life Cycle [54].....	41
Figure 2-7. Research directions in cybersecurity requirements of ESs	44
Figure 3-1. Security Risk Metrics.....	65
Figure 3-2. The relationship between the twelve factors.....	70
Figure 3-3. The MuLFESC framework.	71
Figure 3-4 . Overall landscape of Cyber Security of Embedded Systems.....	75
Figure 4-1. (A) The testbed: A Smart PiCar with its schematic diagram.....	94
Figure 4-2. The experiment landscape on the testbed	96
Figure 4-3. Data Processing Stages	98
Figure 4-4. CPU load patterns for R1, R2, and R3.....	99
Figure 4-5. Memory load for R1, R2, and R3.	100
Figure 4-6. Memory load for R1, R2, and R3.	101
Figure 4-7. Tasks number for R1, R2, and R3.....	102
Figure 4-8. Threads number for R1, R2, and R3	103
Figure 4-9. CPU temp (°C) for R1, R2, and R3	103
Figure 4-10. Voltage measurements for R1, R2, and R3.....	105
Figure 4-11. Current measurements for R1, R2, and R3.	106
Figure 4-12. Received packets rates for R1, R2, and R3.....	107
Figure 4-13. Transmitted packets rates for R1, R2, and R3	108
Figure 4-14. CPU load pattern DoS attack vs R1, R2, and R3.....	110
Figure 4-15. CPU range under DoS attack vs R1, R2, and R3.....	111
Figure 4-16. Memory load under DoS attack vs R1, R2, and R3.....	111
Figure 4-17. Tasks number under DoS attack vs R1, R2, and R3.....	112
Figure 4-18. Tasks range (XgV) under DoS attack vs R1, R2, and R3.....	113

Figure 4-19. Threads pattern under DoS attack vs R1, R2, and R3.	113
Figure 4-20. Threads range (XgV) under DoS attack vs R1, R2, and R3	114
Figure 4-21. Voltage measurements under DoS attack vs R1, R2, and R3.....	114
Figure 4-22. Current measurements under DoS attack vs R1, R2, and R3	115
Figure 4-23. CPU Temp under DoS attack vs R1, R2, and R3	116
Figure 4-24. CPU load pattern under BF attack vs R1, R2, and R3.....	117
Figure 4-25. Memory load pattern under BF attack vs R1, R2, and R3.....	118
Figure 4-26. Tasks pattern under BF attack vs R1, R2, and R3	119
Figure 4-27. Threads pattern under password attack vs R1, R2, and R3	119
Figure 4-28. Voltage pattern under BF attack vs R1, R2, and R3.....	120
Figure 4-29. Current pattern under BF attack vs R1, R2, and R3	120
Figure 4-30. CPU temp under BF attack vs R1, R2, and R3.....	121
Figure 4-31. CPU load pattern under RCE attack vs R1, R2, and R3.....	122
Figure 4-32. Memory load pattern under RCE attack vs R1, R2, and R3.	123
Figure 4-33. Alive tasks pattern under RCE attack vs R1, R2, and R3.....	124
Figure 4-34. Threads pattern under RCE attack vs R1, R2, and R3.....	124
Figure 4-35. Voltage pattern under RCE attack vs R1, R2, and R3.....	125
Figure 4-36. Current pattern under RCE attack vs R1, R2, and R3	125
Figure 4-37. Received packets rates under RCE attack vs R1, R2, and R3.	126
Figure 4-38. Transmitted packets rates under RCE attack vs R1, R2, and R3.....	126
Figure 4-39. CPU temp under RCE attack vs R1, R2, and R3.....	127
Figure 4-40. CPU load pattern under MITM attack vs R1, R2, and R3.....	129
Figure 4-41. Memory load pattern under MITM attack vs R1, R2, and R3.....	129
Figure 4-42. Tasks pattern under MITM attack vs R1, R2, and R3	130
Figure 4-43. Threads pattern under MITM attack vs R1, R2, and R3.....	130
Figure 4-44. Voltage pattern under MITM attack vs R1, R2, and R3.....	131
Figure 4-45. Current pattern under MITM attack vs R1, R2, and R3	131
Figure 4-46. Received packets rates under MITM attack vs R1, R2, and R3	132
Figure 4-47. Transmitted packets under MITM attack vs R1, R2, and R3	132
Figure 4-48. CPU temp under MITM attack vs R1, R2, and R3.....	133
Figure 5-1. Machine Learning roots.	149
Figure 5-2. Assembled Smart PiCar as a testbed.....	151

Figure 5-3. The support vector machine algorithm principle.	152
Figure 5-4. Typical patterns (Rs) vs. anomalous patterns (DoS and BF).....	159
Figure 5-5. Typical patterns (Rs) vs. anomalous patterns (RCE and MITM).	160
Figure 5-6. Confusion matrix 1 (Rs cases vs. attack cases).....	164
Figure 5-7. Confusion matrix 2 (Rs cases vs. attacked cases).....	165
Figure 5-8. CPU pattern classification (Rs cases vs. DoS and BF).....	166
Figure 5-9. CPU pattern classification (Rs cases vs. RCE and MITM).	167
Figure 5-10. Memory pattern classification (Rs cases vs. DoS and BF).....	167
Figure 5-11. Memory pattern classification (Rs cases vs. RCE and MITM).	168
Figure 5-12. Task pattern classification (Rs cases vs. DoS and BF).....	169
Figure 5-13. Task pattern classification (Rs cases vs. RCE and MITM)	169
Figure 5-14. Thread pattern classification (Rs cases vs. DoS and BF).	170
Figure 5-15. Thread pattern classification (Rs cases vs. RCE and MITM).....	170
Figure 5-16. CPU temp. pattern classification (Rs cases vs. DoS and BF).....	172
Figure 5-17. CPU temp. pattern classification (Rs cases vs. RCE and MITM).	172
Figure 5-18. Voltage pattern classification (Rs cases vs. DoS and BF).....	173
Figure 5-19. Voltage pattern classification (Rs cases vs. RCE and MITM).	174
Figure 5-20. Current pattern classification (Rs cases vs. DoS and BF).	174
Figure 5-21. Current pattern classification (Rs cases vs. RCE and MITM).....	175
Figure 5-22. RX-rate pattern classification (Rs cases vs. RCE and MITM).	175
Figure 5-23. TX-rate pattern classification (Rs cases vs. RCE and MITM).	176
Figure 5-24. Architectural framework of ARCD approach.	182
Figure 5-25. Chronology of the attack detection and events sequence.	183
Figure 6-1. Overall CPU ranges for attacked cases vs standard cases.	194
Figure 6-2. Overall memory ranges for attacked cases vs standard cases.....	196
Figure 6-3. Overall tasks range for attacked cases vs standard cases.....	198
Figure 6-4. Overall threads range for attacked cases vs standard cases.	199
Figure 6-5. Overall temp ranges for attacked cases vs standard cases.	200
Figure 6-6. Overall voltage patterns for attacked cases vs standard cases.	201
Figure 6-7. Overall current patterns for attacked cases vs standard cases.....	202
Figure 6-8. Overall RX patterns for MITM attack vs standard cases.....	203
Figure 6-9. Overall TX patterns for RCE attack vs standard cases	204

Figure 6-10. Overall TX patterns for MITM attack vs standard cases.....	205
Figure 6-11: Snapshots of real time observation.....	208

List of Tables

Table 1-1: Thesis Structure.....	7
Table 2-1. Limitations due to the characteristics of ESs.	21
Table 2-2. Security problems due to the limitations of the ES.	22
Table 2-3. Summary of the research directions on security risks aspects of the ESs....	31
Table 2-4. Research directions in cybersecurity requirements of ESs.....	45
Table 3-1. Security risks against MuLFESC layers.....	74
Table 4-1: Parameters of the testbed	93
Table 4-2: Statistical Analysis Criteria.....	93
Table 4-3: CPU Utilisation Under Normal Operating Conditions	99
Table 4-4: Memory performance under standard operating conditions	100
Table 4-5: Values of tasks number under standard operating conditions.....	102
Table 4-6: Values of Threads number under standard operating conditions.....	102
Table 4-7: CPU Temp Under Standard Operating Conditions	104
Table 4-8: values of voltage (V) under typical operating conditions	105
Table 4-9: current values (Ampere: A) Under typical operating conditions	105
Table 4-10: Received packets rate under standard operating conditions	106
Table 4-11: Transmitted packets rate under standard operating conditions	107
Table 4-12: values of the Generated standard model	108
Table 4-13: Parameters Values under DoS Attack.....	110
Table 4-14: Parameters Values under Brute-Force Attack	117
Table 4-15: Parameters Values under Remote Code Execution Attack	122
Table 4-16: Parameters Values under MITM Attack	128
Table 4-17: Timestamps During Dos Attack.....	134
Table 4-18: Timestamps during Password attack	135
Table 5-1: Summary of the related studies	147
Table 5-2: Statistical classification Results	158
Table 5-3: case classification and response	162
Table 5-4: dataset features	162
Table 5-5: dataset classification.....	163
Table 5-6: trained and test models.....	163
Table 5-7: CPU temperature (°C).....	171

Table 6-1: Overall CPU Performance for all Cases 193

Table 6-2: Overall Memory Performance for all Cases..... 195

Table 6-3: Overall Tasks Number for all Cases 197

Table 6-4: Overall Threads Number for all Cases..... 199

Table 6-5: Overall CPU Temp Number for all Cases 200

Table 6-6: Overall Voltage Consumption for all Cases 202

Table 6-7: Overall Current Consumption for all Cases 202

Table 6-8: Overall Received Packets for all Cases..... 203

Table 6-9: Overall Transmitted Packets for all Cases 204

List of Abbreviations

AI – Artificial Intelligence
APChain – Attack Pattern Chain algorithm
APTs – Advanced Persistent Threats
ARCD – Anomalous Resource Consumption Detection
ASICs – Application Specific Integrated Circuits
BF – Brute Force
CERT – Computer Emergency Response Team
CIA – Confidentiality, Integrity, and Availability
CPS – Cyber-Physical System
CPU – Central Processing Unit
CREST – Council for Registered Ethical Security Testers
CRMF – Cybersecurity Risk Management Framework
CSES – Cybersecurity for Embedded Systems
CSRI – Cyber Security Risk Indicator
CSV – Comma-Separated Values
DCS – Distributed Control System
DDoS – Distributed Denial-of-Service attack
DEMA – Differential Electromagnetic Analysis Attacks
DoS – Denial-of-Service attack
DPA – Differential Power Analysis
DSPs – Digital Signal Processors
DTE – Distribution Transforming Encoder
ES – Embedded system
ESs – Embedded Systems
FNR – False Negative Ratio
FPGAs – Field Programmable Gate Arrays
GLIFT – Gate-Level Information Flow Tracking
HATs – Hardware Attached on Tops
HIL – Hardware-in-the-Loop
IACS – Industrial Automation and Control Systems

ICS – Industrial Control Systems
ICs – Integrated Circuits
IDPS – Intrusion Detection and Prevention Systems
IDS – Intrusion Detection Systems
IEMI – Intentional Electromagnetic Interference attacks
IIoT – Industrial Internet of Things
IoS – Internet of Services
IoT – Internet of Things
ISO – International Organization for Standardization
LOIC – Low Orbit Ion Cannon
MANET – Mobile Adoc Networks
MBD – Model-Based Development
MILP – Mixed Integer Linear Programming
MITM – Man-In-The-Middle
MLS – Multiple Levels of Security
MuLFESC – Multiple Layers Feedback Framework of Embedded System Cybersecurity
NADSs – Network Anomaly Detection Systems
NIDSs – Network Intrusion Detection Systems
NIST – National Institute of Standards and Technology
NOC – Network Operations Centre
NSF – National Science Foundation
OS – Operating System
PLCs – Programmable Logic Controllers
PUF – Physical Unclonable Function
RAM – Random-Access Memory
RaNN – Random Neural Network
RBAC – Role-Based Access Control
RCE – Remote Code Execution
RCP – Resource Consumption Performance
ROM – Read Non-volatile Memory
RTES – Real-Time Embedded System
RX – Received packets

SBCs – Single-Board Computers
SCA – Side-Channel Attacks
SCADA – Supervisory Control and Data Acquisition Systems
SCAs – Side-Channel Attacks
SEMA – Simple electromagnetic analysis Attack
SOC – Security Operations Center
SoC – System on Chip
SPD – Security, Privacy, and Dependability
SSH – Secure Shell protocol
SSL – Secure Sockets Layer
SVM – Support Vector Machine
TCP/IP – Transmission Control Protocol/Internet Protocol
TLS – Transport Layer Security
TPR – True Positive Ratio
TX – Transmitted packets
UDP – User Datagram Protocol
VPs – Virtual Prototypes
WSNs – Wireless Sensor Networks

Chapter 1: Introduction

CHAPTER 1: INTRODUCTION

1.1. Background

The embedded system (ES), in its simplest form, is manifested when a processing unit is integrated into a larger physical system to steer its functions. The system has experienced several stages of development over the decades. The capabilities of ESs evolved in conjunction with several key technologies. The most common technologies are integrated circuits (ICs), such as field programmable gate arrays (FPGAs) and application specific integrated circuits (ASICs). The difference between FPGAs and ASICs is that FPGAs are reconfigurable, whereas ASICs must be pre-configured for the purpose for which they are manufactured. During the development of the embedded system, the inclusion of programmable logic controllers (PLCs), microcontrollers and microprocessors played a vital role in advancing the capabilities of ESs and allowed them to be used in a wide variety of applications. ESs have shown great potential in internet of things (IoT) network connected systems, and their capabilities have been increasingly improved, moving closer to those of traditional IT systems.

Considering the enormous expansion and spread of embedded systems in different application domains, such as communication, transportation, education, defence, energy, and medicine, ESs form critical components in cyber-physical systems (CPS) and IoT-enabled systems. Industry 4.0, the industrial internet of things (IIoT), integrates all systems into the internet, such as supervisory control and data acquisition systems (SCADA), industrial automation and control systems (IACS), industrial control systems (ICS), and distributed control systems (DCS). Hence, cybersecurity by design is a critical challenge for the success of these modern applications. This highlights the urgent need to secure these systems against cyber-attacks, which can have catastrophic consequences for both humanity and economies. There are many mature techniques for protecting IT infrastructure. However, compared with conventional multitasking systems, ESs face significant challenges in adopting the existing advanced security solutions due to their capabilities and limiting characteristics, such as small size, small volume of memory, less computational capabilities, low energy consumption, mobility, independence and low

cost. It is necessary to have effective security solutions that maintain security goals and match the capabilities and characteristics of the ES.

Therefore, the lack of effective and efficient security solutions compatible with the capabilities of the ES determines the research gap, where the inability to implement advanced security solutions efficiently is due to the conflict between cybersecurity requirements and the capabilities of the ES. Thus, there is an urgent need to find effective and efficient security solutions compatible with the capabilities of the ES. Since the computational resources of embedded systems are limited [1], [2–5], and the requirements of advanced security solutions are high [6], the security of embedded systems, therefore, is limited by the resource constraints of ESs, rather than the absence of advanced security solutions, as most of the advanced security solutions require a lot of computational resources and high-power consumption. The ESs have limited system resources, and these resources are insufficient to allocate excess system performance for advance cryptographic operations or advance security mechanisms [1]. Therefore, finding effective and efficient solutions that do not drain the ES's resources [1] is a critical challenge (Figure 1.1).

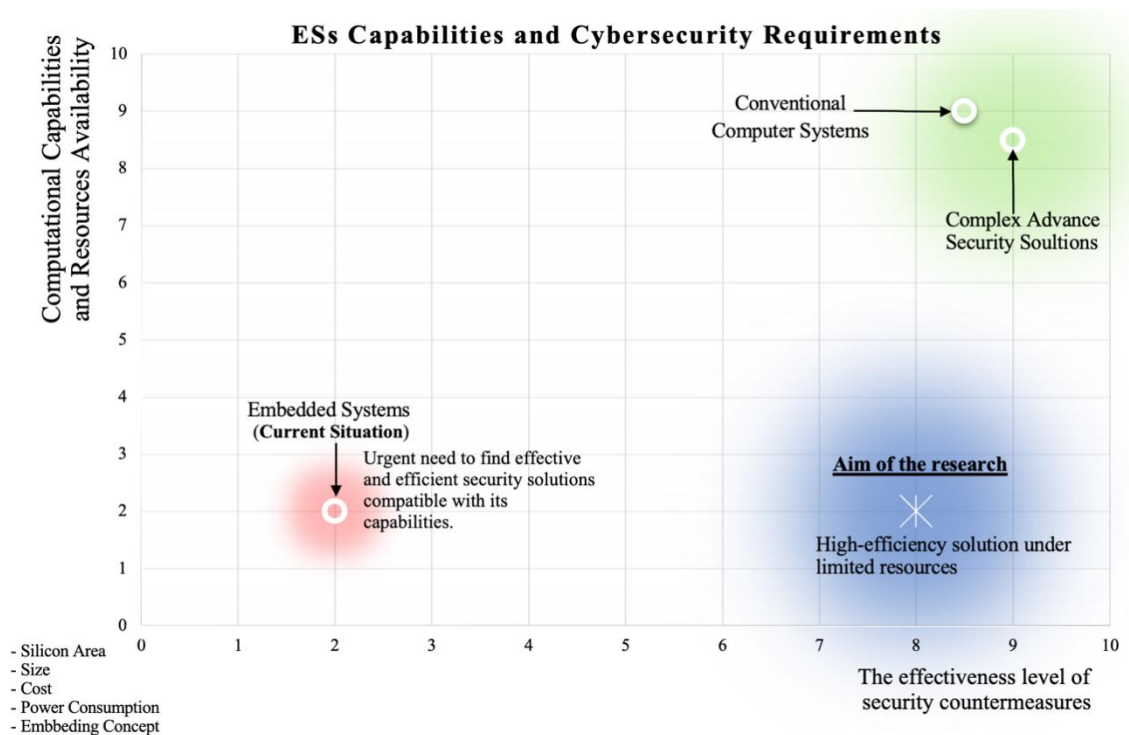


Figure 1-1. Conflict between Cybersecurity Requirements and ESs' capabilities

The reason behind this challenge is the nature of the embedded systems or their characteristics, which dictate that they should be easy to integrate within larger systems to perform a specific task; therefore, ESs should be practical and inexpensive. Consequently, the embedded systems should be small, and require less power consumption and cost. However, this creates a gap between the capability of the embedded system and the requirements of cybersecurity [7][8].

Therefore, the lack of compatible security solutions in line with the capabilities of embedded systems has given attackers the chance to exploit vulnerabilities to conduct various attacks. As with conventional computer systems, the embedded systems are exposed to many security threats, but they are significantly limited in their ability to properly manage the advanced security solutions which are implemented for conventional computers and servers. The relationship between the requirements of cybersecurity and the capabilities of embedded systems is a reversible one. Any attempt to improve an embedded system's physical components to meet the requirements of advanced security solutions will immediately conflict with one of the characteristics of the ES [1] [9].

As long as the advanced countermeasures require more resources to be feasible, a novel security approach for detecting cyber-attacks without draining the resources or conflicting with characteristics of the ES is presented in this research [10], [11]. This approach provides an additional layer of protection that strengthens the current countermeasures without conflicting or replacing the existing solutions. On the contrary, it will harden and empower the operating system to efficiently detect cyber-attacks

1.2. Aim and Objectives.

Having addressed the motivations behind this research and determining its research gap, the main aim and objectives to bridge the gap are defined as follows: the main aim is to improve the cybersecurity of embedded systems by delivering a novel security approach to detecting cyber-attacks. To achieve this aim, six linked objectives have been determined and are described below.

Objective 1. To conduct a literature review in the field of Cybersecurity for Embedded Systems.

Objective 2. To develop a security risks assessment framework supported by security risks metrics by identifying the influencing factors in cybersecurity of ESs based on the research directions.

Based on the literature review, it was hypothesised that: *‘In ESs, which are designed to perform specific functions, performance and resource consumption are within a determinable pattern. Thus, an anomalous pattern, if it exists and is identifiable, can be exploited in comparison to a pre-identifiable reference pattern as an indicator to detect cyber-attacks’*. Accordingly, the remaining objectives of this research were determined as follows:

Objective 3. To set up a controlled testing environment by determining the requirements of the experiment and targeted parameters for performance measurement under different operating conditions – normal and attacked cases.

Objective 4. To develop a statistical classification method – septenary tuple model /the detection mechanism – to evaluate a standard pattern’s determinability and anomalous patterns’ observability.

Objective 5. To validate the efficiency of the proposed approach computationally based on the prediction accuracy percentage results by applying the machine learning method for anomaly detection.

Objective 6. To develop an architectural framework which reflects the concept of the validated approach to facilitate its adoption.

1.3. Thesis Structure

This research has been formatted as a ‘paper-format thesis’ in line with university guidelines. A series of chapters based on published papers forms the content of this thesis. Chapters 2, 3, 4, 5 and 6 have been published in IEEE Xplore, while the adopted methodological approaches to achieve the aim and stated objectives are presented in line with the related chapters. All published papers were written by the first author and have

been reviewed by two primary supervisors, two associate supervisors and an expert invited from the industry, in addition to the reviewers from IEEE, who evaluated and accepted the contribution of this research to be published in the IEEE Xplore.

Chapter 2 includes a literature review of ESs, with a focus on cybersecurity for these systems, where the concept of ESs, their characteristics, the problems resulting from the limitations imposed by those characteristics, and terminologies relating to ESs are addressed. Additionally, the challenges facing ESs resulting from security requirements and their limited capabilities are discussed. Furthermore, the cybersecurity of ESs, including security objectives, countermeasures and risk management are addressed.

Chapter 3 identifies the factors that influence the overall landscape of cybersecurity for ESs. Additionally, a security risks metrics model has been developed to facilitate the implementation of a multiple layers feedback framework of embedded system cybersecurity (MuLFESC). This consists of nine layers of protection from the initial design stage to the operational phase. The security risks metrics model and the 12 influencing factors have been employed to shape the MuLFESC framework, where it can be used as an assessment instrument.

Chapter 4 presents a novel security approach to bridge the research gap and contribute to the main body of knowledge. A series of experiments was executed under different operating conditions to measure the performance and resource consumption of an ES. A septenary tuple model consisting of seven parameters, which shape the detection mechanism, is described in this chapter. A statistical classification method was developed and applied to the collected data to evaluate the effectiveness of this approach regarding the standard pattern determinability and anomalous patterns' observability.

In chapter 5, machine learning (ML) modelling was applied to validate the effectiveness of the proposed approach computationally by using ML algorithms to discover the prediction accuracy in terms of classifying anomalous patterns from typical patterns, thus detecting the existence of the attack. The final part of this research, which involves the development of an architectural framework to facilitate the adoption of the proposed approach, also is presented in this chapter.

An overall discussion regarding the intellectual contribution, implementation of this work and the potential impact of the findings is presented in chapter 6.

Finally, the conclusions from this research are presented in chapter 7. This chapter also provides recommendations and suggestions for future work. A summary and an illustration of the structure of this thesis are shown in Table 1-1 and Figure 1.1.

Table 1-1: Thesis Structure

Chapter	Objective	Focus/ Deliverables/Contribution	Journal	Status
1	-	Introduction		
2	1	Literature Cybersecurity of Embedded Systems, Research gap determination (Review Paper).	IEEE Access	Published
3	2	Influencing factors, Security Risks Metrics Model, and MuLFESC security assessment framework.	IEEE Access	Published
4	3 and 4	Developing the Anomalous Resources Consumption Detection (ARCD) approach by applying a developed Statistical Classification method.	IEEE Access	Published
5	5 and 6	Delivering the Architecture Framework for the proposed approach (ARCD) by using Machine Learning method (The Support Vector Machine algorithm).	IEEE Access	Published
6	-	Discussion.	IEEE Access	Published
7	-	Conclusions		

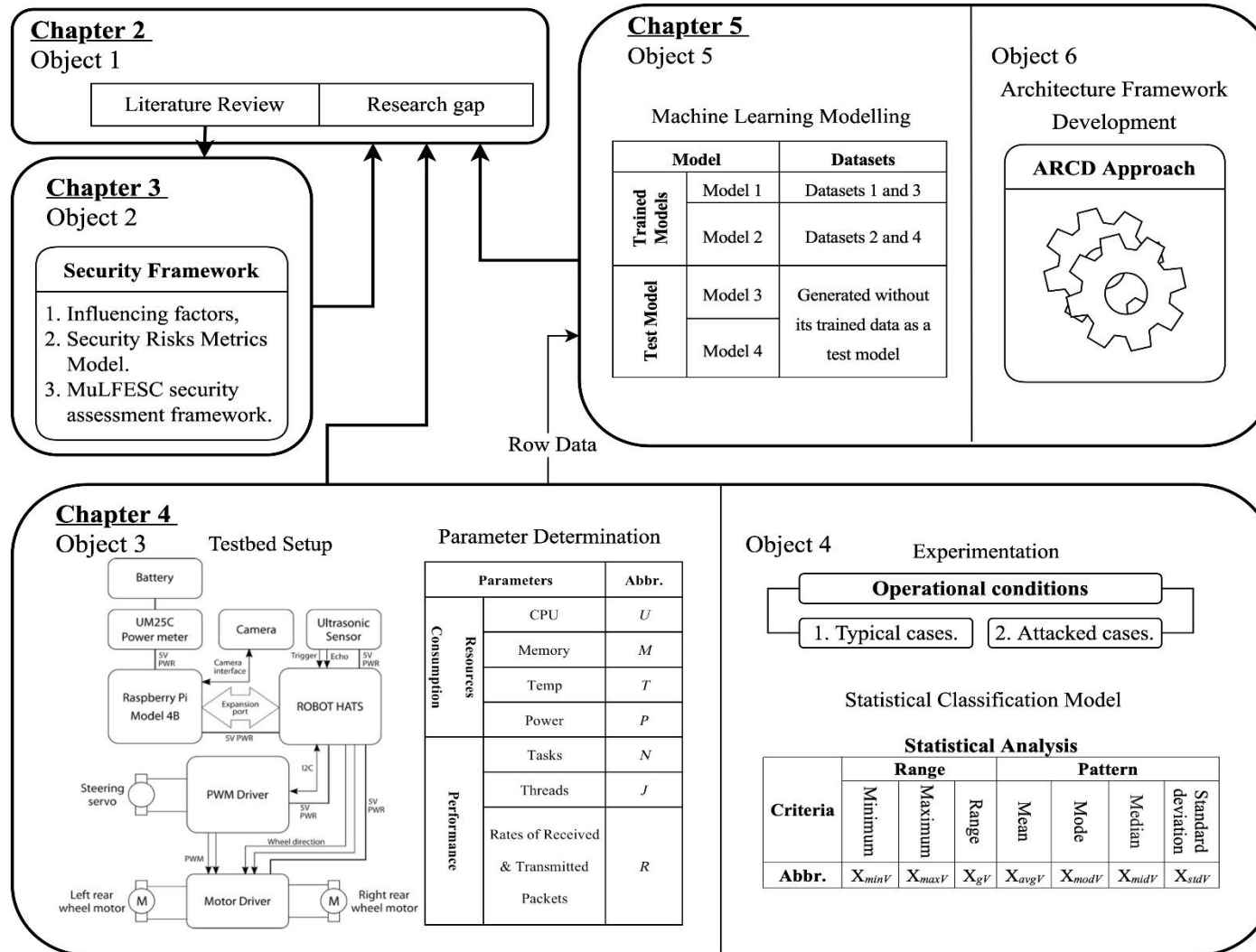


Figure 1-2. Thesis chapters content

1.4. List of Publications

- **Paper 1:** Analytical Review of Cybersecurity for Embedded Systems [1]:
DOI: [10.1109/ACCESS.2020.3045972](https://doi.org/10.1109/ACCESS.2020.3045972)
- **Paper 2:** A Novel Approach for Detecting Cyberattacks in Embedded Systems Based on Anomalous Patterns of Resource Utilization-Part I, [10]:
DOI: [10.1109/ACCESS.2021.3088395](https://doi.org/10.1109/ACCESS.2021.3088395)
- **Paper 3:** Attack-Detection Architectural Framework Based on Anomalous Patterns of System Performance and Resource Utilization—Part II, [11]:
DOI: [10.1109/ACCESS.2021.3088411](https://doi.org/10.1109/ACCESS.2021.3088411)

1.5. References:

1. Alooseel A., He H., Shaw C., Khan MA. Analytical Review of Cybersecurity for Embedded Systems. *IEEE Access*. 2021; 9: 961–982. Available at: DOI:10.1109/ACCESS.2020.3045972
2. Wang W., Zhang X., Hao Q., Zhang Z., Xu B., Dong H., et al. Hardware-enhanced protection for the runtime data security in embedded systems. *Electronics (Switzerland)*. 2 January 2019; 8(1): 52. Available at: DOI:10.3390/electronics8010052 (Accessed: 8 September 2019)
3. Ali S., Balushi T., Nadir Z., Hussain O., Ali S., Balushi T., et al. *Cyber Security for Cyber Physical Systems*. Springer. Cham: Springer International Publishing; 2018; 768: 11–33. Available at: DOI:10.1007/978-3-319-75880-0_2 (Accessed: 15 August 2019)
4. Bodei C., Chessa S., Galletta L. Measuring security in IoT communications. *Theoretical Computer Science*. Elsevier B.V.; 2019; 764: 100–124. Available at: DOI:10.1016/j.tcs.2018.12.002
5. Loukas G., Karapistoli E., Panaousis E., Sarigiannidis P., Bezemskij A., Vuong T. A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles. *Ad Hoc Networks*. Elsevier B.V.; 2019; 84: 124–147. Available at: DOI:10.1016/j.adhoc.2018.10.002
6. Habibzadeh H., Nussbaum BH., Anjomshoa F., Kantarci B., Soyata T. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*. Elsevier; October 2019; 50(June): 101660. Available at: DOI:10.1016/j.scs.2019.101660
7. Radoglou Grammatikis PI., Sarigiannidis PG., Moscholios ID. Securing the Internet of Things: Challenges, threats and solutions. *Internet of Things*. Elsevier B.V.; 2018; 5: 41–70. Available at: DOI:10.1016/j.iot.2018.11.003
8. Ravi S., Kocher P., Lee R., McGraw G., Raghunathan A. Security as a new dimension in embedded system design. *Proceedings of the 41st annual conference on Design automation - DAC '04*. New York, New York, USA: ACM Press; 2004. p. 753. Available at: DOI:10.1145/996566.996771
9. Marwedel P. *Embedded System Design*. Cham: Springer International Publishing; 2018. Available at: DOI:10.1007/978-3-319-56045-8 (Accessed: 15 August 2019)

10. Aloheel A., Al-Rubaye S., Zolotas A., He H., Shaw C. A Novel Approach for Detecting Cyberattacks in Embedded Systems Based on Anomalous Patterns of Resource Utilization-Part I. IEEE Access. 2021; 9: 103204–103229. Available at: DOI:10.1109/ACCESS.2021.3088395
11. Aloheel A., Al-Rubaye S., Zolotas A., Shaw C. Attack-Detection Architectural Framework Based on Anomalous Patterns of System Performance and Resource Utilization—Part II. IEEE Access. 2021; 9: 87611–87629. Available at: DOI:10.1109/ACCESS.2021.3088411

CHAPTER 2: CYBERSECURITY FOR EMBEDDED SYSTEMS: REQUIREMENTS AND CHALLENGES

CHAPTER 2: CYBERSECURITY FOR EMBEDDED SYSTEMS: REQUIREMENTS AND CHALLENGES

Abdulmohsan Alooseel¹, Hongmei He (Senior Member, IEEE)¹, Carl Shaw², Muhammad Ali Khan¹

¹School of Aerospace, Transport and Manufacturing (SATM), Cranfield University

²Cerberus Security Laboratories Ltd, UK.

2.1. Abstract

To identify the key factors and create the landscape of cybersecurity for embedded systems (CSES), a literature review of the existing research on CSES has been conducted. The common properties of embedded systems, such as mobility, small size, low cost, independence, and limited power consumption when compared to traditional computer systems, have caused many challenges in CSES. The conflict between cybersecurity requirements and the computing capabilities of embedded systems makes it critical to implement sophisticated security countermeasures against cyber-attacks in an embedded system with limited resources, without draining those resources.

2.2. Introduction

Technology is experiencing significant development because of the expansion of Cyber-Physical Systems (CPS), or IoT-enabled CPS. In all application domains of IoT-enabled CPS, such as Smart Cities, Supervisory Control, and Data Acquisition systems (SCADA), healthcare, transportation, communication, military, unmanned vehicles, smartphone, smart grids, gas distribution systems, avionics, and wearable devices, ESs have played significant roles in sensing, computing, and controlling.

The IoT and its cyber-physical environment bring great benefits by connecting people, processes, and data. However, IoT-enabled systems can be threatened by a wide variety of cyber-attacks from criminals, terrorists, and hackers [1]. Connecting all devices to the Internet and using off-the-shelf solutions is causing the vulnerabilities of CPS to grow [2]. If we look at what damage cyber-attacks can cause to traditional computer systems despite their computing capabilities, we will recognize the scale of the challenge that faces ESs, with their limited capabilities, when dealing with these cyber-attacks. The high profile WannaCry ransomware attacks in May 2017 showed how victims could be prevented from using their computers or accessing their data. The UK, Spain, Russia, Ukraine, and Taiwan

were among the affected countries, with vital data, including confidential medical records, being held to ransom [3]. In another example, a malicious actor infiltrated a German steel facility in 2014, where the adversary used a spear-phishing email to gain access to the corporate network and then moved into the plant network, resulting in massive physical damage [1], [4], [5]. Cyberattacks clearly have the potential to disrupt or damage physical systems in various application domains mentioned above [1], as the previous developers did not take cybersecurity into account in the design of ESs.

With connectivity to the Internet, ESs are more vulnerable to cyberattacks than ever before and with their limited resources, the problem is exacerbated. In addition, the many influencing factors and involved parties that should be taken into account makes it difficult to determine where deficiencies lie in security measures. Therefore, the study of CSES needs to consider the application context, and advanced and comprehensive ESs security solutions are necessary because of their crucial roles in a diversity of domains.

This survey aims to identify the security challenges and gaps in CSES by determining the influencing factors and related parties, thereby assessing the current status of countermeasures and security solutions against cyber-attacks. To appraise the factors that could affect cybersecurity, we need to understand the structure of the embedded system, its hardware and software components, security objectives, and the vulnerabilities that an attacker can exploit, as well the role of the related parties, including manufacturers, operators, users, and legislators. In this way we can draw the overall landscape of the CSES to help find better solutions.

The remaining part of this chapter is divided into four main sections. Section 2.3 addresses the concept of ESs, their characteristics, and related terminologies, as well as the problems that are a result of the limitations imposed by those characteristics. In Section 2.4, the security challenges facing ESs as a result of security requirements and, in contrast, their capabilities are discussed. In Section 2.5, cybersecurity is addressed in relation to security objectives, countermeasures, and risk management. Finally, the conclusion is provided in section 2.6.

2.3. Embedded Systems

There are many definitions of ESs based on different perspectives. As Vahid and Givargis [6] stated, it is not easy to provide a precise definition of embedded computing systems, or simply embedded systems, and they stated that “an embedded system is a computing system built into a larger system, designed for dedicated functions. It consists of a combination of hardware, software, and optionally mechanical parts. Thus, the term refers to any computing systems other than general-purpose PC or mainframe computers.”[7]. It is noticeable that the main criterion in calling a system an embedded system is the embedding of a processing unit or the integration of computational functionality within a larger physical system to steer the functions of that CPS. Thus, naming an embedded system does not depend on a specific type of logic circuit, CPU, or architecture.

2.3.1. Architecture of An Embedded System

Understanding the construction of the embedded system in terms of entry points and the attack surface leads us to predict which aspects should be protected from the risks of cyberattacks. The field of ESs is vast. Due to the widespread application of ESs in different technical domains, the design of the architecture of ESs in different applications is not limited to a particular form. Manufacturers seek to configure the design to fit the purpose it was designed for. An embedded system is typically comprised of CPU, RAM, ROM, and input/output ports [8]. Figure 2-1 depicts the typical architecture of ESs.

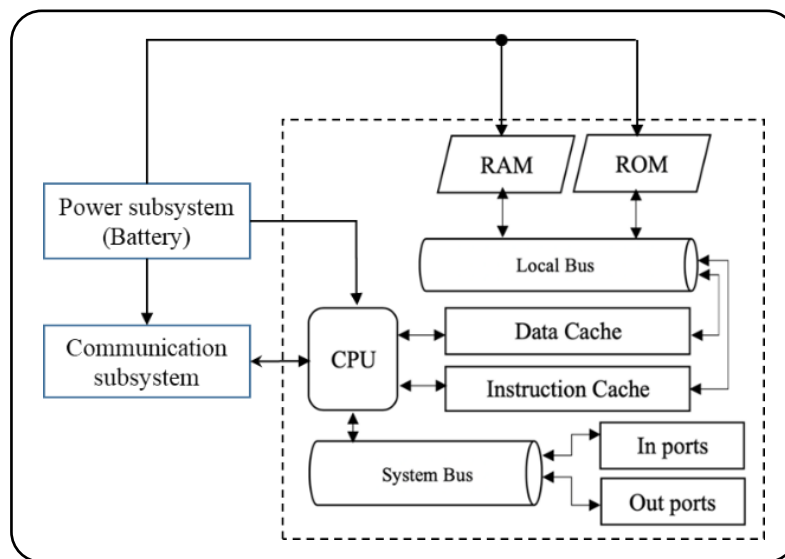


Figure 2-1. Typical architecture of embedded system.

Also, the embedded system CPU can be constructed with instruction cache and data cache or without the I/D caches to keep the CPU architecture simpler and less expensive. To support information exchange or communication, the bus system of an embedded system includes the system bus and the local bus. The CPU is the heart of an embedded system, but other components must be added, such as memory and peripheral interfaces, in order to construct the embedded system.

Designs range from small electronic circuits, through microcontrollers with a small number of transistors and the capacity of 8 bits, to multiple core 64-bit microprocessors with speeds over 1 GHz. Various application-specific CPU implementations and architectures are also used, such as FPGA soft or hard cores, digital signal processors (DSPs), or even recent cores optimized for machine learning. This leads us to an important term, System on Chip (SoC): an integrated circuit (IC, also known as a “chip”) that integrates all components of a computer, in addition to the digital and analogue interfaces. A SoC can be built based on a microcontroller or microprocessor, depending on the purpose of the application. An embedded system can exchange information with external devices through I/O ports. To exchange information remotely, an ES usually is connected to a communication subsystem. The power subsystem provides the power to the components of the ES, with many being battery-powered.

There are various types of embedded systems currently on the market. For example, **Raspberry Pi** is a series of small, inexpensive, single-board computers (SBCs) developed in the UK by the Raspberry Pi Foundation; **Beaglebone** is a low-power, open-source SBC produced by Texas Instruments in association with Digi-Key and Newark element14; and **Jetson Nano** is a small, powerful computer for embedded applications and AI IoT that delivers the power of modern AI in a module. These SBCs have been used widely in education, experimentation, and innovation projects. Süzen et al. [9] provided a benchmark analysis study addressing this category of systems.

2.3.2. The Role of Embedded Systems

When discussing embedded systems, it is necessary to know the relationship and difference between embedded systems and some terminologies, such as CPS and IoT. In 2006, the term “CPS” was coined by Helen Gill from the National Science Foundation (NSF).

According to [10], “The term of cyber-physical systems refers to the tight conjoining of and coordination between computational and physical resources”. One of the essential characteristics that shape the cyber-physical system concept is the ability to interact with the physical world via actuators or sensors. Whereas a cyber-physical system interacts with the external physical world, the responsibility of computational operations lies on the embedded system to steer the physical parts to perform its predefined functions. An embedded system is a co-design of hardware and software. The architecture of the hardware system is shown in Figure 2-1. The software system of an embedded system consists of the Operating System (OS) and applications [1], [11]. One of the differences between embedded systems and conventional computers is that they are designed to perform specific functions and they are integrated into a larger physical system. Sensors are used to sense the external environment, and actuators are used to steer the larger physical system. From this point of view, the embedded system is, as a computing unit, added to a physical system to shape the concept of the cyber-physical system [11], [2], [12], as shown in Figure 2-2.

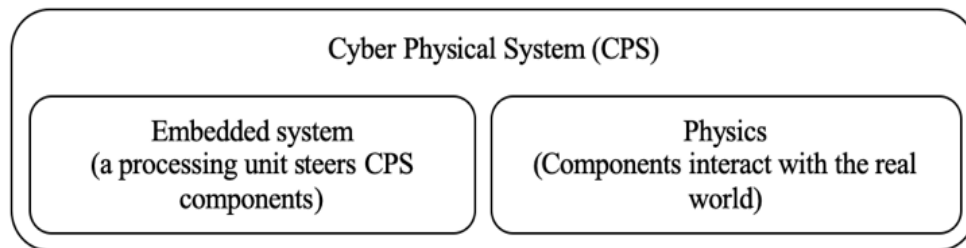


Figure 2-2. Relationship between ESs and cyber-physical systems.

Therefore, CPS is the result of the combination of information processing and the physical environment by using computing processing. Similarly, in [11], [13], “Cyber-physical systems are integrations of computation and physical processes.”[12] The European Commission [14] also defined the concept of cyber-physical systems as “the next generation of embedded ICT systems that are interconnected and collaborated through the Internet of things and provide citizens and business with a wide range of innovative applications and services.” Another definition of CPS is given in [15]: “A system is comprised of a set of interacting physical and digital components, which may be centralized or distributed, and provide a combination of sensing, control, computation and networking functions, to influence outcomes in the real world through physical processes.”

Industrial Automation and Control Systems (IACS) and Industrial Control Systems (ICS) are other types of CPS [15]. They are further associated with two concepts, Industry 4.0 and Industrial Internet of Things (IIoT), between which there exists an overlap. “Industry 4.0” was initially coined by the German government as part of its “High-Tech Strategy 2020” in 2010 and is all about connected value chains—connecting and automatically integrating things and processes to form cyber-physical systems [16]. Within the modular structured smart factories of Industry 4.0, CPS monitor physical processes, create a virtual copy of the physical world and make decentralized decisions. With IoT technologies, CPSs communicate and cooperate with each other and with humans in real time. Via the Internet of Services (IoS), both intra- and inter-organizational services are offered and utilized by participants of the value chain [15]. IIoT, first mentioned by General Electric, is a subset of IoT. It leverages the power of smart machines and real-time analytics to take advantage of the data in industries such as manufacturing, transportation, energy and health care, thereby enhancing the productivity and reliability of communication and control in mission-critical applications for transformational business outcomes [15], [17].

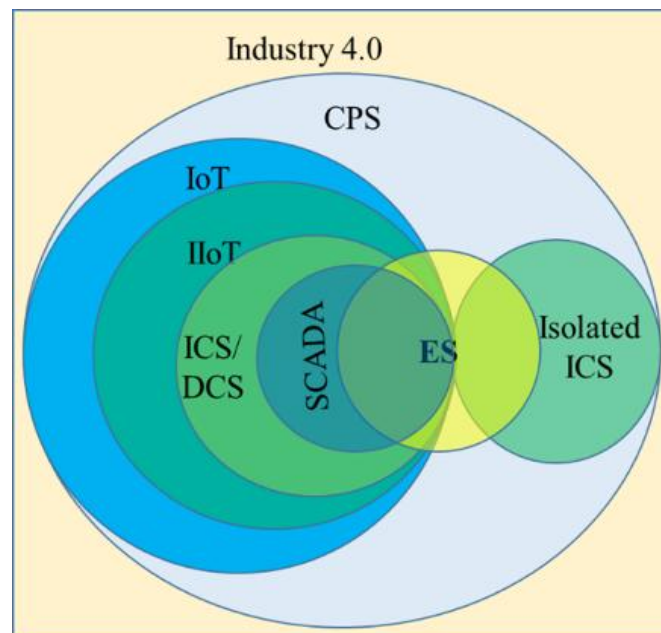


Figure 2-3. The relations between all relevant concepts.

In addition, there are two other terms: Distributed Control System (DCS) and Supervisory Control and Data Acquisition (SCADA). A DCS is a computerized control system for a process or plant, usually with many control loops, in which autonomous controllers are

distributed throughout the system but there is no central operator supervisory control. SCADA is a system comprised of software and hardware to control and monitor a process or application. It allows an operator in a local centre to monitor widely distributed processes (e.g., an oil or gas field, pipeline system, or hydroelectric generators), make set-point changes on distant process controllers (e.g., opening or closing valves or switching), observe alarms, and gather measurement information [4],[15],[18]. The above figure (Fig. 2-3) depicts the abstract relations between all the concepts mentioned above. From Figure 2-3, it can be seen that embedded systems (ES) are the core component in all of these concepts. Therefore, securing ESs is very important in all application domains.

2.3.3. Characteristics and Limitations of Embedded Systems

Embedded systems have been applied in broad fields. In addition to their use in the daily life of individuals, such as cell phones, tablets, and wearable products, ESs have been used in various application domains. For example, in smart home applications they are used to implement surveillance cameras, remote control, cooling systems and temperature control or thermostat systems. The applications of ESs can be extended for governments, organizations, companies, institutions, national infrastructures, in transportation, or to implement the future trend towards smart cities. In terms of their application conditions, embedded systems usually have such characteristics as low power consumption, small size, specific functionality, remote accessibility, unmanned operation, real-time performance, and low cost. These characteristics of ESs demonstrate their superiority over conventional computers in pervasive and ubiquitous computing. However, the connectivity of ESs to the Internet exposes them to the same cyber threats as conventional computers. ESs are characterized as remotely unmanned operation devices, and the nature of ESs, and the fact that they operate without human intervention, increases the chances of an attacker exploiting vulnerabilities to penetrate these systems. Sometimes, embedded systems are required to operate in harsh environmental conditions or under autonomous control where they are far from human supervision, increasing the potential for unauthorized physical access to these systems. This is a fundamental security problem for most IoT devices. Hence, if the attacker gains a fully unauthorized physical access to the system, the confidentiality, integrity, and availability of the system could be breached. As a result, a new challenge has emerged: how to ensure that the security goals of the system are

maintained under these circumstances. The resource limitations of ESs poses tight constraints on both communication and computing capacity [19]. Moreover, the resource constraint problem [13] has given rise to many challenges in creating advanced security solutions for ESs and makes it difficult to meet their cybersecurity requirements. As stated by Meshram and Sasankar [20], “the limited processing power implies that an embedded system typically cannot run applications for defending against attacks as in conventional computer systems (e.g., virus scanner),” and the limited energy also prevents the implementation of advanced security measures. The limited computing resources of ES cannot support complex security schemes [21]. Several studies have addressed characteristics of ESs such as low power consumption and limited computing power in terms of CPU and memory data processing, not only with regard to the system performance requirements but also the problems and weaknesses of securing ESs [22], [23]. The study in [24] addressed the relationship between the characteristics and the problems of an embedded system in implementing IoT devices. Hence, the capabilities of ESs face the challenge of meeting the requirements of advanced security solutions. Table 2-1 summarizes some of the limitations of ESs due to their characteristics, and Table 2-2 presents some of the security problems resulting from these limitations.

Table 2-1. Limitations due to the characteristics of ESs.

References	Study Purpose	Processing Gap	Battery Gap	Memory Gap	Storage	Cost	Connectivity & Flexibility	Real Time	Implement Advanced Countermeasure
[25]	ES design principles	✓	✓	✓		✓	✓		✓
[19]	ESs' security from new dimension	✓	✓	✓	✓				✓
[26]	Security-aware and real-time ES		✓					✓	✓
[27]	Hardware enhancement of ES	✓	✓			✓			✓
[28]	Cybersecurity for cyber-physical system		✓	✓	✓		✓		
[21]	IoT and security measurements	✓		✓			✓		✓
[29]	Taxonomy of detection approaches	✓	✓				✓		
[30]	Data privacy and policy problems survey								✓
[13]	Security requirements and challenges in IoT								✓
[31]	Challenges, threats and solutions of IoT	✓		✓					✓
[32]	A roadmap for security challenges in the IoT	✓	✓						✓

[7]	A taxonomy of threats, vulnerabilities, and attacks.								✓
[33]	A survey of cyber-physical systems security	✓	✓	✓			✓		
[34]	Security framework for IoT	✓	✓		✓				✓

Table 2-2. *Security problems due to the limitations of the ES.*

Limitation of ES	Problems
Limited processing capability	ES cannot run advanced solutions that are used for defenses against attacks as traditional computer or server systems do
Limited available power supply	ES can dedicate only limited power resources to provide system security
Operating in uncontrolled or harsh environment	ES is vulnerable to physical attack
Remote and unmanned operation	This feature imposes difficulties in physical access, monitoring, downloading updates and patches of vulnerabilities
Network connectivity via wireless or wired	This feature enables the attacker to perform remote attacks. The diversity and uncertainty of cyber-attacks make it difficult to predict how and when they occur, so many vulnerabilities can be exploited

2.4. Security Risks of Embedded Systems

2.4.1. Security Problems

Embedded systems are vulnerable to a wide range of attacks that might breach their security. For instance, an exhaustion attack could drain the power resource by increasing computational tasks or the use of peripherals or sensors. Also, ES is vulnerable to physical attacks: if attackers have physical access to the system, they might conduct a physical intrusion, tamper with the integrity of the system, and/or perform snoop attacks on the system bus, as well as possibly causing sensor or peripheral damage.

No matter what kind of system is under consideration, embedded or conventional, they all have generic security objectives: confidentiality, integrity, and availability. For example, malware (e.g., buffer overflow attacks [24]) can attack networked embedded systems. The stored data or cryptographic keys of an embedded system or electronic currency on smart cards are vulnerable to unauthorized access, and they must be protected to ensure the security of ESs. Also, the authenticity of an embedded system is vulnerable to numerous attacks, such as forged, malicious, or incorrect data or information produced by the system's sensors, an unauthorized user, or unauthorized reprogramming.

The processor's capabilities, which are the heart of the embedded system, are at the top of the list, and they are often unable to implement advanced security techniques such as data encryption. Furthermore, the CPUs themselves have insufficient hardware protection against logical and physical attacks. A more robust CPU could mitigate a lot of attacks, but these are more expensive and normally limited to use on smart cards or as dedicated secure elements in SoCs. Assuming that the performance of the processor has been improved in accordance with the requirements of advanced encryption, this creates a new problem: the need for a significant amount of energy, which may not be available in the case of portable systems. However, if these two problems are resolved, we will face a new problem, which is that of cost. A small increase in the cost of

production, even if only a few cents, would be very expensive and would affect competitiveness if millions of units were manufactured [35].

Cybersecurity specialists often try to know the attacker's capabilities to prevent attacks. Indeed, the attacker's abilities depend on what is made available and unprotected in terms of entry points in the attack surface. Hardware components, such as Wi-Fi, Bluetooth, USB or other input/output interfaces, and software systems, such as operating systems or applications, increase the capabilities and flexibility of ESs, but may provide a greater attack surface for hackers; thus, the system becomes more vulnerable for cyberattacks. In other words, if the capabilities of ESs increase in terms of points of connection and input units, then attack surfaces increase, thereby increasing the probability that the system is hacked. Compounding this problem is the easy availability of advanced, low-cost physical attack tools such as ChipWhisperer and ChipShouter that can be used to generate side-channel attacks (SCAs) or glitch attacks [36].

On the other hand, although imposing restrictions on entry points to the embedded system may contribute to reducing the attacker's chances, this conflicts with the importance of system flexibility. The cybersecurity problems of embedded systems are endless, and they differ according to the assessment perspective and technical domain of application. For example, several security problems are related to Internet connectivity; several studies have addressed this problem [2,37,38]. Furthermore, the problem of data privacy and policies was present in a study on smart cities [30], and the problem of resource constraint and the need to design lightweight encryption [39] and energy-efficient countermeasure strategies were discussed in [13,19,20]. The lack of a unified theoretical framework in the design of CPS is an problem that deserves attention [40]. Also among the problems is the operation of ESs in an unattended environment, which creates several security challenges and is easily accessible to the attacker, as well as the problem of the use of off-the-shelf solutions [19]. The initial design stages and their importance, as well as the neglect of the security requirements in the initial stages of design, are discussed in [12] [39], which reinforces the urgent

need to adopt a ‘security by design’ concept, not only for this reason but also because the embedded systems are designed for fixed purposes; thus, a successful attack on one sample of the embedded system’s applications could facilitate the repetition of the attack on other embedded systems of the same type without additional cost or effort.

2.4.2. Classic Attacks and Impact on ESs

Abomhara and Køien [24] addressed security risks in terms of four aspects: vulnerabilities, exposure, threat, and attacks. Vulnerabilities refer to weaknesses in a system, design deficiencies, or weaknesses in policies or procedures that might allow the attackers to have unauthorized access to data, execute illegitimate commands or conduct attacks. Furthermore, vulnerabilities might be found in different software layers: applications, operating systems, or communication protocol stacks [24], [41], [42]. In the context of cybersecurity, a vulnerability is a weakness that can be exploited by a cyberattack to gain unauthorized access to or perform unauthorized actions on a computer system. Vulnerabilities can allow attackers to run code, access a system’s memory, install malware, and steal, destroy, or modify sensitive data.

Exposure risks refer to problems or mistakes in a system configuration that might be exploited by an intruder. Threats refer to the activities that take advantage of security weaknesses in a system to conduct a harmful impact [24], [43]. A cyber threat is a potential malicious act that might exploit a vulnerability to breach security and, therefore, cause possible harm. This threat can be an intentional action, accidental event, or an abnormal circumstance. Cyber threats include unstructured threats, which use existing hacking tools, and structured threats, e.g., Advanced Persistent Threats (APTs), conducted by an expert attacker [24], [28], [44], [45]. APT is a prolonged and targeted cyberattack in which an intruder gains access to a network and tries to remain undetected. An APT attack usually seeks to monitor network activity and breach the confidentiality of data rather than to cause direct damage to the network or organization. APT attacks are often preceded by planning, require tremendous experience, and are intended to spy for a longer term [46].

Cyber-attacks refer to the actions taken by an attacker to cause damage or harm to the system or disrupt normal operations by using different techniques or tools. There are many types of attacks: (a) physical attacks, (b) reconnaissance attacks, (c) denial-of-service (DoS), (d) access attacks, (e) attacks on privacy, (f) cyber-crimes, and (g) destructive [24], [47], [48][52–49]. Several challenges were presented by [2], such as safety, security, and confidentiality, as well as reliability, reparability, and availability; this highlights the importance of cybersecurity defence countermeasures implementation in embedded systems. For network-connected systems, considering the four layers of Transmission Control Protocol/Internet Protocol (TCP/IP) in early stages of designing the embedded system will contribute to hardening the ES. The layers of TCP/IP are Application layer, Transport layer, Network layer, and Link and Physical layer [28]; these layers play an important role in terms of the security of the embedded system, as the weakness of the measures taken in these layers will create many vulnerabilities that the attacker can exploit, and in return, the implementing of best practices in these layers will enhance the stability of the system. The biggest challenge facing an embedded system is when it is connected to the public Internet, as it faces unpredictable cyber threats. Although embedded systems usually sit at the bottom layer—the physical layer of IoT systems—it is crucial to take into account the four layers of the TCP/IP model to consider cyber-threats from upper layers and the direct threat at the physical layer in the design stage of embedded systems. Ali et al. [4] extensively discuss the security threats and vulnerabilities according to the relationship between cyber-physical systems and the TCP/IP model. Fitz et al. [53] discuss the effect of network topography on the stability of cyber-physical systems' connectivity. Networks can be categorized into six types: Star, Bus, Linear, Ring, Tree, and Mesh. Mesh design, which could be partially or fully connected, is the highest cost among these topologies to maintain the connectivity of CPS and its sensors. The International Organization for Standardization (ISO) defines a 7-layer reference network model. The physical layer accounts for an important proportion of energy consumption, in addition to the existence of a lack of unified specific standards for designers and developers of

CPS to mitigate cyber risks. Figure 2- 4 summarizes classic cyberattacks on the TCP/IP layers.

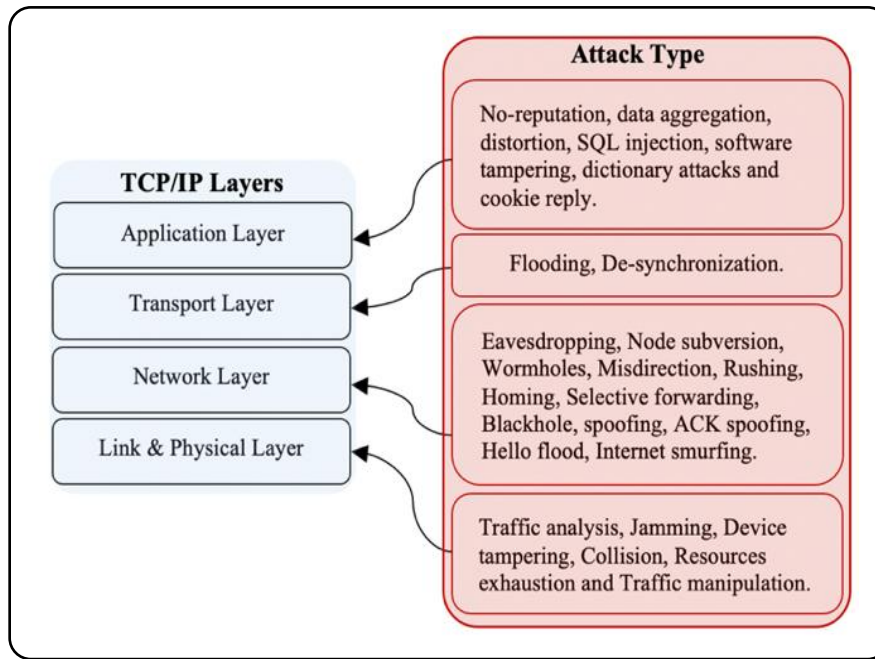


Figure 2-4. TCP/IP layers and attacks [4].

Several valuable documents in the field of research were published by the National Institute of Standards and Technology (NIST) and related to NIST standards [54–60]. The impact of cyber-attacks on the functions of a cyber-physical system was presented in [61] by reviewing a case study of a rail transport system. The case study was performed based on Hardware-in-the-Loop (HIL) simulation to avoid any severe damage or danger for humans in the real world. HIL acts as an interface platform between the physical components (sensors in this case) and an embedded system, acting as the computational part. The effect of a cyber-attack on the efficiency of the functions of CPS was studied. It was shown that digital attacks can affect the effectiveness of the functions of CPS, causing significant delays transiting a signal between a sender and a receiver when the infrastructure is attacked.

Prevention of cyber-attacks is a critical challenge due to the diversity of attacks and the constraints of ESs. One of the most critical stages in dealing with a cyberattack is the detection of the attack itself. Late detection of an attack could allow severe consequences, such as system damage, to occur, whereas early detection allows for a suitable response. However, detection may require significant resources and limit the functionality of the system. An inappropriate response itself could also contribute to an attack and even be used by an attacker. For example, suppose a system disables network connectivity to prevent an attack. In this case, it could be used to direct the re-connection to a fake access point, not to mention the loss of availability during the disconnection time. Some unfinished or unnecessary responses could also conflict with the operation of a device, for example, safety-critical operation, real-time or necessity of immediate functional reaction and synchronization. Hence, an appropriate strategy for detection and response is needed to avoid possible damage but maintain the required functionality of a system, and this is often a compromise.

Each embedded system has its own requirements and, therefore, requires its own security methods. The absence of specific manufacturing standards has exacerbated the problem of creating a unified and comprehensive security solution, [40] although the essence and architecture of embedded systems are, in general, similar. As each system is designed for its own purpose, specific security mechanisms are required to support the functional requirements of the system.

2.4.3. Challenges of Implementing CSES

IoT-enabled cyber-physical systems greatly increase the diversity of ES applications. Conversely, the cybersecurity vulnerabilities of ESs open the doors to countless types of cyber-attacks, and this is one of the biggest challenges facing ESs enabled by IoT technology [2,37,38]. Another challenge for the cybersecurity of ESs lies in the fact that ESs could work in a non-controlled environment [19], in a stand-alone and independent manner. Industry 4.0 raises the new concept of security by design.

Cybersecurity should be considered when designing an embedded system, with specific regard to the security challenges caused by the characteristics of that system.

One of the most challenging aspects of embedded system security design is having to implement the security objectives within the system's capabilities and to do this without focusing on a specific aspect and neglecting to take into account other aspects, or providing non-comprehensive solutions. Habibzadeh et al. [30] found that the problem of existing cybersecurity research lies in the focus on a single component in a system, and they suggested that a robust CPS should have the cybersecurity capabilities of all of its components and that the security of a system is typically determined by its weakest link. Hence, Habibzadeh et al. considered ensuring the overall security of the system is the weakest link that needs to be addressed to have a robust CPS. The "weakest link" concept has been discussed at length in [62], and we can define it in this context as "A guardian is an entity in the system that the attacker could try to pass to gain access to an asset. The cost of passing a guardian determines the negative utility for the attacker when deciding to pass. The cost is typically dependent on the entities an attacker already has access to, such as keys or passwords" [62].

It is important to clearly understand the terminology of security risks, security threats, cyberattacks, vulnerabilities, and exposure risks [24], [7]. The distinction between these terms contributes to clarifying the vision of the nature of the risks facing ESs and their applications and, thus, facilitates the diagnosis of the problem and the finding of an appropriate security solution.

The challenges facing ESs begin at the initial design stages and continue up to the final operational phase. During these stages, some of the most obvious challenges hinder the design of highly efficient countermeasures against cyberattacks, such as processing gap, battery gap, flexibility, tamper resistance, assurance gap, and cost [11,19]. The design process of an ES is influenced predominantly by cost; in terms of the time factor, ES industries always pursue a fast development cycle for market competition. This adversely affects manufacturers in applying high standards for the development of advanced security solutions. Another critical challenge facing ESs is the consumption

and measurement of energy that supports the functions of IoT components [63]. The optimization of energy is demanded due to the constraints on embedded system resources. The battery gap or the power consumption optimization constitutes one of the most challenging design factors [11],[19]. The following table summarizes the research directions on the security risks domain of ESs.

Table 2-3. Summary of the research directions on security risks aspects of the ESs.

Research Directions		Addressed Aspects	References
Risks Taxonomy	Attacks	Actions taken by attacker (techniques or tools).	[24], [47],[48], [52–49]
	Threats	Unstructured threats, Structured threats Threats by Humans or Nature (Unauthorized physical access, Natural Disasters, Earthquake, Hurricanes, or flood).	[4], [19] [28], [24] [44], [45] [46]
	Vulnerabilities	Weaknesses in the system design.	[4], [24] [41], [42]
	Exposure	Problems or mistakes in the system configuration.	[24], [43]
Attack elements	Methods of the attacks	Classification of the attack methods.	[64]
	Surface of the attack	Defining the attack surfaces to determine the entry points of the attack.	[65]
	Attacker capabilities and Tools	Attacker’s skills, Availability of the attack tools such as ChipWhisperer and ChipShouter.	[36]
	Asset’s value	Data sensitivity, Privacy	[30], [61]
	Type of the Attacks	Categorizing security risks based on their nature whether threats, exposure, attack, or vulnerabilities.	[24]

	Connectivity	Network topography, Layers of TCP/IP (Application layer, Transport layer, Network layer, and Link and Physical layer)	[4], [28] [53], [2] [36] ,[37]
Challenges of Implementing CSES	Lightweight cryptographic	Encryption requirements should consider power consumption.	[13]
	Denial of Service attack	DoS attacks can break the availability of the system.	[13], [24]
	Profiling and tracking Localization	Tracking and localization can be a challenge against privacy.	[13]
	Early detection of attacks	It needs the efficient use of system resources.	[13]
	Secure data transmission	The connectivity causes a large number of routing security problems.	[11], [40] ,[41]
	Advanced Persistent Threats (APT)	An attack in which an unauthorized user gains access to a system or network and remains there for an extended period without being detected.	[24]
	Energy Challenge	It is important to concern the consumption and measurement of energy in improving the performance of IoT-enabled physical systems.	[63]
	Processing gap	Weak CPU capabilities versus encryption requirements.	[9], [18]

	Battery gap	One of the biggest challenges, affecting the lifespan of the system.	[26]
	Flexibility (different security protocols)	Compatibility problem due to the difference in the protocol used for data exchange due to flexibility in design as per requirement.	[11]
	Cost sensitivity	Cost is one of the biggest acute factors that constrain investors.	[9], [18]
	Physical attacks	Causing unpredicted damage.	[24]
	Reconnaissance attacks.	Scanning network ports, packet sniffers, traffic analysis, and queries about IP address.	[24]
	Access attacks	Due to the unattended nature of the CPS, might be vulnerable to physical access or unauthorized remote access.	[24]
	Attacks on privacy	Data mining, Cyberespionage, Eavesdropping, Tracking, and password-based attacks.	[24]
	Cyber-crimes	Intellectual property or identity theft or fraud.	[24]
	Destructive attacks	Terrorism and revenge attacks.	[24]
	Attacks against (SCADA)	As an embedded concept, it is subject to the same threats.	[24]

2.5. Cybersecurity of Embedded Systems

In this section, we will address three different aspects: (1) security objectives, (2) security countermeasures, and (3) risk management and security incident response.

2.5.1. Security Objectives

Cybersecurity, as defined in [66], [24], is a process to protect an object against physical damage, unauthorized access, theft, or loss, by maintaining high confidentiality and integrity of information about the object and making information about that object available whenever needed. To implement effective countermeasures, we need to state the security objectives clearly. The generic security objectives for all systems and services are Confidentiality, Integrity, and Availability, called the CIA triangle. Confidentiality means ensuring the information is not made available or disclosed to unauthorized entities; integrity aims to protect the accuracy and completeness, and the availability implies the information is accessible and usable by an authorized entity when it is demanded. In addition to the security triangle, according to [67,68] and based on ISO/IEC 27001:2013, [69], embedded systems should also be designed with concerns of Authenticity, Accountability, Non-repudiation, Reliability, Access Control, Dependability, Safety, and Privacy. These security objectives are the cornerstone of the cybersecurity industry in ESs. From the aspect of attackers, the barriers implemented to meet the security objectives of embedded systems are the target elements of attacks; on the other hand, these security objectives are the goals to be achieved, maintained, and guaranteed by cybersecurity practitioners.

Many studies [19,67,68] have referred to the security triangle, and these security goals are breached by a number of different types of attacks. For example, confidentiality could be breached by side-channel attacks, authentication attacks, password attacks, packet sniffing, and session hijacking. Integrity could be breached by packet dropping or packet delay attacks and spoofing attacks. The availability could be breached by a buffer overflow or Denial of Service (DoS) attack, which target low memory

capabilities and limited computation resources. Most CPS devices are vulnerable to such resource enervation attacks [24].

Industry 4.0 raises the concept of “Security by Design.” Cybersecurity is a critical challenge for the success of industry 4.0. Taking security problems and challenges into account in the design stage of a cyber-physical system is the most efficient and effective solution. Also, it is considered the least expensive approach in the long term, compared to the post-processing of cyberattacks, and reduces the need for more modifications or improvements in the final product. Implementing the convergence between the capabilities of embedded systems and cybersecurity objectives is a dilemma: it conflicts with the current approach, where we always strive to design embedded systems with low cost, small size, and low energy consumption, compatible with mobility and dependability concepts, embeddable in larger CPS, and with efficient and sufficient processing capacity. On the other hand, the requirements of cybersecurity are inconsistent with what we seek, as advanced security measures such as sophisticated encryption or intrusion detection systems (IDS) require high computing capabilities which require increasing the transistor count, which in turn increases the cost, size, and power consumption. Even adopting smaller silicon geometries (e.g., 7nm chips) that could help in terms of size and power has a more expensive up-front cost and, therefore, require higher sales volumes to be profitable and cost-effective [70].

2.5.2. Security Countermeasures of ESs

Security countermeasures for embedded systems have been extensively studied, and most security solutions can be developed in the form of tools, methods, mechanisms, or approaches. Habibzadeh et al. [30] suggested that security countermeasures must be done in four dimensions of physical security: firmware-level, device-level, circuit-level, and energy-harvesting- and storage-level. Dibaji et al. [71] categorized defence mechanisms against cyberattacks into three types: prevention, resilience, and detection and isolation. The prevention mechanism is designed to counter disclosure attacks, such as Advanced Persistent Threats (APTs), and the two main methods are cryptography

and randomization. Resilience refers to the ability of the system to continue to perform its function despite the effects caused by the cyber-attack. Several approaches to implement this mechanism can be applied, for instance, game theory, event-triggered control, mean subsequence reduced algorithms and trust-based approaches. The detection and isolation mechanism consists of five types: observer-based techniques, analytical consistency, watermarking, baiting, and learning-based anomaly detection. Ashibani and Mahmoud [72] highlighted that security measures should take place at three levels to achieve maximum protection: perception, transmission, and application layers.

Attack detection is one of the most important counteractions because it is critical for active countermeasures as it is directly associated with security countermeasures. We must discover the existence of an attack before dealing with it. There are different levels of defence: the first level of defence is to prevent the attack entirely by design, using techniques such as encryption and authentication [73]; the second level is to detect the attack early and deal with it immediately to stop any damage occurring by applying a detection mechanism such as an Intrusion Detection System (IDS) [73]; the third level is to prevent the recurrence of the attack again by taking the required countermeasures after knowing the type of attack and impact of the attack. These levels of defence against cyberattacks require more efficient techniques in different research areas [74], such as vulnerability identification, impact analysis, mitigation, cybersecurity metrics, data and model development, penetration testing, interoperability, and digital forensics. Trawczynski et al. [75] provided an approach to detect a DoS-type attack based on the failure of a single node communication interface. Intrusion Detection and Prevention Systems (IDPS) with multi-mode counteractions is also one of the suggested security solutions [76]. The counteraction technique is to block the attacker's IP address via a firewall, based on the number of packets exceeding the threshold limit in one second. In the case of failure, a remote stop of the corresponding service takes place as a third counteraction. In this context, it is important to note that the requirements of the IDS to

inspect every packet requires a high resource consumption that is not generally compatible with the capabilities of ESs.

A comprehensive survey of physics-based attack detection techniques was provided by [77], where the researchers highlighted that physical components of cyber-physical systems (e.g., actuators or sensors) need to be monitored to detect the attack based on any abnormality in the performance of these physical components. Also, a discrete-time energy-based attack detection mechanism for a networked cyber-physical system was proposed by [78], where the detecting mechanism is based on the energy balance of the system. Among the existing solutions, Poongothai and Duraiswamy [73] applied a machine learning technique in an IDS to mobile ad hoc networks (MANET), which are not conventionally designed with an IDS, as an example of embedded system applications. Whereas encryption and authentication techniques work as the first line of defence, the IDS can work as a second line of defence. Also, problems such as lack of central points, co-operation, shared radio channel, limited resource availability, and the lack of a clear line of defence and secure communication in MANETs have been addressed in [73].

Gu et al. [79] suggested improving security by using a co-processor with the implementation of Mixed Integer Linear Programming (MILP) formulation. Although this approach may contribute to enhancing security aspects, it might conflict with the characteristics of ESs' resources or cost. Wang et al. [27] presented a hardware-enhanced protection method to maintain the confidentiality and integrity of data by using an AES stream encryption engine. Also, a combinational logic binding technique against cloning attacks for FPGA-based embedded systems is discussed in [80]. Negi et al. [81] discussed the embedded systems in the application field of networks, and the study conducted a test in the transfer of data based on Secure Sockets Layer (SSL) and Transport Layer Security (TLS). The adoption of this protocol as a security protocol has shown promising results in terms of sending and receiving data securely on the level of embedded systems.

A survey of EU research efforts in the security solutions of ESs has been done in [82], where security solutions for ESs were classified to several levels: (i) Node-based security technologies, for example a physical unclonable function (PUF), a physically-defined “digital fingerprint” that serves as a unique identity [30]; and (ii) network-based security technologies, focusing on secure routing and Intrusion Detection System (IDS) for a distributed ES network, implemented with middleware and overlay technologies. Among the studies that dealt with security solutions is also a preemptive security mechanism, which is a thin-layer hypervisor-based memory introspection engine on ESs and was proposed by Lukacs et al. [83]. The concept of this mechanism is based on hardware virtualization technology, and this mechanism works on two different levels: privilege level and isolation; and hardware-level virtualization. This technique has been implemented on an x86 CPU, which paved the way for testing this mechanism on ARM Cortex A53 and A57 chips.

Evaluating security requirements to adopt appropriate security countermeasures based on different axes was presented by Elmiligi et al. [84]. According to Elmiligi et al., the security requirements can be evaluated from 27 different angles and based on three main axes. These axes are the programmability level axis, integration level axis, and life-cycle phase axis. Figure 2-5 depicts these axes and their different angles [84].

It is also worth mentioning the criticality of a real-time embedded system (RTES). Specific security countermeasures for RTES can be implemented in two stages: (i) identify specific attacks that could threaten the systems; and (ii) implement security-guaranteed services, overcoming the challenges of real-time performance and energy consumption [26]. The study in [85] showed how security measures could be circumvented in different platforms. This demonstrates the importance of highly robust solutions and their availability for a long period.

A non-intrusive runtime monitoring technique for ensuring the safety and security of ESs was presented in [86]. It is based on the principle that finding and implementing solutions on one aspect may depend on another aspect, because the monitoring of non-intrusive runtime through power consumption has been used to enforce safety and

security in ESs. This shows that some security solutions are indirect. In other words, enhancing specific security aspects of the system will reflect positively on other aspects.

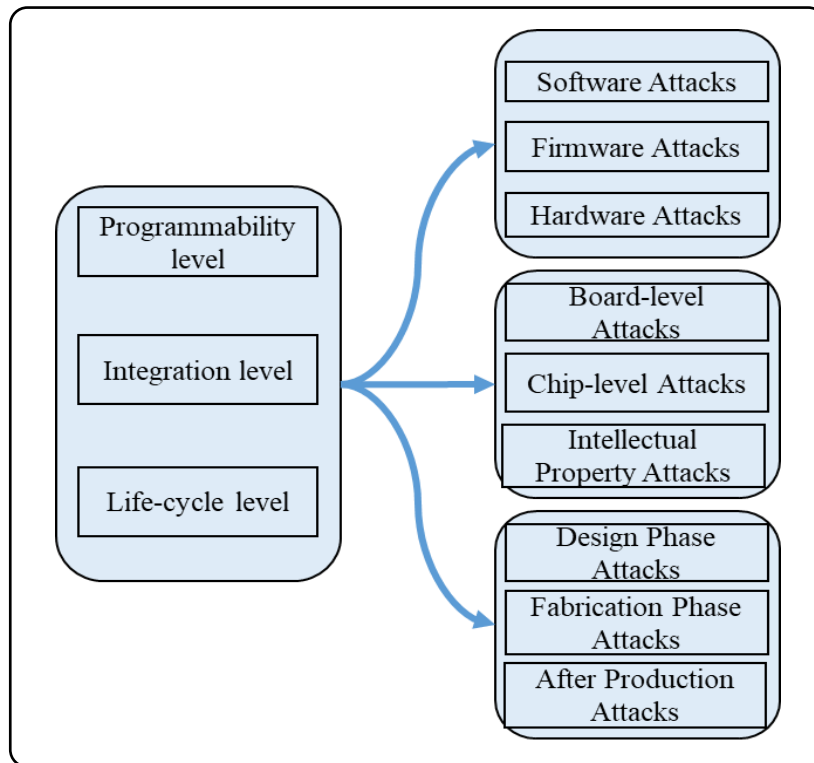


Figure 2-5. The 27 different angles [84].

A multi-metrics approach to ensure and evaluate Security, Privacy, and Dependability (SPD) in ESs is provided in [87], using a smart vehicle as a case study. Also, Mu et al. [88] presented a bottom-up approach for the information flow security of a verifiable embedded system based on Gate-Level Information Flow Tracking (GLIFT), at the early stages of designing ESs. The concept of this approach is based on applying restrictions to the information flow to allow only legitimate data to pass through. Liu [89] proposed a security kernel prototype system to support several security verification strategies—for example, multiple levels of security (MLS), Role-Based Access Control (RBAC), and Distribution Transforming Encoder (DTE) [89]. This security

kernel prototype system focuses on the security kernel in an embedded system, and it is a very generic security prototype system.

“Security by design” is critically required by Industry 4.0. At the design stage of ESs, it is required to integrate security mechanisms into embedded systems according to Model-Based Development (MBD) [90]. Thayer [91] stated that the adversarial testing in the early stage of designing and developing the embedded system would increase the overall awareness of the threats posed to a system. Also, the high energy efficiency of systems supports the implementation of advanced cryptographic techniques [39]. While a stable and sufficient energy source is essential, thus, it is important to optimize the system for minimizing the energy consumption, so that there is enough energy for preventing attacks. Hasler and Shah [92] addressed the security implications for the ultra-low energy consumption of SoC FPGA embedded systems.

A comprehensive framework for modelling and assessment for penetration testing of IoT systems, taking attack surface into account, is presented by [93], using a virtual prototype to validate the design of an IoT system. The adopted model uses virtual prototypes (VPs) as a concept, which is a method or technique implemented to validate a development design before any real implementation. The VP is used to develop a framework that aims to support security measures in the initial stages of designing embedded systems. Also, the authors in [94] presented a comprehensive experimental analysis of automotive attack surfaces. The experiment showed severe vulnerabilities that an attacker could exploit, and the results were shared with relevant industry and government stakeholders. Reducing the attack surface by lowering the attacker's access based on a permission-based security model is presented by [95] for Android applications. The suggested approach is designed for detecting permission gaps, using permission-based software.

In general, the adoption of a security solution depends on several factors: the purpose for which it was designed; the capabilities of ES to handle the solution; the nature of the risks that may be exposed; and technical implementation domains. It is also important to train operators with security awareness and relevant knowledge.

2.5.3. Risk Management and Security Incident Response

Risk management and incident response are important for the cybersecurity of embedded systems, especially networked devices, because security threats cannot be eliminated entirely [73]. A NIST report in 2014 [54] presented a Cybersecurity Risk Management Framework (CRMF) for modern vehicles, where embedded systems are important components. Figure 2-6 depicts the security lifecycle presented by NIST [54].

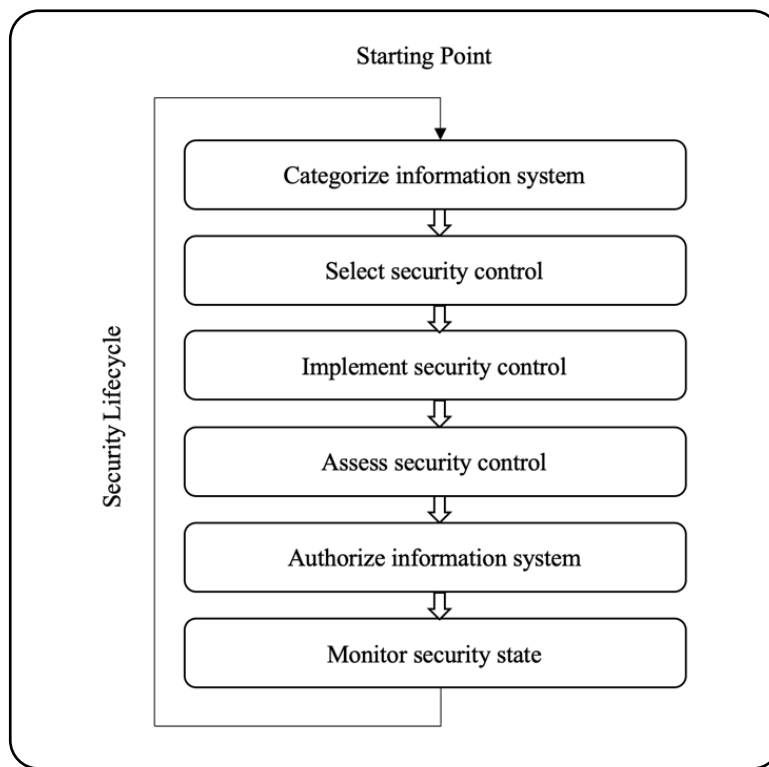


Figure 2-6. NIST Security Life Cycle [54].

Wilbanks [96] proposed a Cyber Risk Management Framework (CRMF) and Cyber Security Risk Indicator (CSRI). CRMF applied three principles: (i) integrating security countermeasures into the systems development lifecycle, (ii) monitoring and maintaining the status of the system, and (iii) interacting with the current situation by making a risk mitigation decision. CSRI measures the efficiency and effectiveness of

the system by using quantitative criteria to assess the robustness of the system, [96], [54].

In terms of incident response, the term ‘incident response’ may be related to other terms, such as ‘incident handling’ and ‘incident management’. NIST does not give strict definitions of “incident handling” and “incident response”. CERT®/CC uses “incident handling” to refer to the overall process of incident detection, reporting, analysis, and response, while “incident response” refers to incident containment, recovery, and notification of others [97]. As stated in the Cyber Security Incident Response Guide from the Council for Registered Ethical Security Testers (CREST) [98], “There is no common understanding of what a cybersecurity incident is, with a wide variety of interpretations. With no agreed definition, many organizations adopt different views.” NIST breaks incident response down into four broad phases: (1) Preparation; (2) Detection and Analysis; (3) Containment, Eradication and Recovery; and (4) Post-Event Activity. Phase 2 and Phase 3 are interactive with each other. Dorofee et al. [99] classified incident management into five major steps: prepare, protect, detect, respond, and sustain. Incident response is not exclusive to administrative level. Some technical solutions can support early incident response, S. Sultana et al. [100] provided a security incident response and prevention system (Kinesis) for Wireless Sensor Networks (WSNs). This system can dynamically respond to anomalous events, based on a suspect’s security status, and does not require any central authority to trigger an action.

According to CREST [98],[101], cybersecurity incidents, particularly serious cybersecurity attacks (e.g., advanced persistent threats (APTs)) have been causing serious damage to organizations, governments, and international bodies. Computer Emergency Response Team (CERT) [99],[102], and NIST [53],[54] have made significant contributions in the subject of cybersecurity incident responses.

As long as the ESs are as essential as traditional computer systems and given the widespread applications of ESs in many domains and at different levels in governments, organizations, and individuals, the supervising parties must have plans to respond to possible incidents following recommended standards such as CRMF or

CSRI. If all security measures at all levels fail to prevent and tackle a cyber-attack, the responsible parties must at least be able to have a fast response to the incident caused by the attack, thereby reducing the damages and economic loss. They must learn from the incident to ensure that the attack does not recur in the future again. Table 2-4 and Figure 2-7 summarize the research directions on the cybersecurity domain of the ES.

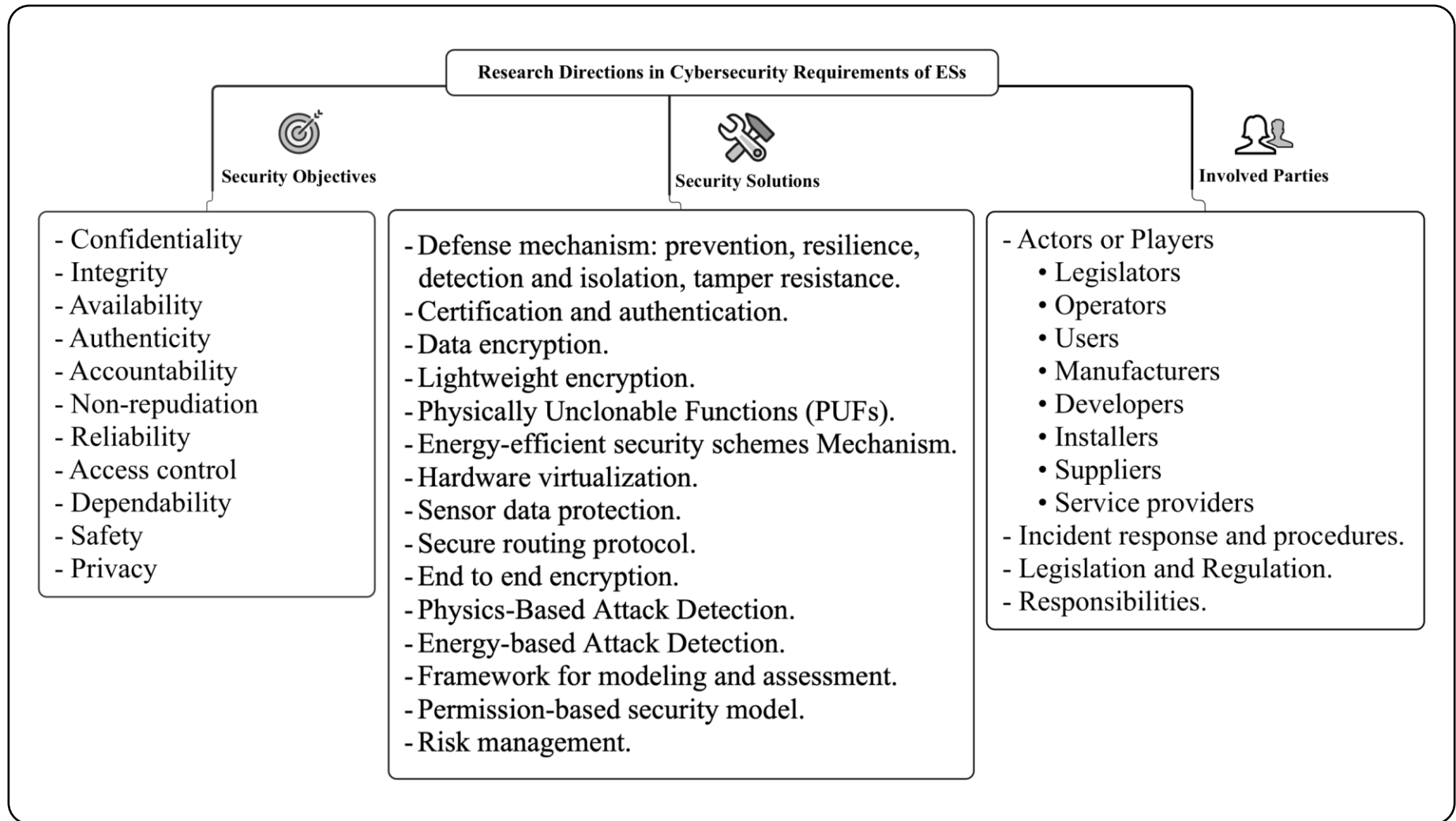


Figure 2-7. Research directions in cybersecurity requirements of ESs

Table 2-4. Research directions in cybersecurity requirements of ESs.

Research Directions and addressed Aspects	References
<u>Security Objectives:</u> <ul style="list-style-type: none"> - Confidentiality - Integrity - Availability - Authenticity - Accountability - Non-repudiation - Reliability - Access control - Dependability - Safety - Privacy 	<ul style="list-style-type: none"> [19] [67] [18] [68] [19] [67] [68] [19] [67] [68] [19] [67] [68] [67] [68] [67] [68] [67] [68] [67] [68] [68] [68] [68]
<u>Security Solutions:</u> <ul style="list-style-type: none"> - Defense mechanism: prevention, resilience, detection and isolation, tamper resistance. - Certification and authentication. - Data encryption. - Lightweight encryption. - Physically Unclonable Functions (PUFs). - Energy-efficient security schemes Mechanism. - Hardware virtualization. - Sensor data protection. - Secure routing protocol. - End to end encryption. - Physics-Based Attack Detection. - Energy-based Attack Detection. - Framework for modelling and assessment - Permission-based security model - Risk management and incident response 	<ul style="list-style-type: none"> [71][103] [72] [104] [105] [72] [106] [39] [72] [107] [25] [72] [98] [99] [110] [111] [83] [112] [72] [107] [72] [106] [72] [113] [114] [77] [78] [103] [77] [78] [110] [54] [73] [96] [93] [95] [96]
<u>Involved Parties:</u> <ul style="list-style-type: none"> - legislations and responsibilities - Actors: users, operators, developer, etc. 	<ul style="list-style-type: none"> [54] [73] [96] [97] [98] [99] [100] [102] [115]

2.6. Conclusion

In this chapter, we conducted an analytical review in the field of cybersecurity for embedded systems in order to identify the deficiencies or gaps that need further research to improve the cybersecurity of ESs. The lack of compatible security solutions in line with the capabilities of embedded systems has provided the opportunities for attackers to find exploitable vulnerabilities and carry out various attacks. This is because the security of embedded systems is limited by their resource constraints, rather than the absence of advanced security solutions. Unfortunately, most of the advanced security solutions require a lot of computational resources and high-power consumption, so there is an urgent need to find effective and efficient solutions that do not drain the resources of the system.

2.7. References:

1. He H., Maple C., Watson T., Tiwari A., Mehnen J., Jin Y., et al. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing other computational intelligence BT - 2016 IEEE Congress on Evolutionary Computation, CEC 2016, July 24, 2016 - July 29, 2016. IEEE Internet of Things Journal. 2016; : 1015–1021. Available at: DOI:10.1109/CEC.2016.7743900
2. Levy E. Crossover: online pests plaguing the off line world. IEEE Security & Privacy. November 2003; 1(6): 71–73. Available at: DOI:10.1109/MSECP.2003.1253573
3. M. Patrick. How MCUs Actually Fight Security Attacks on Embedded Systems, New Electronics, the site for electronic design engineers. Available at: <http://www.newelectronics.co.uk/electronics-technology/how-mcus-actually-fight-security-attacks-on-embedded-systems/176924/> (Accessed: 2 November 2019)
4. Ali S., Al Balushi T., Nadir Z., Hussain OK. ICS/SCADA system security for CPS. Studies in Computational Intelligence. 2018. 89–113 p. Available at: DOI:10.1007/978-3-319-75880-0_5 (Accessed: 15 August 2019)
5. R. M. Lee, M. J. Assante and TC. “German steel mill cyber attack,” ICS Defense Use Case (DUC), SANS Ind. Control Syst. (ICS), Swansea, U.K., Tech. Rep., Dec. 2014. [Online]. 2014. Available at: https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf
6. F. V. and T. Givargis. Embedded System Design: A Unified Hardware/Software Introduction. Hoboken, NJ, USA: Wiley, 2002. John Wiley & Sons; 2002. 352 p. Available at: <http://esd.cs.ucr.edu>
7. Papp D., Ma Z., Buttyan L. Embedded systems security: Threats, vulnerabilities, and attack taxonomy. 2015 13th Annual Conference on Privacy, Security and Trust, PST 2015. IEEE; 2015; : 145–152. Available at: DOI:10.1109/PST.2015.7232966
8. Pham Van P Van., Binh NN. Embedded System Architecture Design and Optimization at the Model Level. International Journal of Computer and Communication Engineering. 2012; 1(4): 345–349. Available at:

- DOI:10.7763/ijcce.2012.v1.87
9. Suzen AA., Duman B., Sen B. Benchmark Analysis of Jetson TX2, Jetson Nano and Raspberry PI using Deep-CNN. 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE; 2020. pp. 1–5. Available at: DOI:10.1109/HORA49412.2020.9152915
 10. Cyber-Physical Systems (CPS) nsf08611. Available at: <https://www.nsf.gov/pubs/2008/nsf08611/nsf08611.htm> (Accessed: 4 September 2019)
 11. Marwedel P., Marwedel P. Embedded System Hardware. Embedded System Design. 2011. pp. 119–175. Available at: DOI:10.1007/978-94-007-0257-8_3 (Accessed: 15 August 2019)
 12. Lee EA. Cyber physical systems: Design challenges. Proceedings - 11th IEEE Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing, ISORC 2008. IEEE; 2008. pp. 363–369. Available at: DOI:10.1109/ISORC.2008.25 (Accessed: 26 August 2019)
 13. Hameed S., Khan FI., Hameed B. Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review. Journal of Computer Networks and Communications. 10 January 2019; 2019: 1–14. Available at: DOI:10.1155/2019/9629381
 14. Cyber-Physical Systems | Digital Single Market. Available at: <https://ec.europa.eu/digital-single-market/en/cyber-physical-systems> (Accessed: 26 August 2019)
 15. Boyes H., Hallaq B., Cunningham J., Watson T. The industrial internet of things (IIoT): An analysis framework. Computers in Industry. Elsevier; October 2018; 101(December 2017): 1–12. Available at: DOI:10.1016/j.compind.2018.04.015 (Accessed: 5 September 2019)
 16. Tay SI., Lee TC., Hamid NZA., Ahmad ANA. An overview of industry 4.0: Definition, components, and government initiatives. Journal of Advanced Research in Dynamical and Control Systems. 2018; 10(14): 1379–1387.
 17. Ntalampiras S. Automatic identification of integrity attacks in cyber-physical systems. Expert Systems with Applications. Elsevier Ltd; 2016; 58: 164–173. Available at: DOI:10.1016/j.eswa.2016.04.006

18. Pasquini A. Computer Safety, Reliability and Security. Berlin, Heidelberg: Springer Berlin Heidelberg; 1999. Available at: DOI:10.1007/3-540-48249-0
19. Ravi S., Kocher P., Lee R., McGraw G., Raghunathan A. Security as a new dimension in embedded system design. Proceedings of the 41st annual conference on Design automation - DAC '04. New York, New York, USA: ACM Press; 2004. p. 753. Available at: DOI:10.1145/996566.996771
20. MESHRAM VH., SASANKAR AB. Security in Embedded Systems: Vulnerabilities , Pigeonholing of Attacks and Countermeasures. IOSR Journal of Computer Engineering. 2016; : 11–15.
21. Bodei C., Chessa S., Galletta L. Measuring security in IoT communications. Theoretical Computer Science. Elsevier B.V.; 2019; 764: 100–124. Available at: DOI:10.1016/j.tcs.2018.12.002
22. Parameswaran S., Wolf T. Embedded systems security—an overview. Design Automation for Embedded Systems. 17 September 2008; 12(3): 173–183. Available at: DOI:10.1007/s10617-008-9027-x (Accessed: 27 July 2019)
23. Hwang DD., Schaumont P., Tiri K., Verbauwhede I. Securing embedded systems. IEEE Security & Privacy Magazine. March 2006; 4(2): 40–49. Available at: DOI:10.1109/MSP.2006.51
24. Abomhara M., Køien GM. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility. 2015; 4(1): 65–88. Available at: DOI:10.13052/jcsm2245-1439.414 (Accessed: 27 July 2019)
25. Marwedel P. Embedded System Design. Cham: Springer International Publishing; 2018. Available at: DOI:10.1007/978-3-319-56045-8 (Accessed: 15 August 2019)
26. Chai H., Zhang G., Zhou J., Sun J., Huang L., Wang T. A Short Review of Security-Aware Techniques in Real-Time Embedded Systems. Journal of Circuits, Systems and Computers. 12 February 2019; 28(02): 1930002. Available at: DOI:10.1142/S0218126619300022 (Accessed: 8 September 2019)
27. Wang W., Zhang X., Hao Q., Zhang Z., Xu B., Dong H., et al. Hardware-Enhanced Protection for the Runtime Data Security in Embedded Systems. Electronics. 2 January 2019; 8(1): 52. Available at: DOI:10.3390/electronics8010052 (Accessed: 8 September 2019)

28. Ali S., Al Balushi T., Nadir Z., Hussain OK. Risk Management for CPS Security. springer. Cham: Springer International Publishing; 2018. pp. 11–33. Available at: DOI:10.1007/978-3-319-75880-0_2 (Accessed: 15 August 2019)
29. Loukas G., Karapistoli E., Panaousis E., Sarigiannidis P., Bezemskij A., Vuong T. A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles. *Ad Hoc Networks*. Elsevier B.V.; March 2019; 84: 124–147. Available at: DOI:10.1016/j.adhoc.2018.10.002
30. Habibzadeh H., Nussbaum BH., Anjomshoa F., Kantarci B., Soyata T. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*. Elsevier; October 2019; 50(June): 101660. Available at: DOI:10.1016/j.scs.2019.101660
31. Radoglou Grammatikis PI., Sarigiannidis PG., Moscholios ID. Securing the Internet of Things: Challenges, threats and solutions. *Internet of Things*. Elsevier B.V.; 2018; 5: 41–70. Available at: DOI:10.1016/j.iot.2018.11.003
32. Riahi Sfar A., Natalizio E., Challal Y., Chtourou Z. A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*. Elsevier Ltd; 2018; 4(2): 118–137. Available at: DOI:10.1016/j.dcan.2017.04.003
33. Humayed A., Lin J., Li F., Luo B. Cyber-Physical Systems Security - A Survey. *IEEE Internet of Things Journal*. 2017; 4(6): 1802–1831. Available at: DOI:10.1109/JIOT.2017.2703172
34. Liu X., Zhao M., Li S., Zhang F., Trappe W. A Security Framework for the Internet of Things in the Future Internet Architecture. *Future Internet*. 28 June 2017; 9(3): 27. Available at: DOI:10.3390/fi9030027 (Accessed: 27 July 2019)
35. Koopman P. Embedded system security. *Computer*. July 2004; 37(7): 95–97. Available at: DOI:10.1109/MC.2004.52
36. O’Flynn C., Chen Z. ChipWhisperer: An Open-Source Platform for Hardware Embedded Security Research. 2014. pp. 243–260. Available at: DOI:10.1007/978-3-319-10175-0_17
37. Yampolskiy M., Horvath P., Koutsoukos XD., Xue Y., Sztipanovits J. Taxonomy for description of cross-domain attacks on CPS. *HiCoNS 2013 - Proceedings of the 2nd ACM International Conference on High Confidence Networked Systems, Part of CPSWeek 2013*. New York, New York, USA: ACM Press; 2013; : 135.

- Available at: DOI:10.1145/2461446.2461465 (Accessed: 17 August 2019)
38. Khelladi L., Challal Y., Bouabdallah A., Badache N. On security issues in embedded systems: challenges and solutions. *International Journal of Information and Computer Security*. 2008; 2(2): 140. Available at: DOI:10.1504/ijics.2008.018515
 39. Bansod G., Raval N., Pisharoty N. Implementation of a new lightweight encryption design for embedded security. *IEEE Transactions on Information Forensics and Security*. IEEE; 2015; 10(1): 142–151. Available at: DOI:10.1109/TIFS.2014.2365734
 40. Liu Y., Peng Y., Wang B., Yao S., Liu Z. Review on cyber-physical systems. *IEEE/CAA Journal of Automatica Sinica*. January 2017; 4(1): 27–40. Available at: DOI:10.1109/JAS.2017.7510349 (Accessed: 27 July 2019)
 41. Kizza JM. *Computer and Network Forensics. A Guide to Computer Network Security*. London: Springer London; 2009. pp. 299–328. Available at: DOI:10.1007/978-1-84800-917-2_14 (Accessed: 25 August 2019)
 42. Bertino E., Martino L., Paci F., Squicciarini A., Bertino E., Martino LD., et al. *Web Services Threats, Vulnerabilities, and Countermeasures. Security for Web Services and Service-Oriented Architectures*. Berlin, Heidelberg: Springer Berlin Heidelberg; 2009. pp. 25–44. Available at: DOI:10.1007/978-3-540-87742-4_3 (Accessed: 25 August 2019)
 43. Brauch HG. *Concepts of Security Threats, Challenges, Vulnerabilities and Risks*. 2011. pp. 61–106. Available at: DOI:10.1007/978-3-642-17776-7_2 (Accessed: 25 August 2019)
 44. Dahbur K., Mohammad B., Tarakji AB. A survey of risks, threats and vulnerabilities in cloud computing. *ACM International Conference Proceeding Series*. New York, New York, USA: ACM Press; 2011. pp. 1–6. Available at: DOI:10.1145/1980822.1980834 (Accessed: 25 August 2019)
 45. Yan A. *Introduction to Information Sys - R. Kelly Rainer (1)*. Available at: https://www.academia.edu/28734440/Introduction_to_Information_Sys_-_R_Kelly_Rainer_1 (Accessed: 25 August 2019)
 46. Li F., Lai A., Ddl D. Evidence of Advanced Persistent Threat: A case study of malware for political espionage. 2011 6th International Conference on Malicious

- and Unwanted Software. IEEE; 2011. pp. 102–109. Available at: DOI:10.1109/MALWARE.2011.6112333
47. Ansari S., Rajeev SG., Chandrashekar HS. Packet sniffing: a brief introduction. IEEE Potentials. December 2002; 21(5): 17–19. Available at: DOI:10.1109/MP.2002.1166620
48. De Vivo M., Carrasco E., Isern G., De Vivo GO. A review of port scanning techniques. Computer Communication Review. ACM; 1999. pp. 41–48. Available at: DOI:10.1145/505733.505737 (Accessed: 25 August 2019)
49. Iguere VM., Laughter SA., Williams RD. Security issues in SCADA networks. Computers & Security. October 2006; 25(7): 498–506. Available at: DOI:10.1016/j.cose.2006.03.001 (Accessed: 26 August 2019)
50. Nicholson A., Webber S., Dyer S., Patel T., Janicke H. SCADA security in the light of cyber-warfare. Computers and Security. Elsevier Advanced Technology; 1 June 2012; 31(4): 418–436. Available at: DOI:10.1016/j.cose.2012.02.009 (Accessed: 26 August 2019)
51. Wilson C. Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. 2008. Available at: <https://apps.dtic.mil/docs/citations/ADA477642> (Accessed: 26 August 2019)
52. Naumann I., Hogben G. Privacy features of European eID card specifications. Network Security. Elsevier Advanced Technology; 1 August 2008; 2008(8): 9–13. Available at: DOI:10.1016/S1353-4858(08)70097-7 (Accessed: 26 August 2019)
53. Fitz T., Theiler M., Smarsly K. A metamodel for cyber-physical systems. Advanced Engineering Informatics. Elsevier; August 2019; 41(December 2018): 100930. Available at: DOI:10.1016/j.aei.2019.100930
54. NIST. National Institute of Standards and Technology (NIST) Cybersecurity Risk Management Framework Applied to Modern Vehicles. NIST. 2014. Available at: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812073_natlinstitstandardstechcyber.pdf
55. NIST. nist.gov. Available at: <https://www.nist.gov/> (Accessed: 16 October 2019)
56. Pallett DS. National Institute of Standards and Technology (NIST). Proceedings of the workshop on Speech and Natural Language - HLT '89. Morristown, NJ, USA: Association for Computational Linguistics; 1989. p. 191. Available at:

- DOI:10.3115/100964.1138540 (Accessed: 26 August 2019)
57. Draft IP. NIST Guide to Supervisory and Data Acquisition-SCADA and Industrial Control Systems Security (2007).pdf (application/pdf Object). Available at: [http://www.cyber.st.dhs.gov/docs/NIST Guide to Supervisory and Data Acquisition-SCADA and Industrial Control Systems Security \(2007\).pdf](http://www.cyber.st.dhs.gov/docs/NIST_Guide_to_Supervisory_and_Data_Acquisition-SCADA_and_Industrial_Control_Systems_Security_(2007).pdf)
 58. Chew E., Swanson M., Stine K., Bartol N., Brown A., Robinson W. Performance Measurement Guide for Information Security. 2008. Available at: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf>
 59. NIST. NIST Special Publication 800-181: National initiative for cybersecurity education (NICE) cybersecurity workforce framework. 2017; : 144. Available at: DOI:10.6028/NIST.SP.800-181
 60. Williams MG. A Risk Assessment on Raspberry PI using NIST Standards. International Journal of Computer Science and Network Security. 2015; 15(6): 22–30.
 61. Potteiger B., Emfinger W., Neema H., Koutosukos X., Tang CY., Stouffer K. Evaluating the effects of cyber-attacks on cyber physical systems using a hardware-in-the-loop simulation testbed. Proceedings - 2017 Resilience Week, RWS 2017. 2017; : 177–183. Available at: DOI:10.1109/RWEEK.2017.8088669
 62. Pieters W. Defining ‘the weakest link’: Comparative security in complex systems of systems. Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom. IEEE; 2013; 2: 39–44. Available at: DOI:10.1109/CloudCom.2013.101
 63. Georgiou K., Xavier-De-Souza S., Eder K. The IoT Energy Challenge: A Software Perspective. IEEE Embedded Systems Letters. 2018. pp. 53–56. Available at: DOI:10.1109/LES.2017.2741419 (Accessed: 12 August 2019)
 64. Ambrose JA., Ragel RG., Jayasinghe D., Li T., Parameswaran S. Side channel attacks in embedded systems: A tale of hostilities and deterrence. Proceedings - International Symposium on Quality Electronic Design, ISQED. IEEE; 2015; 2015-April: 452–459. Available at: DOI:10.1109/ISQED.2015.7085468
 65. Bhunia S., Tehranipoor M. Chapter 1 - Introduction to Hardware Security. In: Bhunia S, Tehranipoor M (eds.) Hardware Security. Morgan Kaufmann; 2019. pp. 1–20. Available at: DOI:<https://doi.org/10.1016/B978-0-12-812477-2.00006-X>

-
66. Kizza JM. Understanding Computer Network Security. 2013. pp. 43–59. Available at: DOI:10.1007/978-1-4471-4543-1_2
 67. Alguliyev R., Imamverdiyev Y., Sukhostat L. Cyber-physical systems and their security issues. *Computers in Industry*. Elsevier; 2018; 100(July 2017): 212–223. Available at: DOI:10.1016/j.compind.2018.04.017 (Accessed: 27 July 2019)
 68. Serpanos DN., Voyiatzis AG. Security challenges in embedded systems. *ACM Transactions on Embedded Computing Systems*. ACM; 29 March 2013; 12(1s): 1–10. Available at: DOI:10.1145/2435227.2435262 (Accessed: 14 August 2019)
 69. ISO. ISO/IEC 27001:2013. ISO. 2013. Available at: <https://www.iso.org/standard/54534.html> (Accessed: 9 November 2019)
 70. Hsu I., Chen CY., Lin S., Yu TJ., Cho NJ., Hsieh MC. 7Nm Chip-Package Interaction Study on a Fine Pitch Flip Chip Package With Laser Assisted Bonding and Mass Reflow Technology. *Proceedings - Electronic Components and Technology Conference*. IEEE; 2019; 2019-May: 289–293. Available at: DOI:10.1109/ECTC.2019.00050
 71. Dibaji SM., Pirani M., Flamholz DB., Annaswamy AM., Johansson KH., Chakraborty A. A systems and control perspective of CPS security. *Annual Reviews in Control*. Elsevier Ltd; 2019; 47: 394–411. Available at: DOI:10.1016/j.arcontrol.2019.04.011 (Accessed: 27 July 2019)
 72. Ashibani Y., Mahmoud QH. Cyber physical systems security: Analysis, challenges and solutions. *Computers and Security*. Elsevier Ltd; July 2017; 68: 81–97. Available at: DOI:10.1016/j.cose.2017.04.005 (Accessed: 27 July 2019)
 73. Poongothai T., Duraiswamy K. Intrusion detection in mobile AdHoc networks using machine learning approach. *2014 International Conference on Information Communication and Embedded Systems, ICICES 2014*. IEEE; 2015; (978): 1–5. Available at: DOI:10.1109/ICICES.2014.7033949
 74. Hahn A., Ashok A., Sridhar S., Govindarasu M. Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *IEEE Transactions on Smart Grid*. 2013; 4(2): 847–855. Available at: DOI:10.1109/TSG.2012.2226919
 75. Trawczynski D., Zalewski J., Sosnowski J. Design of Reactive Security Mechanisms in Time-Triggered Embedded Systems. *SAE International Journal of Passenger Cars - Electronic and Electrical Systems*. 1 April 2014; 7(2): 527–535.

- Available at: DOI:10.4271/2014-01-0341 (Accessed: 9 September 2019)
76. Yousufi RM., Lalwani P., Potdar MB. A network-based intrusion detection and prevention system with multi-mode counteractions. Proceedings of 2017 International Conference on Innovations in Information, Embedded and Communication Systems, ICIIECS 2017. 2018; 2018-Janua: 1–6. Available at: DOI:10.1109/ICIIECS.2017.8276023
 77. Giraldo J., Urbina D., Cardenas A., Valente J., Faisal M., Ruths J., et al. A survey of physics-based attack detection in cyber-physical systems. ACM Computing Surveys Jul 25, 2018 pp. 1–36. Available at: DOI:10.1145/3203245 (Accessed: 27 July 2019)
 78. Eyisi E., Koutsoukos X. Energy-based attack detection in networked control systems. HiCoNS 2014 - Proceedings of the 3rd International Conference on High Confidence Networked Systems (Part of CPS Week). New York, New York, USA: ACM Press; 2014. pp. 115–124. Available at: DOI:10.1145/2566468.2566472 (Accessed: 15 August 2019)
 79. Gu Z., Han G., Zeng H., Zhao Q. Security-Aware Mapping and Scheduling with Hardware Co-Processors for FlexRay-Based Distributed Embedded Systems. IEEE Transactions on Parallel and Distributed Systems. 1 October 2016; 27(10): 3044–3057. Available at: DOI:10.1109/TPDS.2016.2520949 (Accessed: 8 September 2019)
 80. Zhang JL., Wang WZ., Wang XW., Xia ZH. Enhancing Security of FPGA-Based Embedded Systems with Combinational Logic Binding. Journal of Computer Science and Technology. 13 March 2017; 32(2): 329–339. Available at: DOI:10.1007/s11390-017-1700-8 (Accessed: 8 September 2019)
 81. Negi V., Verma H., Singh I., Vikram A., Malik K., Singh A., et al. Network security in embedded system using TLS. International Journal of Security and its Applications. 28 February 2016; 10(2): 375–384. Available at: DOI:10.14257/ijisia.2016.10.2.33 (Accessed: 8 September 2019)
 82. Manifavas C., Fysarakis K., Papanikolaou A., Papaefstathiou I. Embedded Systems Security: A Survey of EU Research Efforts. Security and Communication Networks. 25 July 2015; 8(11): 2016–2036. Available at: DOI:10.1002/sec.1151 (Accessed: 27 July 2019)

-
83. Lukacs S., Lutas A V., Lutas DH., Sebestyen G. Hardware virtualization based security solution for embedded systems. *Proceedings of 2014 IEEE International Conference on Automation, Quality and Testing, Robotics, AQTR 2014*. IEEE; 2014; : 1–6. Available at: DOI:10.1109/AQTR.2014.6857879
 84. Elmiligi H., Gebali F., El-Kharashi MW. Multi-dimensional analysis of embedded systems security. *Microprocessors and Microsystems*. Elsevier B.V.; March 2016; 41: 29–36. Available at: DOI:10.1016/j.micpro.2015.12.005 (Accessed: 27 July 2019)
 85. Read H., Sutherland I., Xynos K., Roarson F. Locking Out the Investigator: The Need to Circumvent Security in Embedded Systems. *Information Security Journal*. Taylor & Francis; 25 July 2015; 24(1–3): 39–47. Available at: DOI:10.1080/19393555.2014.998847 (Accessed: 27 July 2019)
 86. Moreno C., Fischmeister S. Non-intrusive runtime monitoring through power consumption to enforce safety and security properties in embedded systems. *Formal Methods in System Design*. 19 August 2018; 53(1): 113–137. Available at: DOI:10.1007/s10703-017-0298-3 (Accessed: 8 September 2019)
 87. Garitano I., Fayyad S., Noll J. Multi-Metrics Approach for Security, Privacy and Dependability in Embedded Systems. *Wireless Personal Communications*. 13 April 2015; 81(4): 1359–1376. Available at: DOI:10.1007/s11277-015-2478-z (Accessed: 8 September 2019)
 88. Ma B., Mu D., Mao B., Hu W. A bottom-up approach to verifiable embedded system information flow security. *IET Information Security*. 1 January 2014; 8(1): 12–17. Available at: DOI:10.1049/iet-ifs.2012.0342 (Accessed: 13 August 2019)
 89. Shian L. Design and Development of a Security Kernel in an Embedded System. *International Journal of Control and Automation*. 30 November 2014; 7(11): 49–58. Available at: DOI:10.14257/ijca.2014.7.11.06 (Accessed: 9 September 2019)
 90. Vasilevskaya M., Gunawan LA., Nadjm-Tehrani S., Herrmann P. Integrating security mechanisms into embedded systems by domain-specific modelling. *Security and Communication Networks*. December 2014; 7(12): 2815–2832. Available at: DOI:10.1002/sec.819 (Accessed: 13 August 2019)
 91. Thayer E. Adversarial Testing to Increase the Overall Security of Embedded Systems: A Review of the Process. *IEEE Control Systems*. 2017. pp. 104–108.

- Available at: DOI:10.1109/MCS.2016.2643258 (Accessed: 27 July 2019)
92. Hasler J., Shah S. Security implications for ultra-low power configurable SoC FPAA embedded systems. *Journal of Low Power Electronics and Applications*. 5 June 2018; 8(2): 17. Available at: DOI:10.3390/jlpea8020017 (Accessed: 8 September 2019)
 93. Mahmoodi Y., Reiter S., Viehl A., Bringmann O., Rosenstiel W. Attack surface modeling and assessment for penetration testing of IoT system designs. *Proceedings - 21st Euromicro Conference on Digital System Design, DSD 2018*. IEEE; 2018; : 177–181. Available at: DOI:10.1109/DSD.2018.00043
 94. Checkoway S., Mccoy D., Kantor B., Anderson D., Shacham H., Savage S., et al. Automotive attack surfaces. *USENIX Security*. 2011; Available at: DOI:10.1109/TITS.2014.2342271
 95. Bartel A., Klein J., Le Traon Y., Monperrus M. Automatically securing permission-based software by reducing the attack surface: An application to android. *2012 27th IEEE/ACM International Conference on Automated Software Engineering, ASE 2012 - Proceedings*. 2012; : 274–277. Available at: DOI:10.1145/2351676.2351722
 96. Wilbanks L. Whats Your IT Risk Approach? *IT Professional*. 2018; 20(4): 13–17. Available at: DOI:10.1109/MITP.2018.043141663
 97. Cichonski P., Millar T., Grance T., Scarfone K. *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology*. NIST Special Publication. Gaithersburg, MD; August 2012. Available at: DOI:10.6028/NIST.SP.800-61r2
 98. Creasy J. *Cyber Security Incident Response Guide*. Crest. 2013. Available at: <http://www.crest-approved.org/wp-content/uploads/CSIR-Procurement-Guide.pdf>
 99. Dorofee A., Ruefle R., Zajicek M., McIntire D., Alberts C., Carly SP., et al. *Incident Management Capability Assessment*. 2018. Available at: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2018_005_001_538866.pdf
 100. Sultana S., Midi D., Bertino E. Kinesis: A security incident response and prevention system for wireless sensor networks. *SenSys 2014 - Proceedings of the*

- 12th ACM Conference on Embedded Networked Sensor Systems. 2014; : 148–162. Available at: DOI:10.1145/2668332.2668351
101. <https://www.crest-approved.org/index.html>. crest-org. Available at: <https://www.crest-approved.org/index.html> (Accessed: 16 October 2019)
 102. Division C. CERT Division. Available at: <https://www.sei.cmu.edu/about/divisions/cert/> (Accessed: 16 October 2019)
 103. Ravi S., Raghunathan A., Chakradhar S. Tamper resistance mechanisms for secure embedded systems. Proceedings of the IEEE International Conference on VLSI Design. IEEE; 2004; 17: 605–611. Available at: DOI:10.1109/icvd.2004.1260985
 104. Gupta P., Ravi S., Raghunathan A., Jha NK. Efficient Fingerprint-based User Authentication for Embedded Systems. 2005; : 244–247.
 105. Švéda M., Opluštil V. Experience with integration and certification of COTS based embedded system into advanced avionics system. 2007 Symposium on Industrial Embedded Systems Proceedings, SIES'2007. 2007; : 282–287. Available at: DOI:10.1109/SIES.2007.4297346
 106. Ukil A., Sen J., Koilakonda S. Embedded security for internet of things. Proceedings - 2011 2nd National Conference on Emerging Trends and Applications in Computer Science, NCETACS-2011. IEEE; 2011; : 50–55. Available at: DOI:10.1109/NCETACS.2011.5751382
 107. Wyglinski AM., Huang X., Padir T., Lai L., Eisenbarth TR., Venkatasubramanian K. Security of autonomous systems employing embedded computing and sensors. IEEE Micro. 2013; 33(1): 80–86. Available at: DOI:10.1109/MM.2013.18
 108. Al-Haidary M., Nasir Q. Physically Unclonable Functions (PUFs): A Systematic Literature Review. 2019 Advances in Science and Engineering Technology International Conferences, ASET 2019. IEEE; 2019; (December): 1–6. Available at: DOI:10.1109/ICASET.2019.8714431
 109. Alimohammadi N., Shokouhi SB. Secure hardware key based on Physically Unclonable Functions and artificial Neural Network. 2016 8th International Symposium on Telecommunications, IST 2016. IEEE; 2017; : 756–760. Available at: DOI:10.1109/ISTEL.2016.7881924
 110. Nimgaonkar S., Gomathisankaran M., Mohanty SP. TSV: A novel energy efficient memory integrity verification scheme for embedded systems. Journal of Systems

- Architecture. Elsevier B.V.; 2013; 59(7): 400–411. Available at: DOI:10.1016/j.sysarc.2013.04.008
111. Venčkauskas A., Jusas N., Kazanavičius E., Štuikys V. An energy efficient protocol for the internet of things. *Journal of Electrical Engineering*. 2015; 66(1): 47–52. Available at: DOI:10.1515/jee-2015-0007
 112. Xu D. Virtualization and security. *Proceedings of the 4th ACM conference on Data and application security and privacy - CODASPY '14*. New York, New York, USA: ACM Press; 2014. pp. 73–74. Available at: DOI:10.1145/2557547.2557590
 113. Jha D., Shahi B. A proposed methodology for end to end encryption for communicating embedded systems. *Proceedings of 2017 International Conference on Innovations in Information, Embedded and Communication Systems, ICIIECS 2017*. 2018; 2018-Janua: 1–3. Available at: DOI:10.1109/ICIIECS.2017.8275910
 114. Chatterjee R., Chakraborty R., Mandal JK. Design of cryptographic model for end-to-end encryption in FPGA based systems. *Proceedings of the 3rd International Conference on Computing Methodologies and Communication, ICCMC 2019*. IEEE; 2019; (Iccmc): 459–465. Available at: DOI:10.1109/ICCMC.2019.8819761
 115. Cheng Y., Deng J., Li J., Deloach SA., Singhal A., Ou X. Metrics of security. *Advances in Information Security*. 2014; 62: 263–295. Available at: DOI:10.1007/978-3-319-11391-3_13

**CHAPTER 3: ASSESSMENT FRAMEWORK FOR
EMBEDDED SYSTEMS SECURITY: A MULTIPLE LAYERS
FEEDBACK FRAMEWORK OF EMBEDDED SYSTEM
CYBERSECURITY (MULFESC)**

CHAPTER 3: ASSESSMENT FRAMEWORK FOR EMBEDDED SYSTEMS SECURITY: A MULTIPLE LAYERS FEEDBACK FRAMEWORK OF EMBEDDED SYSTEM CYBERSECURITY (MuLFESC)

Aloseel Abdulmohsan¹, Hongmei He (Senior Member, IEEE)¹, Carl Shaw², Muhammad Ali Khan¹

¹School of Aerospace, Transport and Manufacturing (SATM), Cranfield University

²Cerberus Security Laboratories Ltd, UK

3.1. Abstract

In this chapter, twelve factors influencing CSES have been identified: (1) the components; (2) the characteristics; (3) the implementation; (4) the technical domain; (5) the security requirements; (6) the security problems; (7) the connectivity protocols; (8) the attack surfaces; (9) the impact of the cyber-attacks; (10) the security challenges of the ESs; (11) the security solutions; and (12) the players (manufacturers, legislators, operators, and users). A Multiple Layers Feedback Framework of Embedded System Cybersecurity (MuLFESC) with nine layers of protection is proposed, with new metrics of risk assessment. This will enable cybersecurity practitioners to conduct an assessment of their systems with regard to twelve identified cybersecurity aspects. In MuLFESC, the feedback from the system-components layer to the system-operations layer could help implement “Security by Design” in the design stage at the bottom layer. The study provides a clear landscape of CSES and, therefore, could help to find better comprehensive solutions for CSES.

3.2. Introduction

In the continuous pursuit of humankind to improve quality of life, techniques, and knowledge to meet the aspirations and needs of people, one of the most revolutionary aspects appeared in the field of technology when inventors tried to integrate computing operations into physical systems to enable predefined functionality so-called “Embedded Systems.” During this evolutionary period, significant advances were made in various fields such as industry, health, aviation and communications. The difference between these systems and traditional computers and servers is that they are, as a subsystem, integrated into a larger physical system to perform a specific, essential function. In

contrast, computers and servers are designed for multiple purposes, of which computational operations for data processing are the main purpose.

3.3. Analytical Results of CSES

In this section, we will present the security risk metrics; we will also identify the influencing factors of CSES to shape the MuLFESC framework, which can be used as an instrument of security assessment for the ESs.

3.3.1. Security Risk Metrics

Based on the analysis of the previous studies in this area, multi-security risk metrics have been created and will be presented in this section as part of the contribution of this research. Cybersecurity risk for a system is the probability of exposure or loss resulting from a cyberattack or data breach on the system. The sensitivity of data, its value, and the benefits attackers would gain from hijacking an asset are all large motivations; however, attackers' abilities are contingent on what has been made inadvertently available to them. More entry points mean more possibilities that a system can be exploited. In other words, if the entry points in the attack surfaces are reduced and the unnecessary services are disabled, the chances that a system is attacked are reduced. Many studies have considered security risks from different perspectives, and based on different criteria. According to NIST [1], [2], [3], security metrics are metrics based on IT security performance goals and objectives designed to assist decision-making and improve performance and accountability by collection and analysis of data against potential risk to take an appropriate countermeasure. Within the security risks metrics model, Figure 3-1, the cyberattacks have been addressed from seven different perspectives, providing the broadest coverage of attack probabilities. Thus, having a comprehensive perception of attack possibilities will lead to having a comprehensive awareness that will be reflected positively in the upcoming Multiple Layers Feedback Framework of Embedded System Cybersecurity, Figure 3-3. Optimal countermeasures can then be taken in each layer, according to the perspective of evaluation.

We define security risks within a metrics of different criteria, based on the security triangle: Confidentiality, Integrity, and Availability (CIA) [4–6], as the backbone of the security risk metrics (CIA terms are explained in Chapter 2). They are what attackers intend to breach

ultimately, regardless of the methods or attack surface. Figure 3-1 depicts the adopted security risk metrics, while (X) refers to a security risk. Based on this risk metrics, a security risk can be addressed from 7 perspectives:

(1) A security risk X should be examined against the proposed Multiple Layers Feedback Framework of Embedded System Cybersecurity (MuLFESC), at the same time considering the twelve influencing factors, as illustrated in Figure 3-2. Figure 3-4 also presents these factors with more details.

(2) Security risk can be assessed based on attack methods. According to [7], methods of attacks can be classified into three different typical methods: (1) physical method, (2) logical or software-based method, and (3) Side-Channel attack method.

- **A physical attack**, whether non-invasive, semi-invasive, or invasive attack means an attacker's ability to access the cyber-physical system directly and this direct physical access is unauthorized and unauthenticated [7]. In this case, it is unpredictable to know what the attacker can do. Also, natural disasters fall within this type of security threat [8],[7]. A fault attack is an example of a physical attack that can be generated to attack an electronic device, and it can be executed by stressing a targeted device beyond its expected operational limits, causing errors [9]. These errors might lead to security failures on the system such as bypassing authentication checks or leaking sensitive information.
- **The logical or software-based methods** are often used to attack networked ESs through the Internet. The attacks are carried out by exploiting vulnerabilities or exposing errors in software [8],[7], whether in the operating system (OS), applications, protocols used for data transfer, or decryption of the encrypted data.
- In **Side-Channel Attacks (SCA)**, an attacker studies the often unexpected, indirect physical effects of security operations. In this type of attack, the attacker monitors and analyses system activities produced by its physical components such as electromagnetic emission, power consumption, timing, and cryptanalysis to gain access to protected data [7]. NIST defines a side-channel attack as follows “An attack enabled by leakage of information from a physical cryptosystem. Characteristics that could be exploited in a side-channel attack include timing, power consumption, and electromagnetic and acoustic emissions” [10]. There are 12 possible attacks based on

this method: (1) acoustic attack, (2) brute force attack, (3) cache-based attack, (4) electromagnetic analysis, (5) error message attack, (6) frequency-based attack, (7) glitch attack, (8) power analysis, (9) timing analysis, (10) safe error attack, (11) scan-based attack, and (12) visible light attack [7].

(3) Security risks can be classified into four different types based on their nature: Vulnerabilities, Exposure, Threat, and Attacks [8] (chapter 2, section 2.4.2).

(4) Attack surface is the sum of all possible security risk exposures. There are three types of attack surfaces [11]:

- **The hardware surface** can be any possible components in a cyber-physical system or an embedded system, such as sensors for receiving or sending signals, USB ports or Input/output units.
- **The software surface**, including the logicity of algorithms and protocols, can be in any levels of OS, firmware, protocol handlers or applications.
- Finally, **the network-components surface**.

As mentioned earlier, a smaller attack surface can help make the system less exploitable, reducing the risk; and a greater attack surface makes the system more vulnerable to attacks, which increases the risk. Cheng et al. [12] verify this security problem through using redundant controller architecture to avoid unpredictable mechanical failures, but unfortunately this technique increases the chance of exploiting the attack surface and lowers the sensitivity to respond to ongoing attacks.

(5) The security risk due to network connectivity can be assessed in terms of the four-layers TCP/IP model: Application layer, transport layer, network layer, and link and physical layer [13]. There could be different attacks in each layer; examples of these attacks were discussed in chapter 2.

(6) The security challenges in terms of the limitations of the embedded system have been discussed by [14], including processing gap, battery gap, independence, flexibility, installation in an uncontrolled or harsh environment, remoteness and unmanned operation, connectivity to the network, the function's nature of the CPS, and cost. The cybersecurity risk often arises from the limited resources in embedded systems.

(7) Taking into account the attacker's capabilities and the value of the assets is essential for the assessment. A skilled attacker with significant resources poses a much higher risk than

a low skilled attacker with few resources. The value of assets, including data, is important. The more sensitive the data, the more security measures are required to ensure its confidentiality, integrity, and availability. While evaluating the efficiency and effectiveness of the applied measures, taking attackers' capabilities and assets' values into account might help improve the adoption of appropriate security. The following figure depicts the suggested security risk metrics.

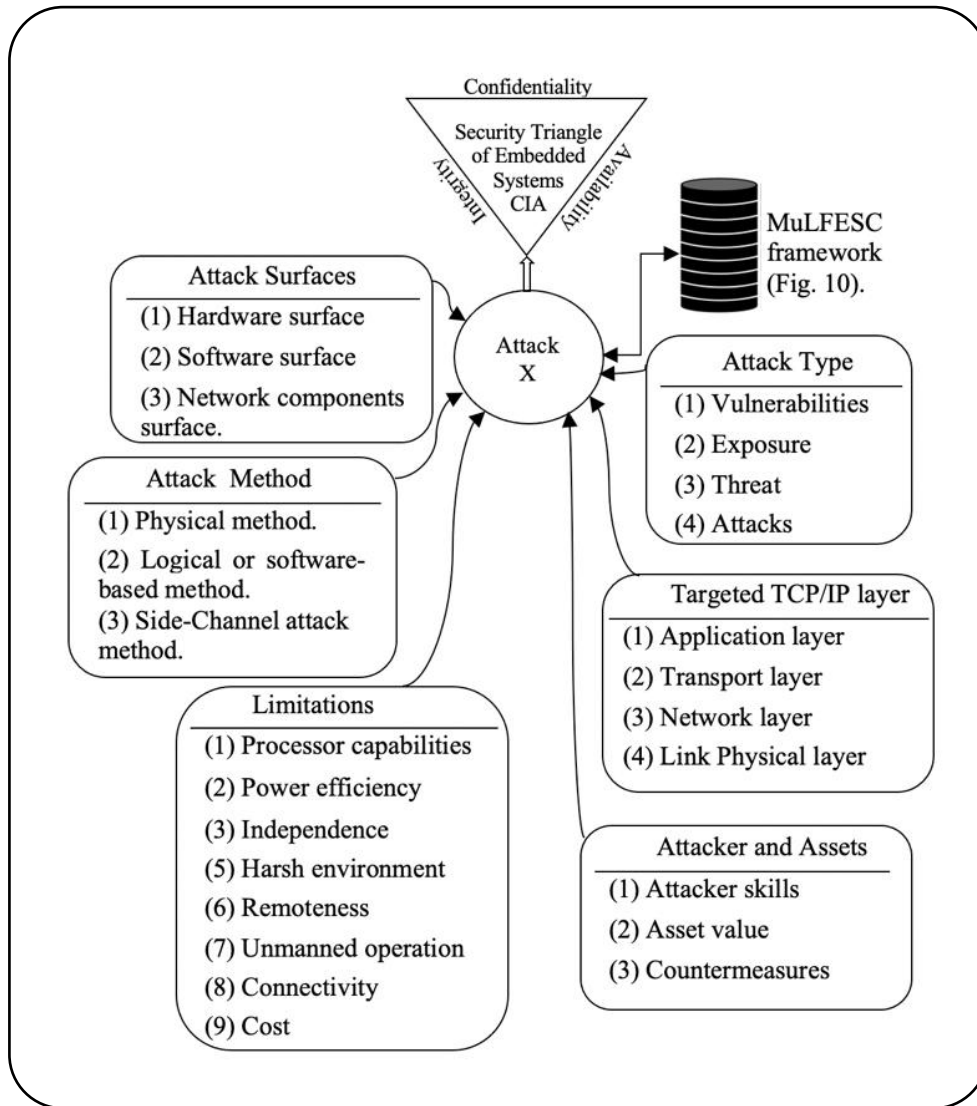


Figure 3-1. Security Risk Metrics.

3.3.2. Key Factors of the MuLFESC Framework

After presenting the multi-security risk metrics, which can predict the largest possible number of cyberattacks in terms of methods, types, surfaces, TCP/IP layer, and limitations

of the ES's resources, this section addresses the key factors that affect the CSES. The determination of the influencing factors could help identify the gaps and weaknesses in the current countermeasures. Figure 3-2 represents these influencing factors that have been extracted from the existing research trends, while Figure 3-3 represents the MuLFESC framework layers with its involved parties and system components affected by these factors. The MuLFESC framework has been shaped by taking into account the following factors:

3.3.2.1. The Architecture of ES in CPS

Weak computing capabilities of ES could limit the ability to implement advanced security solutions regarding the components and architecture of ES in CPS. Failure to consider security requirements at the design stage of ESs could increase the complication of implementing cybersecurity objectives and requirements in a complicated CPS [15], [16], [17], [18], [19].

3.3.2.2. The Characteristics of ES

Features of embedded systems and their flexibility in meeting the requirements of modern technologies earned them excellence over traditional computers. However, these characteristics pose many challenges for the cybersecurity of ESs [20], [1].

3.3.2.3. The Implementations of ES

“Embedding systems” is a broad concept applied to form the computational part of a wide diversity of applications. Therefore, the diversity of ESs reflects positively on its applications [21], [22], [23], and the constraints of ESs’ characteristics and the attack surfaces that can be exploited pose many security challenges. This requires developing market-appropriate security solutions whether in the field of healthcare, communications, military, etc.

3.3.2.4. The Technical Domains of ES

Embedded systems are the core or the basic block of advanced technologies, such as DCS, SCADA, IACS, ICS, Industry 4.0, Industrial, IIoT, IoT, and CPS. The realization of an embedded system with security by design could therefore support the security, stability, and reliability of advanced systems [24], [25]. However, security requirements and

solutions need to be considered in the context of different technical domains. The study and test of the embedded system should be done under the context of its real-world applications; thus, the goals of the applications as well as the performance in efficiency, reliability, and stability can be reached.

3.3.2.5. The Security Objectives of ES

Embedded systems have the same objectives of cybersecurity as traditional computer systems, which include: confidentiality, integrity, availability, authenticity, accountability, non-repudiation, reliability, access control, dependability, safety, and privacy. The security requirements depend on the context of application domains. In contrast, the characteristics of ESs raise the challenges in the implementation of embedded system security to achieve these objectives [4–6].

3.3.2.6. The Diversity of Security Problems in ES

Security risks of embedded systems are raised due to various factors, such as the existence of various attack surfaces in a CPS, the connectivity of the Internet, and human factors. Different application systems may have different security problems. For example, if a CPS is characterized as an autonomous system without human intervention, security problems are more likely referred to the physical security of ESs. If a CPS is characterized as an IoT-enabled system with the function of exchanging data or information with the Internet, a remote attack could threaten the CPS through the Internet. If a CPS is characterized as a system with a moveable power source and low energy utilisation rate, the security problems may affect the sustainability of the energy source and the capacity of providing sufficient energy to meet the requirements of advanced applications. Embedded systems are lightweight and compact. The characteristics of ESs have given the limitations in the implementation of cybersecurity of ESs, which may require increasing the capability of the CPU to perform more complex operations, thus enabling ESs to apply complex encryption, other strong security algorithms, and so on [26–28].

3.3.2.7. Connectivity And TCP/IP Model

The connection of ESs to the Internet enables them to provide services and features that were not available without the connection. However, embedded systems could become

vulnerable to a large number of cyber-attacks remotely [13]. For example, wireless connectivity can lead to the leakage of sensitive data [29].

3.3.2.8. Attack Surface and Channels

The main factors that could cause cyber threats or problems are: the attack surfaces which provide attackers with the entry points; network connection, which provides a way to remotely approach the system; and actors/operators, who provide opportunities to attackers for social engineering. The security problems and the characteristics of the embedded system make the implementation of a secure embedded system challengeable. Attacks are always carried out through one of the components of the targeted embedded system, such as Wi-Fi, Bluetooth, sensors or USB, as an attack surface. An attack could have different attack channels [7], [11]. Attacks on embedded systems can be carried out in different forms and on different attack surfaces and channels. Security vulnerabilities exist at different levels, and security threats come from the exploitation of existing vulnerabilities in a system.

3.3.2.9. Impact of Cyber Attacks

Once an embedded system is attacked, the impact of the cyber-attack could affect the whole targeted system and the systems connected to the targeted system. Therefore, the requirements and solutions of cybersecurity should be considered from the design, implementation to responses, thus, to prevent and mitigate the damage and economic loss due to cyber-attacks. Figures 3-2 and 3-4 illustrate the relationship between the twelve factors with some examples.

Cyberattacks usually aim to damage or breach a security objective, such as confidentiality, integrity, and availability of assets or a combination of these security objectives. For example, when an attacker intends to monitor the traffic of data, violating the confidentiality of the data, the attacker also needs to breach the authentication of the connection; when an attacker gets unauthorized access to the storage of data and tampers with the stored data, this is violating the integrity and confidentiality of the data, and the impact of this attack might be on system resources in the form of increasing energy consumption or draining processor capabilities [30], [31]. A cyber-attack could produce severe consequences, e.g., the damage of all systems connected to the targeted system.

Hence, it is important to consider the impacts and responses to potential cyber incidents, caused by attacks on these levels [32], [33], [34], [35], [25].

3.3.2.10. The Security Challenges of ES

The compromise between maintaining the characteristics of embedded systems and meeting cybersecurity requirements are the challenges of secure ESs [12],[38],[132],[134]. Therefore, there is an urgent need to find comprehensive and advanced security solutions while not draining the resources of the embedded system or conflicting with its properties. These solutions should be implemented, crossing all levels of the ES, as shown in Figure 3-3. In the nine levels of protection, the first level is to implement “security by design,” and the design should consider all cyber threats from level 2 to level 9. In section 3.3.3, we will explain all these levels in more detail.

3.3.2.11. The Security Solutions of ES

To ensure security solutions are effective and comprehensive, they must be compatible with the nature of the system characteristics and must be adaptive at all levels. In general, security solutions can be developed in the form of tools, methods, mechanisms or approaches. The best solution is to implement “Security by Design”, regarding the security crossing all levels.

3.3.2.12. Actors or Players

Manufacturers, suppliers, developers, installers, operators, and legislators play an important role to secure embedded systems. User behaviour and the awareness of social-engineering-based attacks are also important [37,40–44], [45]. As shown in Figures 3-2 and 3-4, the twelve factors are strictly related to each other, and to design a protected CPS in an interconnected domain; it is important to secure ESs, as they are connected to each other and may be linked to the Internet.

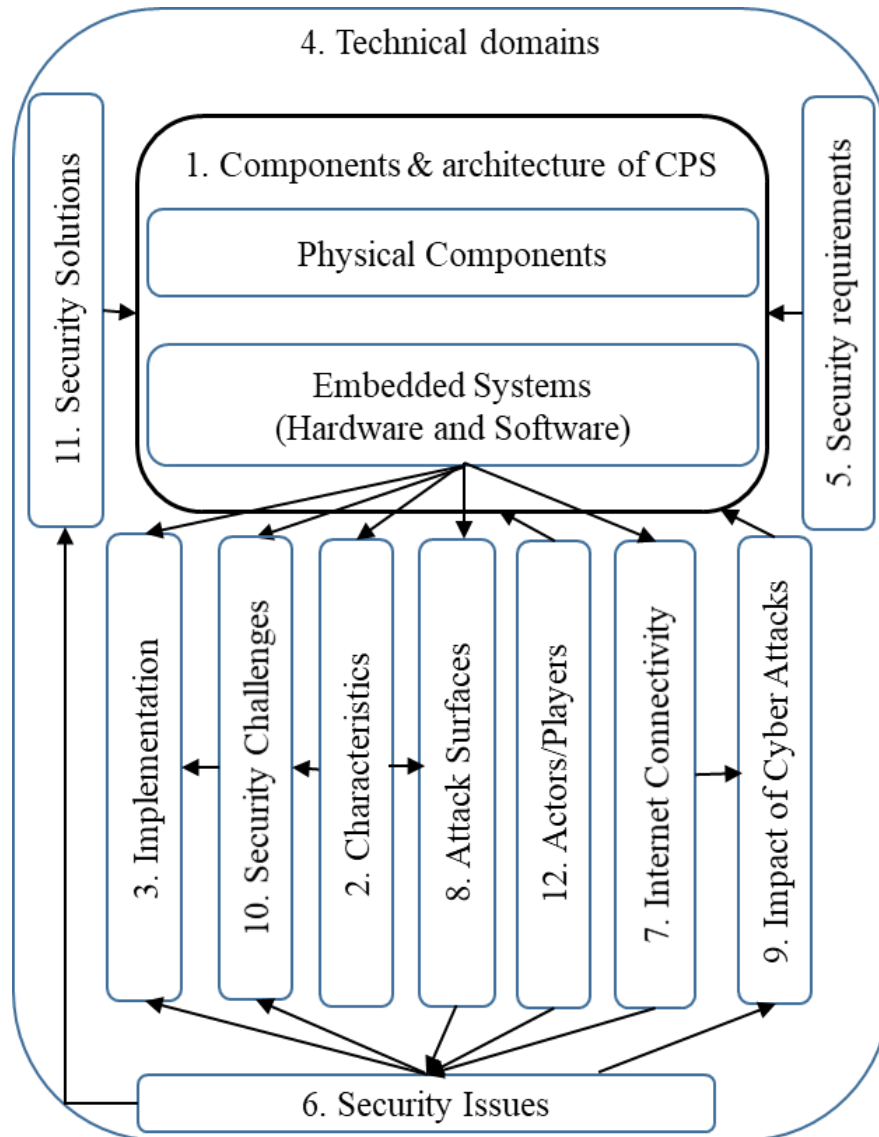


Figure 3-2. The relationship between the twelve factors.

3.3.3. Multiple Layers Feedback Framework of Embedded System Cybersecurity (MuLFESC)

Taking the determined twelve factors into account in conjunction with the MuLFESC layers (Figure 3-3) will lead to building a robust and secure embedded system to the highest standards. The nine layers of exposed risks that need to be protected are depicted in the following figure. The MuLFESC framework consists of nine layers. These layers represent the involved entities and components in the CSES abstractly, and based on the nine layers, we can identify the vulnerabilities and cyber threats in each layer, which can be the inputs for improving the design of the system.

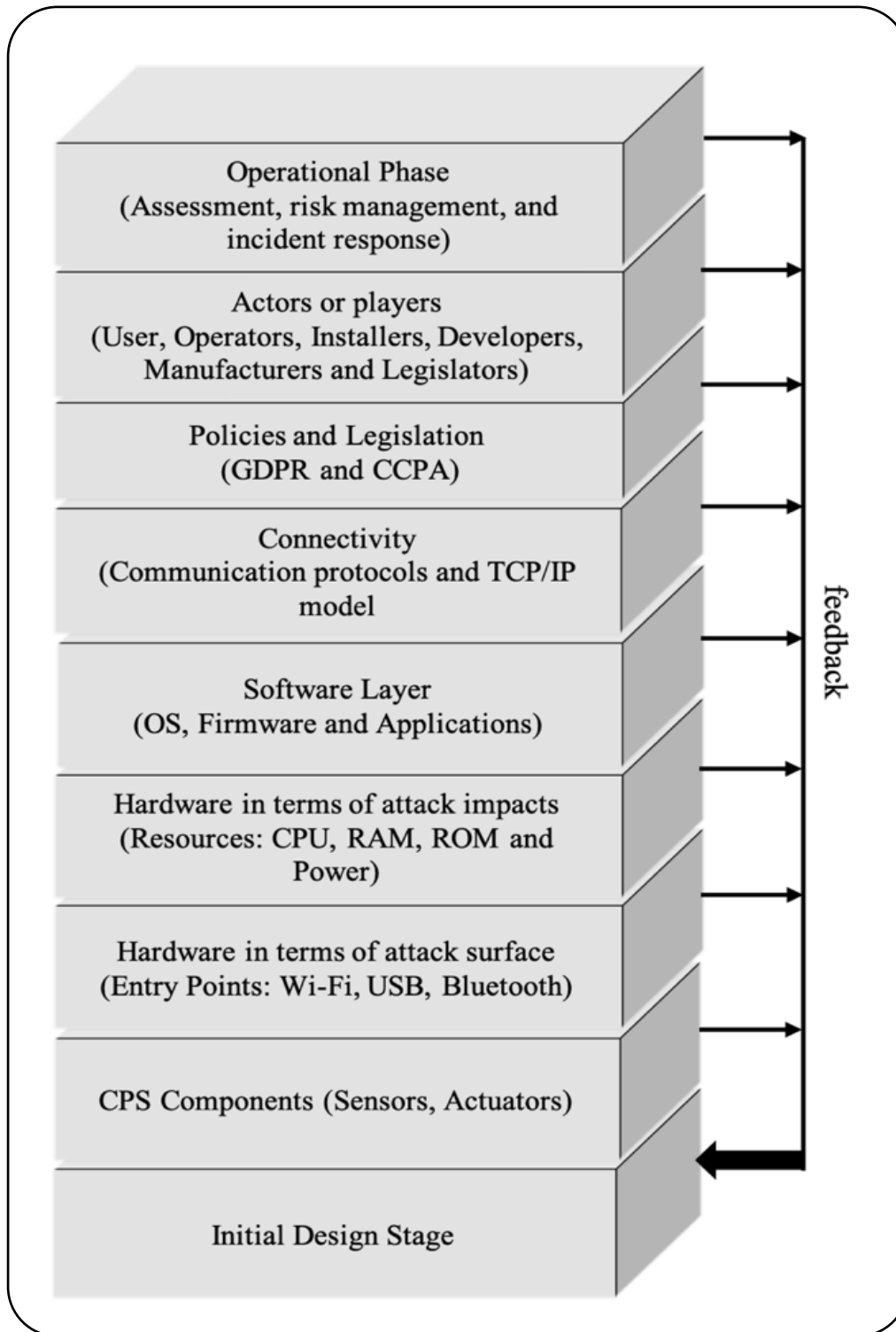


Figure 3-3. The MuLFESC framework.

The first layer is the initial design stage, and this layer is critical: it must be improved iteratively based on the feedback from the other eight layers to implement the “Security by Design” concept. The second layer (CPS) is the most abstract concept of the applications

of ESs in different aspects of life. The third, fourth and fifth layers are the core of the MuLFESC framework and are the components targeted by the attacker. Therefore, better-adapted standards in the other layers will be reflected positively on these three layers. The communication layer with its protocols are the window to the outside world of CPS, and the gateway for remote exploitation. Layers 7 and 8 represent the required role of legislators, operators, users, manufacturers, developers, installers, suppliers, and service providers to set the appropriate policies that guarantee privacy, proper use, and right of access to the parties concerned in a manner that guarantees them the highest safety standards. Finally, the impact of the adopted security countermeasures taken in all layers will be monitored in the operational stage, which is considered as a real test layer of the strength and durability of security measures, and the feedback must be positively reflected onto the first layer from which we set out to improve the security countermeasures.

From the protection perspective, security countermeasures should be integrated at the design stage (Layer 1) and take the properties at different layers of embedded systems into account. The ability to adopt more efficient generic security solutions means the ability to design more robust systems despite the different technical domains. Layer 2 is to secure the physical components of CPS that interact with the outside world, such as sensors and actuators; Layer 3 is to secure the attack surfaces, such as I / O modules, access points such as Wi-Fi, Bluetooth, and USB; Layer 4 is to secure the computation components that might be compromised as a result of the attack such as CPU, memory, and power source; Layer 5 is to secure the software layer, including the operating systems, firmware and applications that should be able to deal with various attacks and handle advanced security solutions; Layer 6 is to secure the Internet connection layer (TCP/IP model) by securing routes and adopting security protocols to ensure a secure transfer of data between a sender and a receiver. Therefore, it is necessary to provide the most secure communication protocols to reduce the capabilities of the attacker and to design ESs with capabilities compatible with the most secure protocols. Layer 7 is to ensure the designed embedded systems are compliant to the legislation and regulations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), thus ensuring the privacy and protection of users' data. Layer 8 is to regard the role of actors and players, including users, operators, manufacturers and legislators, etc.; therefore, their roles must be defined clearly to prevent cyber-attacks. Layer 9, the operational phase, should set up necessary risk

management and assessment. The feedback from Layer 2 to Layer 9 can be used to improve the security design of ESs, and based on the feedback from the operational phase, the developers of CSES can refine the design of the system, thus eliminating cyber risks.

From the security risk perspective, these nine layers are exposed to many risks. The following table summarizes some security risks against each layer of the MuLFESC framework.

Table 3-1. Security risks against MuLFESC layers.

MuLFESC Layers	Related security risks and challenges
Operational layer	Absence of service desk, customer service, customer servers, after-sales services, warranty services, unmonitored and unmaintained system. Absence of network operations center (NOC), and security operations center (SOC), patches delay, absence of feedback-cycle system, and neglected complaints.
Actors or players (Involved parties)	Absence of unified standards, untrained operators and users, social engineering attack awareness, platform incompatibility problems, lack of regular updates.
Policies and legislations	Absence of regulations, policies, and legislation, such as GDPR, CCPA, unsigned responsibilities, undesignated roles, lack of manuals and procedures, and unclear job description.
Connectivity layer	Blackhole attacks, traffic analysis, jamming, device tampering, collision and traffic manipulation, misdirection, flooding, DoS attacks, eavesdropping, spoofing.
Software layer	SQL injection, software tampering, malicious software, remote code execution (RCE) attacks, password attacks, dictionary attacks, brute force attacks.
Hardware layer	Resources exhaustion, side-channel attacks (SCA), differential power analysis (DPA) attacks.
Attack surface	Unprotected entry points, enabling unnecessary ports, features, and services.
CPS components (Sensor, actuators)	Simple electromagnetic analysis (SEMA) attacks, differential electromagnetic analysis (DEMA) attacks, intentional electromagnetic interference (IEMI) attacks, frequency-constrained sensor and actuator attacks, unintended emissions or emanating spurious transmissions attacks.
Design stage	Neglecting security requirements, ignoring security-by-design principles, specs incompatible with purpose of use.

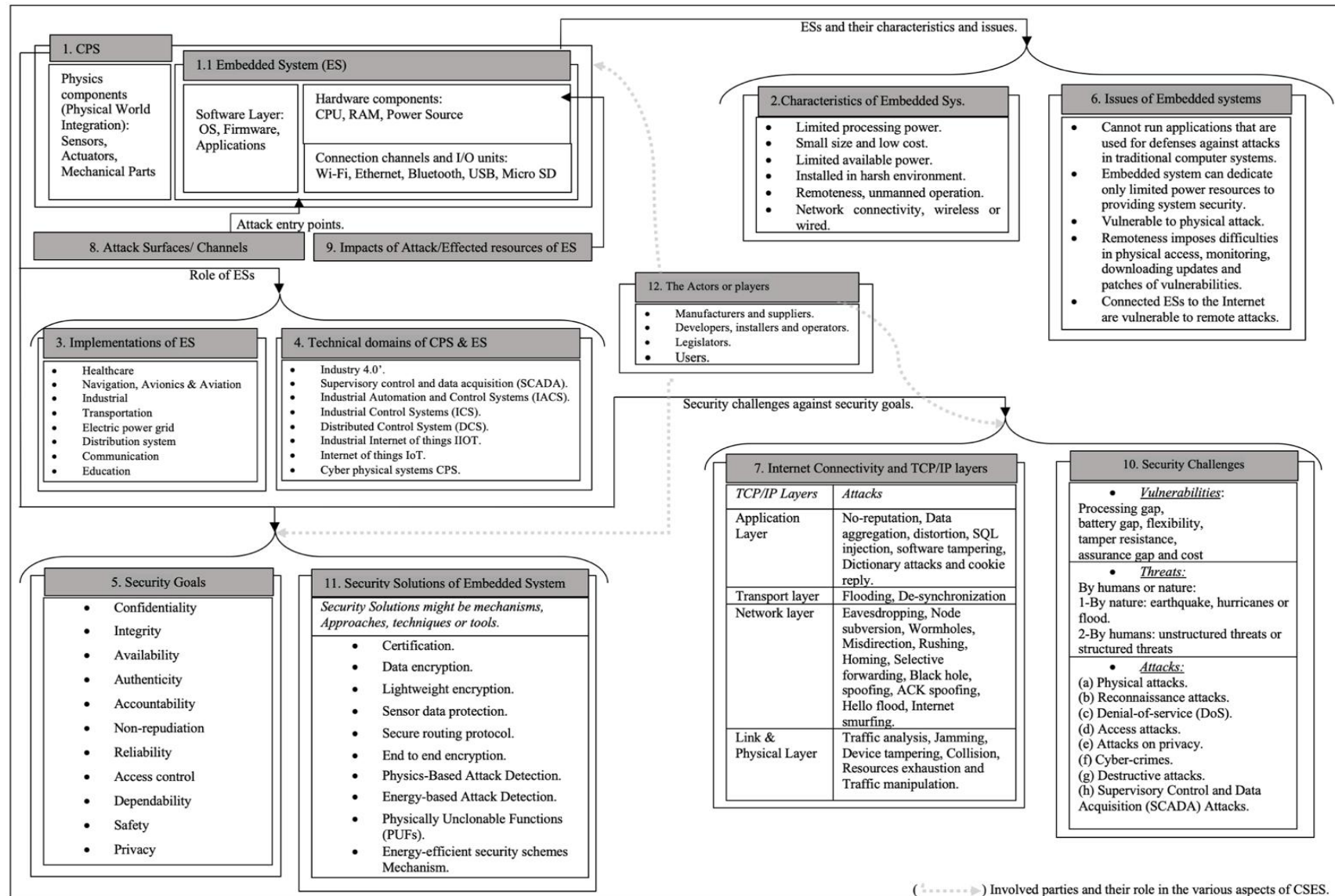


Figure 3-4 . Overall landscape of Cyber Security of Embedded Systems

3.4. Conclusion

Based on the architecture of ESs and the studies carried out in this field, we have identified the most critical factors that play an essential role in the cybersecurity industry for embedded systems. These factors draw the overall landscape of the cybersecurity industry for CSES, and they affect each other directly or indirectly. Also, we have reviewed the research on security risks and assessment methodologies regarding all aspects of cybersecurity of ESs and proposed a new assessment perspective within a metrics of risk assessment linked to MuLFESC. The determined influencing factors have been employed to shape the Multiple Layers Feedback Framework of Embedded System Cybersecurity (MuLFESC) in line with the security risk metrics model. The proposed MuLFESC Framework could contribute to the implementation of comprehensive and effective “Security by Design” solutions by providing feedback to the design stage of CSES.

3.5. References:

1. Pallett DS. National Institute of Standards and Technology (NIST). 1989. p. 191. Available at: DOI:10.3115/100964.1138540 (Accessed: 26 August 2019)
2. Cheng Y., Deng J., Li J., Deloach SA., Singhal A., Ou X. Metrics of security. *Advances in Information Security*. 2014; 62: 263–295. Available at: DOI:10.1007/978-3-319-11391-3_13
3. Educause.edu. <https://www.educause.edu/about>. 2019. Available at: <https://library.educause.edu/topics/cybersecurity/security-metrics> (Accessed: 9 November 2019)
4. Alguliyev R., Imamverdiyev Y., Sukhostat L. Cyber-physical systems and their security issues. *Computers in Industry*. Elsevier; 2018; 100(July 2017): 212–223. Available at: DOI:10.1016/j.compind.2018.04.017 (Accessed: 27 July 2019)
5. Serpanos DN., Voyiatzis AG. Security challenges in embedded systems. *ACM Transactions on Embedded Computing Systems*. ACM; 29 March 2013; 12(1s): 1–10. Available at: DOI:10.1145/2435227.2435262 (Accessed: 14 August 2019)
6. Ravi S., Kocher P., Lee R., McGraw G., Raghunathan A. Security as a new dimension in embedded system design. *Proceedings of the 41st annual conference on Design automation - DAC '04*. New York, New York, USA: ACM Press; 2004. p. 753. Available at: DOI:10.1145/996566.996771
7. Ambrose JA., Ragel RG., Jayasinghe D., Li T., Parameswaran S. Side channel attacks in embedded systems: A tale of hostilities and deterrence. *Proceedings - International Symposium on Quality Electronic Design, ISQED*. IEEE; 2015; 2015-April: 452–459. Available at: DOI:10.1109/ISQED.2015.7085468
8. Abomhara M., Køien GM. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*. 2015; 4(1): 65–88. Available at: DOI:10.13052/jcsm2245-1439.414 (Accessed: 27 July 2019)
9. Biswas S., Chellappa R. *Encyclopedia of Cryptography and Security*. van Tilborg HCA, Jajodia S (eds.) *In the Tree Where the Double Sex Sleeps*. Boston, MA: Springer US; 2011. 38–38 p. Available at: DOI:10.1007/978-1-4419-5906-5
10. NIST. nist.gov. Available at: <https://www.nist.gov/> (Accessed: 16 October 2019)
11. Bhunia S., Tehranipoor M. Chapter 1 - Introduction to Hardware Security. In: Bhunia S, Tehranipoor M (eds.) *Hardware Security*. Morgan Kaufmann; 2019. pp. 1–20.

Available at: DOI:<https://doi.org/10.1016/B978-0-12-812477-2.00006-X>

12. Ma R., Cheng P., Zhang Z., Liu W., Wang Q., Wei Q. Stealthy Attack against Redundant Controller Architecture of Industrial Cyber-Physical System. *IEEE Internet of Things Journal*. IEEE; 2019; PP: 1–1. Available at: DOI:10.1109/jiot.2019.2931349
13. Ali S., Al Balushi T., Nadir Z., Hussain OK. ICS/SCADA system security for CPS. *Studies in Computational Intelligence*. 2018. 89–113 p. Available at: DOI:10.1007/978-3-319-75880-0_5 (Accessed: 15 August 2019)
14. Marwedel P. *Embedded System Design*. Cham: Springer International Publishing; 2018. Available at: DOI:10.1007/978-3-319-56045-8 (Accessed: 15 August 2019)
15. Hameed S., Khan FI., Hameed B. Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review. *Journal of Computer Networks and Communications*. 10 January 2019; 2019: 1–14. Available at: DOI:10.1155/2019/9629381
16. Pham Van P Van., Binh NN. Embedded System Architecture Design and Optimization at the Model Level. *International Journal of Computer and Communication Engineering*. 2012; 1(4): 345–349. Available at: DOI:10.7763/ijcce.2012.v1.87
17. Elahi A. *Computer Systems*. Aerospace America. Cham: Springer International Publishing; 2018. 40 p. Available at: DOI:10.1007/978-3-319-66775-1
18. Elmiligi H., Gebali F., El-Kharashi MW. Multi-dimensional analysis of embedded systems security. *Microprocessors and Microsystems*. Elsevier B.V.; March 2016; 41: 29–36. Available at: DOI:10.1016/j.micpro.2015.12.005 (Accessed: 27 July 2019)
19. Ma B., Mu D., Mao B., Hu W. A bottom-up approach to verifiable embedded system information flow security. *IET Information Security*. 1 January 2014; 8(1): 12–17. Available at: DOI:10.1049/iet-ifs.2012.0342 (Accessed: 13 August 2019)
20. MESHRAM VH., SASANKAR AB. Security in Embedded Systems: Vulnerabilities , Pigeonholing of Attacks and Countermeasures. *IOSR Journal of Computer Engineering*. 2016; : 11–15.
21. Sudhakar S., Praveen Kumar E., Thiyagarajan S. Border security and multi access robot using embedded system. *Indian Journal of Science and Technology*. 10 May

- 2016; 9(16). Available at: DOI:10.17485/ijst/2016/v9i16/92205 (Accessed: 8 September 2019)
22. Negi V., Verma H., Singh I., Vikram A., Malik K., Singh A., et al. Network security in embedded system using TLS. *International Journal of Security and its Applications*. 28 February 2016; 10(2): 375–384. Available at: DOI:10.14257/ijisia.2016.10.2.33 (Accessed: 8 September 2019)
23. Britto C. *International Journal of Innovative Technology and Research*. [Verlag nicht ermittelbar]; 2014; 3075(2): 1101–1106. Available at: https://plu.mx/plum/a/?elsevier_id=2-s2.0-85061817104&theme=plum-scopus-theme (Accessed: 8 September 2019)
24. Kimani K., Oduol V., Langat K. Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*. Elsevier B.V.; 2019; 25: 36–49. Available at: DOI:10.1016/j.ijcip.2019.01.001
25. Waidner M., Kasper M. Security in industrie 4.0 - Challenges and solutions for the fourth industrial revolution. *Proceedings of the 2016 Design, Automation and Test in Europe Conference and Exhibition, DATE 2016*. EDAA; 2016; : 1303–1308. Available at: DOI:10.3850/9783981537079_1005
26. Levy E. Crossover: online pests plaguing the off line world. *IEEE Security & Privacy*. November 2003; 1(6): 71–73. Available at: DOI:10.1109/MSECP.2003.1253573
27. Yampolskiy M., Horvath P., Koutsoukos XD., Xue Y., Sztipanovits J. Taxonomy for description of cross-domain attacks on CPS. *HiCoNS 2013 - Proceedings of the 2nd ACM International Conference on High Confidence Networked Systems, Part of CPSWeek 2013*. New York, New York, USA: ACM Press; 2013; : 135. Available at: DOI:10.1145/2461446.2461465 (Accessed: 17 August 2019)
28. Khelladi L., Challal Y., Bouabdallah A., Badache N. On security issues in embedded systems: challenges and solutions. *International Journal of Information and Computer Security*. 2008; 2(2): 140. Available at: DOI:10.1504/ijics.2008.018515
29. Camurati G., Poeplau S., Muench M., Hayes T., Francillon A. Screaming Channels. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. New York, NY, USA, NY, USA: ACM; 2018. pp. 163–177. Available at: DOI:10.1145/3243734.3243802

30. Moreno C., Fischmeister S. Non-intrusive runtime monitoring through power consumption to enforce safety and security properties in embedded systems. *Formal Methods in System Design*. 19 August 2018; 53(1): 113–137. Available at: DOI:10.1007/s10703-017-0298-3 (Accessed: 8 September 2019)
31. Stühling A., Ehmen G., Fröschle S. Analyzing the impact of injected sensor data on an Advanced Driver Assistance System using the OP 2 TIMUS prototyping platform. *Proceedings of the 2016 Design, Automation and Test in Europe Conference and Exhibition, DATE 2016*. 2016; : 523–526. Available at: DOI:10.3850/9783981537079_0361
32. Hasler J., Shah S. Security implications for ultra-low power configurable SoC FPAA embedded systems. *Journal of Low Power Electronics and Applications*. 5 June 2018; 8(2): 17. Available at: DOI:10.3390/jlpea8020017 (Accessed: 8 September 2019)
33. Chai H., Zhang G., Zhou J., Sun J., Huang L., Wang T. A Short Review of Security-Aware Techniques in Real-Time Embedded Systems. *Journal of Circuits, Systems and Computers*. 12 February 2019; 28(02): 1930002. Available at: DOI:10.1142/S0218126619300022 (Accessed: 8 September 2019)
34. Read H., Sutherland I., Xynos K., Roarson F. Locking Out the Investigator: The Need to Circumvent Security in Embedded Systems. *Information Security Journal*. Taylor & Francis; 25 July 2015; 24(1–3): 39–47. Available at: DOI:10.1080/19393555.2014.998847 (Accessed: 27 July 2019)
35. Fournaris AP., Sklavos N. Secure embedded system hardware design - A flexible security and trust enhanced approach. *Computers and Electrical Engineering*. Elsevier Ltd; January 2014; 40(1): 121–133. Available at: DOI:10.1016/j.compeleceng.2013.11.011 (Accessed: 9 September 2019)
36. Lee EA. Cyber physical systems: Design challenges. *Proceedings - 11th IEEE Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing, ISORC 2008*. IEEE; 2008. pp. 363–369. Available at: DOI:10.1109/ISORC.2008.25 (Accessed: 26 August 2019)
37. Arbaugh WA., Van Doorn L. Embedded security: Challenges and concerns. *Computer*. 2001; 34(10): 40–41. Available at: DOI:10.1109/MC.2001.955096
38. Ashibani Y., Mahmoud QH. Cyber physical systems security: Analysis, challenges

- and solutions. *Computers and Security*. Elsevier Ltd; July 2017; 68: 81–97. Available at: DOI:10.1016/j.cose.2017.04.005 (Accessed: 27 July 2019)
39. Song Han., Miao Xie., Hsiao-Hwa Chen., Yun Ling. Intrusion Detection in Cyber-Physical Systems: Techniques and Challenges. *IEEE Systems Journal*. IEEE; 2014; 8(4): 1052–1062. Available at: DOI:10.1109/jsyst.2013.2257594
40. Sakuneka T., Marnewick A., Pretorius J-H. Industry 4.0 competencies for a control systems engineer. 2019 IEEE Technology & Engineering Management Conference (TEMSCON). IEEE; 2019; : 1–6. Available at: DOI:10.1109/temscon.2019.8813717
41. Baron C., Daniel-Allegro B. About adopting a systemic approach to design connected embedded systems: A MOOC promoting systems thinking and systems engineering. *Systems Engineering*. 2019; (September): 1–20. Available at: DOI:10.1002/sys.21513
42. Mohay G. Technical challenges and directions for digital forensics. *Proceedings - First International Workshop on Systematic Approaches to Digital Forensic Engineering*. 2005; 2005: 155–161. Available at: DOI:10.1109/SADFE.2005.24
43. Hasselbring W., Reussner R. Toward trustworthy software systems. *Computer*. IEEE; 2006; 39(April): 91–92. Available at: DOI:10.1109/MC.2006.142
44. Van Engers TM., Glassée E. Facilitating the legislation process using a shared conceptual model. *IEEE Intelligent Systems and Their Applications*. 2001; 16(1): 50–55. Available at: DOI:10.1109/5254.912385
45. Hatzivasilis G., Papaefstathiou I., Manifavas C. Software security, privacy, and dependability: Metrics and measurement. *IEEE Software*. IEEE; 2016; 33(4): 46–54. Available at: DOI:10.1109/MS.2016.61

**CHAPTER 4: A NOVEL APPROACH FOR DETECTING
CYBERATTACKS IN EMBEDDED SYSTEMS BASED ON
ANOMALOUS PATTERNS OF RESOURCE UTILISATION**

CHAPTER 4: A NOVEL APPROACH FOR DETECTING CYBERATTACKS IN EMBEDDED SYSTEMS BASED ON ANOMALOUS PATTERNS OF RESOURCE UTILISATION

Abdalmohsan Alooseel¹, Saba Al-Rubaye (Senior IEEE Member)¹, Argyrios Zolotas (Senior Member, IEEE)¹, Hongmei He (Senior Member, IEEE)², Carl Shaw³

¹School of Aerospace, Transport and Manufacturing (SATM), Cranfield University

²School of Computer Science and Informatics at De Montfort University

³Cerberus Security Laboratories Ltd, UK.

4.1. Abstract

This paper presents a novel security approach called Anomalous Resource Consumption Detection (ARCD), which acts as an additional layer of protection to detect cyberattacks in embedded systems (ESs). The ARCD approach is based on the differentiation between the predefined standard resource consumption pattern and the anomalous consumption pattern of system resource utilisation. The effectiveness of the proposed approach is tested in a rigorous manner by simulating four types of cyberattacks: a denial-of-service attack, a brute-force attack, a remote code execution attack, and a man-in-the-middle attack, which are executed on a Smart PiCar (used as the testbed). A septenary tuple model consisting of seven parameters, representing the embedded system's architecture, has been created as the core of the detection mechanism. The approach's efficiency and effectiveness has been validated in terms of range and pattern by analysing the collected data statistically in terms of mean, median, mode, standard deviation, range, minimum, and maximum values. The results demonstrated the potential for defining a standard pattern of resource utilisation and performance of the embedded system due to a significant similarity of the parameters' values at normal states. In contrast, the attacked cases showed a definite, observable, and detectable impact on resource consumption and performance of the embedded system, causing an anomalous pattern. Thus, by merging these two findings, the ARCD approach has been developed. ARCD facilitates building secure operating systems in line with the ES's capabilities. Furthermore, the ARCD approach can work along with existing countermeasures to augment the security of the operating system layer.

4.2. Introduction

An embedded system (ES) is a processing unit integrated into a larger cyber-physical system (CPS) to steer its functions. Papp et al. [1], [2] described ESs as follows: “An embedded system is a computing system built into a larger system, designed for dedicated functions. It consists of a combination of hardware, software, and optionally mechanical parts. Thus, the term refers to any computing systems other than general-purpose [personal computer], (sic) or mainframe computers.”.

ESs typically consist of a central processing unit (CPU), memory, peripheral interfaces, and are constructed optionally with instruction or data caches [3]. In addition, local bus channels are built around them to support communication and data exchange. ESs are connected to a power subsystem, providing power to the components' systems, and most of the ESs are powered by battery. Marwedel [4] discusses many tight constraints on ES resources, particularly in the case of a system on a chip (SoC), and how these limitations hinder the ability to implement advanced security solutions. These constrained capabilities also make it impossible to apply conventional security mechanisms [5]. ESs must be resource-aware, and cannot have excessive pipeline performance due to limited resources [6]. The gaps in processing, battery, and cost are at the top of the security challenges list. The high barrier of constraints on computational capability, storage, power, and real-time determinism makes it difficult to maintain data confidentiality through encryption and key management [4]. The addition of many software-based security mechanisms on top of the OS layer would compete for computational resources, introducing an incompatibility with ES capabilities [1]. Developed security solutions must consider the capabilities of software and hardware during the earliest stages of design, hence mitigating the additional cost for cybersecurity at the later stages of the system lifecycle.

The execution of advanced cryptography and other advanced security solutions and countermeasures, such as an intrusion detection system (IDS), require intensive computing resources and inevitably consume more energy [7]. ESs are unable to handle intensive cryptographic calculation-based encryption and decryption operations due to SoC resource limitations [6]. The existing cryptographic algorithms require sufficient processing, memory, and energy capabilities, which may be unavailable in limited

resource SoCs [8]. Therefore, running a robust encryption scheme on an ES with its limited resources is a challenge [9] [10]. Conversely, the nature of an ES poses significant tight constraints and their impact reflects on performance capabilities [11] [12] .

Hameed et al. [13] addressed the issue of distributed denial-of-service (DDoS) attack detection and stated, “Detection of DDoS in IoT is a challenging issue as IoT network and traffic characteristics are quite different from the traditional network. Due to the limitation of IoT devices, resource-efficient DDoS detection and countermeasure techniques are required.” Neglecting security countermeasures at the design stage could provide more chances for attackers to destroy these systems successfully. As many ESs are powered by battery and security enhancement could inevitably sacrifice part of the energy, it is crucial to reduce the amount of power consumption with lightweight and efficient solutions [7]. As Ali et al. [14] stated, the conflicting requirements for higher computational capabilities but lower power consumption pose serious challenges to implement effective and efficient solutions for the security of ESs. It is not feasible to implement conventional IT security solutions in ESs in terms of the ES’s capabilities.

In general, embedded systems are exposed to the same security threats as conventional computer systems, but with significant limitations to handle the advanced security solutions that have been implemented on these conventional computers and servers. Therefore, there is an urgent need for lightweight security strategies to enhance system security under these constraints [7] [13] based on existing hardware and software systems and without excessive computational requirements or additional cost for hardware components.

Based on the relevant studies in this field, we have published a comprehensive analytical study that covers all aspects of the cybersecurity of embedded systems [15] and addressed some of the existing solutions. In this study, we are presenting an alternative security solution, where the proposed approach utilizes resource consumption patterns to recognize the existence of a cyberattack. In this chapter, we aim to deliver a novel security approach to detecting and dealing with cyberattacks without conflicting with the ES's characteristics and without depleting its resources, through monitoring system resource consumption and detecting anomalous performance patterns. The proposed approach is referred to as Anomalous Resource Consumption Detection (ARCD).

Anomaly detection as a concept has been previously implemented in applications such as bank fraud and intrusion detection systems (IDS) [16]. It is worth noting, though, that IDS applications concentrated on the network traffic by inspecting every single packet and looking for any malicious activities or unexpected ongoing data traffic using data analysis methods or machine learning algorithms [17] [18]. This is quite different to the concept proposed in our study that focuses particularly on ESs, benefiting from the ES's characteristics (being dedicated to performing specific functions).

The anomaly detection concept is a wide concept on its own, and it can be implemented in conjunction with uncounted technologies. The definition of Anomaly Detection offered by Barnett and Lewis [19] states that: “an outlier is an observation (or subset of observations) which appears to be inconsistent with the remainder of that set of data” [19]. A survey, which addresses what an anomaly is and gives background on the challenges which may be faced when applying anomaly detection techniques is presented in [20]. Also, a comprehensive review of Network Anomaly Detection Systems (NADs) is presented in [21], where the background and literature related to Intrusion Detection System (IDS) have been discussed. The holistic review addressed various aspects of anomaly-based Network Intrusion Detection Systems (NIDSs), which show the important role of anomaly detection concept in the field of network security. Also, in [22], the authors address the problem of efficient anomaly detection for large-scale network traffic data, and they suggest a parallel network traffic anomaly detection algorithm. Among the related works to anomaly detection is [23]. In this study, the authors propose an Attack Pattern Chain algorithm (APChain) which identifies infected systems in real-time network environments by detecting abnormal behavior of network traffic. This statistical analysis method is a powerful technique for detecting attacks based on the anomaly detection concept, and several statistical approaches for detecting DDoS attacks have been reviewed by the authors in [24].

A Novel Attack Detection Scheme for detecting anomalies in Industrial IoT systems is suggested in [25], where the authors propose a novel lightweight random neural network (RaNN)-based prediction model to improve the cybersecurity aspect of (IIoT). The final results of this study show the effectiveness of using a lightweight random neural network technique in terms of detecting attacks and anomalies in IIoT. Also, in [26], the authors propose a novel DDoS detection scheme combining rule-based and anomaly-based,

where three types of system resource usage (throughput, CPU utilisation, memory utilisation) are measured under DDoS attack conditions. A suggested approach of anomaly detection based on job monitoring resource metrics is presented in [27], where the accuracy of anomaly detection based on the abnormal jobs reaches about 92% [27]. A related work to our suggested approach is a proposed framework for detecting anomalous behavior on smartphones based on statistical analysis of usage patterns [28], where three parameters have been parameterized: CPU usage, RAM utilisation, and network data traffic. The final results of this study show the possibility of detecting malwares in smartphones with an accuracy of 86.24% [28]. The statistical analysis method is one of the most powerful techniques for detecting attacks based on the anomaly detection concept. Statistical approaches for detecting DDoS attacks have been reviewed by the authors of [24]. Also, machine learning algorithms have been used widely in the field of anomaly detection [29].

Several frameworks based on anomaly detection have been suggested and a proposed framework for detecting malware on Android mobile devices has been presented by [30]. The detection mechanism of this framework is based on monitoring various features and events that are obtained from the mobile device and then applying Machine Learning algorithms. According to the authors of [30], the proposed framework is effective in detecting malware on mobile devices in general and on Android in particular, even when using a small number features and simple detection algorithms. Also, an anomaly detection framework for dynamic spectrum access networks has been presented in [31], where the problem of detecting unauthorized spectrum usage has been addressed, and a proposed method to enhance the detection rate has been suggested [31]. Moreover, anomaly detection applications also include cloud infrastructure, and the authors in [32] propose a scalable model for automatic anomaly detection on a large system by learning the system characteristic under normal operation. Another related study to detect attacks in IaaS cloud is presented in [33], where the attack detection is based on analyzing resource consumption profiles. An automated anomaly detection framework for enterprise applications has been presented in [34]. The suggested solution in this study is an integration of two techniques: (1) the resource consumption pattern of the application, and (2) the application performance signature, thus, monitoring any anomalies in the CPU consumption pattern. Among the presented frameworks for anomaly detection is a

contextual anomaly detection framework for big sensor data, presented in [35], where the effectiveness of the contextual framework has been evaluated against two real-world sensor datasets. The identification of resource usage anomalies and use of irregular patterns of resource consumption as an indicator for detecting problems in large distributed systems are suggested as analysis methodology by the authors in [36]. This shows the benefit of monitoring resource utilisation in detecting problems despite its complexities. All of these related studies are pointing in the same direction as the approach that we seek to present, however, what distinguishes our proposed approach is its comprehensive detection mechanism, which is based on the septenary tuple model, as well as its generality through focusing on the embedded system abstractly rather than its implementations.

The remainder of this chapter is organized as follows. In Section 4.3, the hypothesis of this study was presented, and the concept of the septenary tuple model was explained. In section 4.4, the hardware and software for the experimental environment are illustrated. The adopted methodology has been described in Section 4.5. The final results and analysis of the typical cases have been summarized in Section 4.6, followed by the attacked cases results in Section 4.7. The detection latency matter based on the proposed approach has been explained and discussed in Section 4.8. Finally, the conclusion is presented in Section 4.9.

4.3. The Hypothesis and Testbed Configuration

4.3.1. The Hypothesis

The proposed security method is based on the hypothesis that a unique characteristic of ESs distinguishes them from conventional multitasking systems, in which these systems are designed to perform specific functions. Thus, the hypothesis states: *In embedded systems designed to perform specific functions, the performance and resource consumption form a narrowly bounded, determinable pattern. Thus, an anomalous pattern, if it exists and is identifiable, can be exploited as an indicator to detect potential cyberattacks.*

The hypothesis comprises two main parts. First, it requires that when an ES is performing its specific functions, we can identify the range and the pattern of the performance and resource consumption under normal operation conditions and in the absence of cyberattacks. The second part implies that an anomalous resource consumption pattern can be inferred as an indicator of a cyberattack occurrence. To validate the hypothesis, we need to prove the feasibility of creating a standard pattern for the system performance and resource consumption under normal operating conditions (with no cyberattacks present) to be used as the control pattern. Also, in an attack case, we need to prove the existence of anomalous performance and resource consumption and their detectability, contrary to the control case. The anomalous pattern should be recognizable and distinguishable from standard resource consumption. To prove the validity of the hypothesis, we conduct an experiment to observe specific parameters' values, which represent resource consumption and the ES's performance under different circumstances.

Based on the collected data, we will be able to confirm the validity of the first part of the hypothesis, which is essential. If the range and pattern of resource consumption under normal operating conditions is highly variable and undeterminable, it would prove difficult to distinguish anomalous patterns from normal patterns. Hence, the second part of the assumption would not be proved without proof of the first part. After proving the first part of the assumption, we will move to the second part of the research hypothesis and execute various scenarios of cyberattacks to see if it is possible to detect the existence of attacks based on the anomalous change on system performance and resource consumption.

4.3.2. The Testbed

Testbeds “are composite abstractions of systems and are used to study system components and interactions to gain further insight into the essence of the real system” [37]. According to Edgar and Manz [38], a testbed is defined as “a controllable cyber environment that enables experimentation.” In our study, a Smart PiCar will be used as a testbed. The ES within this CPS will be monitored to study particular aspects of system performance and its resource consumption under a controlled environment.

The testbed has specific attributes: (1) purpose, (2) resources, (3) resource management, (4) configuration/initialization, (5) experimental design, (6) experimental control, (7) instrumentation and data collection, and (8) access [38]. During the testbed design stages, these attributes have been taken into account.

Three typical design options are normally adopted for experimental design [39]: (1) simple design, (2) fractional factorial design, and (3) full factorial design. Simple design refers to adopting a fixed configuration and changing one factor at a time to determine the impacts of this factor on system performance. Observing impacts when modifying only a few factors against others reflects the concept of fractional factorial design, whereas altering all factors against each other is an example of the full factorial experimental design concept. The fractional factorial or full factorial design options are the most suitable to study how factors interact with each other.

In our experimental design, we first adopt the simple experimental design approach and alter one factor at a time to determine the impact on system performance. The selected factor is the existence or absence of a cyberattack. This is followed by a parameter selection phase to design a septenary tuple model. In this stage, we adopt a full factorial design to find the most influential parameters to build the detection mechanism's core.

The Smart PiCar provides a realistic hardware-software environment to test the embedded system components under different operational circumstances. As a result of the testbed, we will have quantitative results about the operational behaviour of the ES for specific parameters. Thus, our case study's design decision has been taken based on both theoretical and empirical studies.

4.3.2.1. The Parameters of the Testbed

To validate the proposed security approach, it is necessary to monitor, collect and analyse values of specific parameters on the testbed, representing the performance of a real CPS, to be able to make a comparison between unattacked cases and attacked cases. Determining specific parameters to be investigated in the experiments is not arbitrary, but is based on the architecture of an ES. This consists of a central processing unit (CPU) to manage the data and execute the instructions, volatile memory or random-access memory (RAM), read-only memory or non-volatile memory (ROM), as well as the system bus, communication

subsystem, power subsystem (battery), and input/output units. Based on these components, seven important parameters have been identified as follows:

- 1- CPU utilisation: the CPU utilisation percentage parameter represents the percentage of the total available CPU computing power available that is being used to perform the function of the ES. A Broadcom BCM2711, quad-core ARM Cortex-A72 (SoC - ARMv8) 64-bit is working as the compute unit of the CPS.
- 2- Memory load: the memory (Mem) usage percentage parameter indicates the amount of memory resource used. The Smart PiCar is equipped with 4GB LPDDR4-3200 SDRAM to support the processes of the ARM processor. Specifically, we monitored the active system virtual memory usage percentage. (see *psutil commands* documentation [40]).
- 3- Task count: this parameter reflects the total number of current CPU software processes. These processes are the programs currently under execution in the processor or still alive, and which have not been fully completed by the system or user.
- 4- Thread count: a single program can contain multiple threads. Threads provide a mechanism for coordinating parallel instruction flows within a process. However, “Linux has a unique implementation of threads” [41]: threads and processes are executed in an equivalent manner by the operating system kernel, so a multi-threaded software application appears in a task view as multiple related processes, and thread count has been extracted based on the system command syntax according to the manual pages [42]. Thus, all active threads have been recorded.
- 5- CPU temperature: the CPU temperature (in Celsius) of the processor is an important factor affecting the performance of the system. If the temperature rises without a justifiable reason, that might be an indicator of unexpected activity. “Thermal throttling” of the BCM2711 has been taken into consideration based on documentation from the official website of the Raspberry Pi Foundation [43].
- 6- Power consumption: the power consumption rate is the work done per unit of time and is equivalent to the voltage (V) multiplied by the current, which is measured in amperes or “amps” (A). Therefore, the measurements of voltage and current have been monitored.
- 7- Received (RX) and Transmitted (TX) packets rate: the data traffic whether received or transmitted are meaningful and an important indicator of the system’s connection

stability, and proves that the system is immune to any suspicious activities. The Raspberry Pi is equipped with 2.4 GHz and 5.0 GHz IEEE 802.11ac Wi-Fi and 2.4 GHz BLE Bluetooth 5.0. Only traffic travelling over the 802.11 Wi-Fi interface was measured.

4.3.2.2. Symbolic Model for the Testbed

The above-mentioned parameters represent the hardware/software components of the ES that interact instantly with performed functions of the system. Thus, a dynamic reflection of the system's health can be observed by monitoring these parameters' changes. The CPU works as the brain of the system and each process running in the CPU will directly reflect on the memory consumption. The temperature of the ARM processor and its changes will reflect the load of the CPU. In addition, to attest to system stability and reliability, and to ensure that the system performance is accurately measured, the number of alive processes and executed threads have been included among the testbed's parameters. Additionally, energy consumption rate has been included as a parameter because it is one of the most important resources of an ES. Its stability or fluctuation is expected to give a meaningful indication of activity during the experiment. A parameter model reflecting the Smart PiCar ES state is therefore represented by a septenary tuple, $\{U, M, N, \mathcal{G}, T, P, R\}$, shaping the ranges and patterns of performance and resource consumption. It is as described as below:

U : CPU utilisation, $U = \{u_r, u_p\}$, where u_r is the range of the CPU utilisation and u_p is the pattern of CPU utilisation.

M : Memory utilisation, $M = \{m_r, m_p\}$, where m_r is the range of memory utilisation and u_p is the pattern of memory utilisation.

N : Task count, $N = \{n_r, n_p\}$, where n_r is the range of active tasks and n_p is the execution pattern of tasks.

$\mathcal{G}$: Thread count, $\mathcal{G} = \{\mathcal{G}_r, \mathcal{G}_p\}$, where $\mathcal{G}_r$ is the range of executed threads and $\mathcal{G}_p$ is the execution pattern of the threads.

T : CPU temperature, $T = \{t_r, t_p\}$, where t_r is the range of CPU temperature and t_p is the thermal pattern.

P : Power consumption, $P = \{V, I\}$, where V : voltage, $V = \{V_r, V_p\}$, V_r is the range of the voltage, and V_p is its pattern; I : current, $I = \{I_r, I_p\}$, where I_r is the range of current volt and I_p is its pattern.

R : Rate of RX and TX packets, $R = \{RX_r, RX_p\}$, where RX_r is the range of received packets and RX_p is its pattern. Similarly, in TX, TX_r is the range and TX_p the pattern of transmitted packets.

Table 4-1 summarizes these parameters in terms of associated resource or performance measurement, along with the symbol used to represent them, and Table 4-2 summarizes the calculated statistical criteria.

Table 4-1: Parameters of the testbed

Parameters		Abbr.	Executed commands / Tools
Resources Consumption	CPU	U	<code>psutil.cpu_percent()</code>
	Memory	M	<code>psutil.virtual_memory()</code>
	Temp	T	<code>/sys/class/thermal/thermal_zone0/temp</code>
	Power	P	UM25C USB power meter, for (Voltage, Current)
Performance	Tasks	N	<code>'sudo ps aux wc -l'</code>
	Threads	$\mathcal{G}$	<code>'sudo ps -eLf wc -l'</code>
	Rates of Received & Transmitted Packets	R	<code>int(open('/sys/class/net/wlan0/statistics/tx_packets').read());</code> (and for transmitted packets (rx) instead of tx)

Table 4-2: Statistical Analysis Criteria

Criteria		Abbr.	Value
Range	Minimum	X_{minV}	The lowest value.
	Maximum	X_{maxV}	The highest value.
	Range	X_{gV}	The difference between the lowest and highest.
Pattern	Mean	X_{avgV}	The average.
	Mode	X_{modV}	The highest frequency value (density point).
	Median	X_{midV}	The middle number in a sorted list of values.
	Standard deviation	X_{stdV}	A measure of how spread out numbers are.

The U , M , T , and P parameters represent resource consumption, while the N , $\mathcal{G}$, and R parameters represent aspects of system performance. All the values of these parameters in both resource consumption and performance will be analysed based on seven statistical criteria that define their ranges and patterns. For the ranges, the minimal (X_{minV}), maximal (X_{maxV}), and range (X_{gV}) values will be calculated to determine the range, where X refers to

a parameter. To determine the pattern, the following values will be calculated: the median (X_{midV}), mean (X_{avgV}), mode (X_{modV}), and standard deviation (X_{stdV}).

4.4. Hardware and software of the testbed

A Smart PiCar (equipped with a Pi camera) has been designed for reconnaissance purposes and is used as the testbed of the validation experiments. A Raspberry Pi 4 Model B is integrated as a processing unit (the ES) to handle the computational processes and steer the actions of the PiCar. The Smart PiCar consists of the following components: ultrasonic obstacle avoidance module, robot hardware attached on tops (HATs) Raspberry Pi module, and a motor driver module. The bus PWM driver supports independent output power and uses four wires to control the back wheels. The system was configured with DEBIAN RASPBIAN GNU/Linux version 10.2, and to complete the programmatic settings of the Smart PiCar the system was configured according to the documentation provided by SunFounder Inc. In addition, the Secure Shell protocol (SSH) and the Pi camera were enabled. Figure 4-1 depicts the hardware configuration of the assembled Smart PiCar testbed.

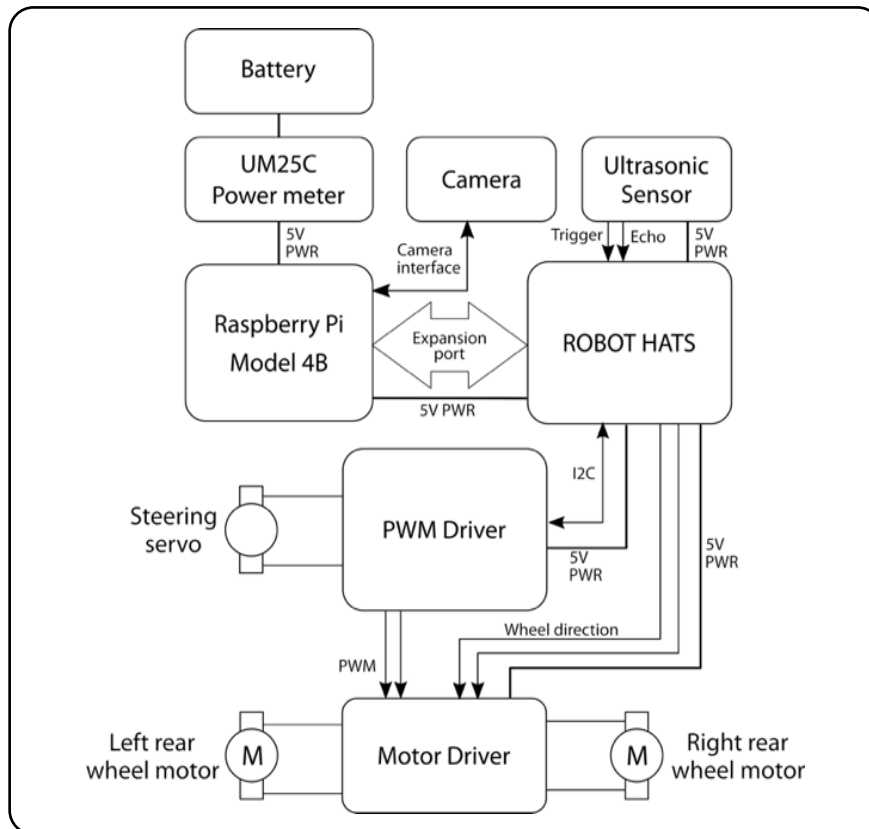


Figure 4-1. (A) The testbed: A Smart PiCar with its schematic diagram

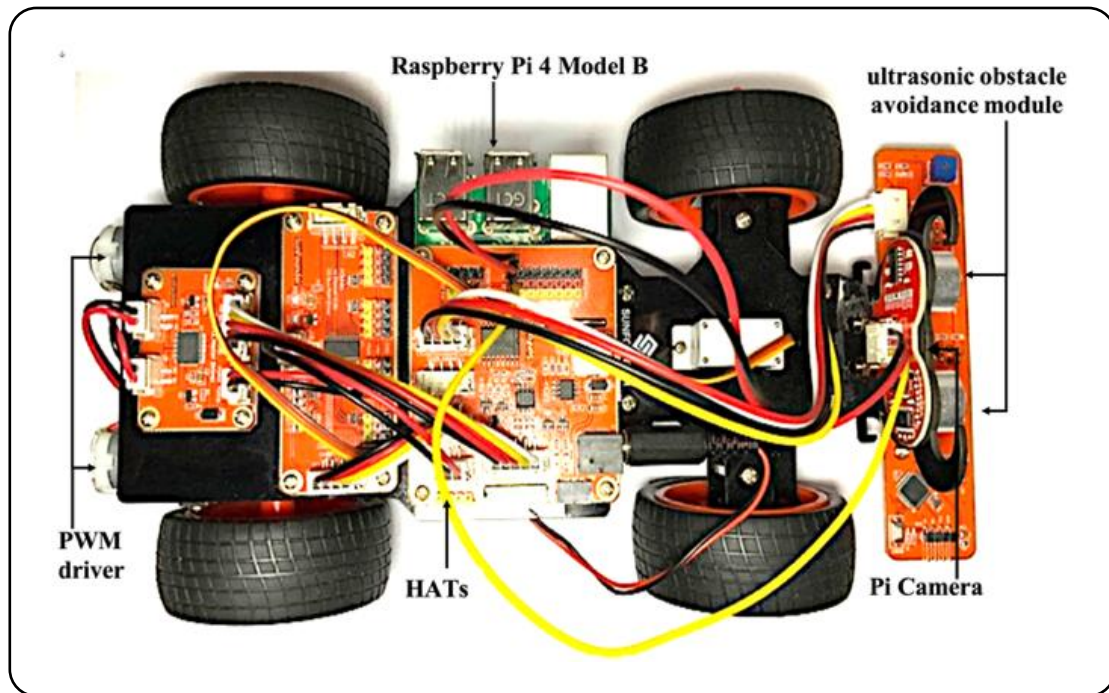


Figure 4-1. (B) The testbed: A Smart PiCar with its schematic diagram

4.5. Methodology

To prove the effectiveness of the proposed approach, we conducted a series of scientific experiments using the testbed. This series of experiments was performed on a healthy system and under attack conditions by exposing the same system to four different types of cyberattacks to validate the accuracy of the hypothesis, which states there exist discernable patterns in system resource consumption.

The methodology of this study consists of three main phases: (1) initializing the experiment environment, (2) conducting the experiments, and (3) using an analysis method for validation (Figure 4-2).

4.5.1. Configuration of the Experiment Environment

Phase I is to create a suitable testbed environment and its procedure should be applicable across different platforms. To extract the values of specific parameters from Raspberry Pi, specific Linux commands are inserted in compatible Python syntax, (*Appendix A*). Based on the official Linux and Python references [42] [44], Table 4-1 shows the executed

commands to extract the required parameters' values and the tool that has been used to measure the power consumption. A UM25C USB power meter tester was attached to the Smart PiCar to take voltage and current measurements and was connected to a portable power source to supply the Smart PiCar with the needed energy.

In Phase II, two cases are studied:

- 1- **Normal case:** The Smart PiCar is run repeatedly without any cyberattacks to generate three rounds of data reference sets (Rs): R1 first round, R2 second round, and R3 third round. The values of the selected parameters will be collected and analysed according to the statistical criteria. Based on the values analysis, a standard model (*Std*) will be generated, where the range is *Std_r* and pattern is *Std_p*.
- 2- **Attacked case:** The Smart PiCar is run repeatedly four times but this time under different types of cyberattacks: (1) Denial-of-Service (DoS), (2) password attack (Brute-Force (BF)), (3) Remote Code Execution (RCE), and (4) Man-in-the-Middle attack (MITM). The landscape of the experiments is shown in Figure 4-2.

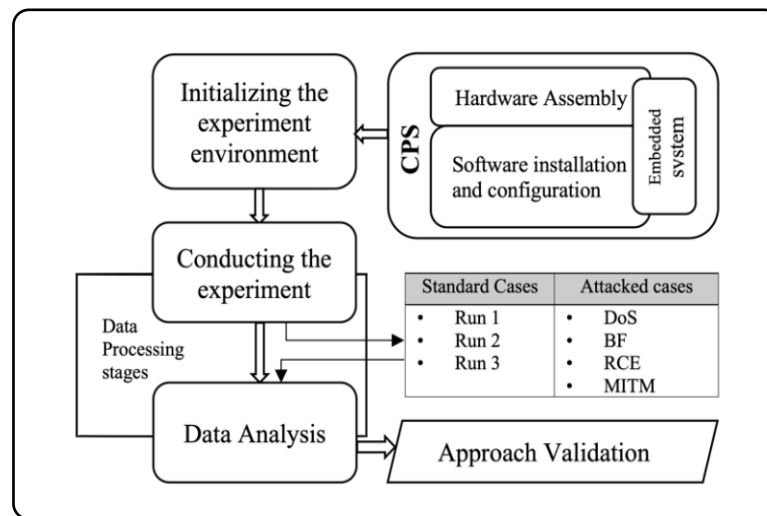


Figure 4-2. The experiment landscape on the testbed

To ensure the data collection's accuracy and integrity, the system was rebooted before each experiment and the following steps were taken:

- All the physical components and connecting cables were checked visually.
- The USB meter tester was activated to monitor the energy consumption via Bluetooth.
- The electrical power source was connected.
- The Raspberry Pi and Smart PiCar were switched on.

- The IP address of the test device was determined by using the following command:
`pi@raspberrypi: ~ $ arp -a`
- After determining the IP address, the Smart PiCar was remotely accessed.
- The accuracy of the system time and time zone was checked in order to ensure a precise time stamp during the data collection period.
- The recording function for the built-in camera was activated in the Smart PiCar by executing the following command: `pi@raspberrypi: ~ $ raspivid -o video.h264 -t 360000`
- The ultrasonic obstacle avoidance module was activated according to the instructions provided by the manufacturer.
- The Python program that had been written for the purpose of extracting and saving the values of the testbed's parameters was started.
- Finally, the ambient and initial temperatures of the system were recorded.

After completing all these steps and after the system had completed an entire cycle of performing its functions, parameter values representing (336 seconds) of operation were extracted and stored as records. These steps have been repeated for each round. At the end of the video recording period, the system stops its recording function automatically. After that, the following steps were followed to collect and save the data in preparation for the analysis phase: (1) the log file and the recorded video were renamed with unique names to avoid being overwritten by the next run; (2) the produced files for R1, R2, and R3 were relabelled; and (3) the system was rebooted in preparation for the next round. The steps were then repeated.

4.5.2. Experiment Conduction and Analysis Method

After completing the data collection of the recurring experiments (*Appendix C*), the third phase of data analysis was started, aiming to generate a reliable standard model for measurement and comparison. This should allow the validity of the first part of the hypothesis to be tested in terms of the determinability and definability of the standard range and pattern of regular consumption. Then, moving to the second part of the hypothesis, the same steps will be repeated but under different cyberattack scenarios that are expected to have an anomalous impact. The execution of attack scenarios will be explained in the upcoming sections. The third phase consists of six stages, starting with data generation and ending with approach validation. Figure 4-3 summarizes these six stages.

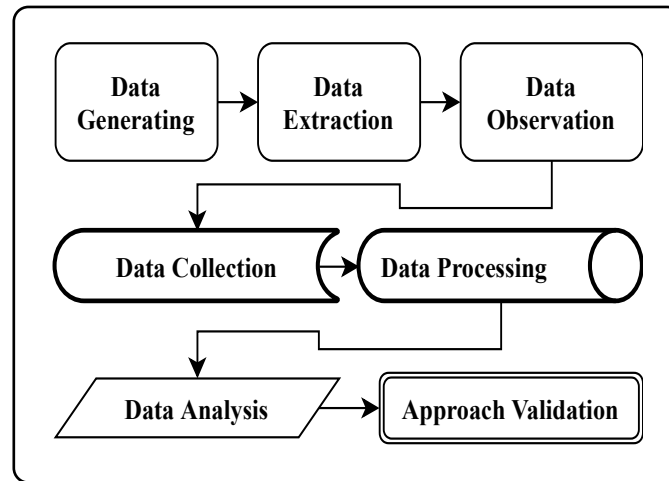


Figure 4-3. Data Processing Stages

To generate the data, we will operate the Smart PiCar remotely through the terminal using the SSH protocol. The targeted parameters were linked to an IoT analytics platform (*ThingSpeak*) to visualise and analyse the data when needed as an option. To collect and store the data in a log file, the following command was included in the Python code:

`'sys.stdout = open("log.csv","a+")'`. Log entries were written to this file following a comma-separated values (CSV) file convention within the Python code. During the data processing stage, the timestamp of each entry was checked and any corrupted or duplicated data was excluded.

By comparing the values of the selected parameters in terms of the statistical criteria, the range and pattern of the system performance and resource consumption, whether under normal operating conditions or under attack impacts, could be defined. For the first part of the experiment, if the results of these criteria show similarity, consistency, identity, or conformity in terms of the parameters' values, the validity of the first part of the hypothesis will be proven. A standard model, based on typical operating cases, will be generated by filling the defined statistical criteria according to the septenary tuple model after the analysis stage. For the second part of the experiment, if the parameters' values of these criteria under the cyberattack circumstances diverge, deviate, or differ from standard cases in terms of the range and patterns, then the mechanism of the approach will be an efficient security solution as long as this anomalous consumption can be monitored and is detectable and distinguishable.

4.6. Results and Analysis of Normal Cases

4.6.1. CPU Utilisation

In this section, the acquired results from the testbed were analysed and the analytical results of the collected data of the embedded system's functions under normal operating conditions showed great similarity in terms of U , where the U_{avgV} ranged between 12.39%, 12.68%, and 12.74% for R1, R2, and R3, respectively. Also, the U_{modV} was concentrated between 7.90%, 7.70%, and 7.50%. The range (U_{gV}) of the distribution of the values was between 20.20%, 20.50%, and 22.80%. Table 4-3 summarizes these criteria values, and Figure 4-4 demonstrates the CPU utilisation patterns, showing their great similarity among R1, R2, and R3.

Table 4-3: CPU Utilisation Under Normal Operating Conditions

CPU (U)		Abb.	R1	R2	R3
Pattern	Mean	U_{avgV}	12.39	12.68	12.74
	Mode	U_{modV}	7.90	7.70	7.50
	Median	U_{midV}	11.80	12.40	12.50
	Std. Deviation	U_{stdV}	4.40	4.35	4.53
Range	Range	U_{gV}	20.20	20.50	22.80
	Minimum	U_{minV}	6.20	4.60	5.70
	Maximum	U_{maxV}	26.40	25.10	28.50

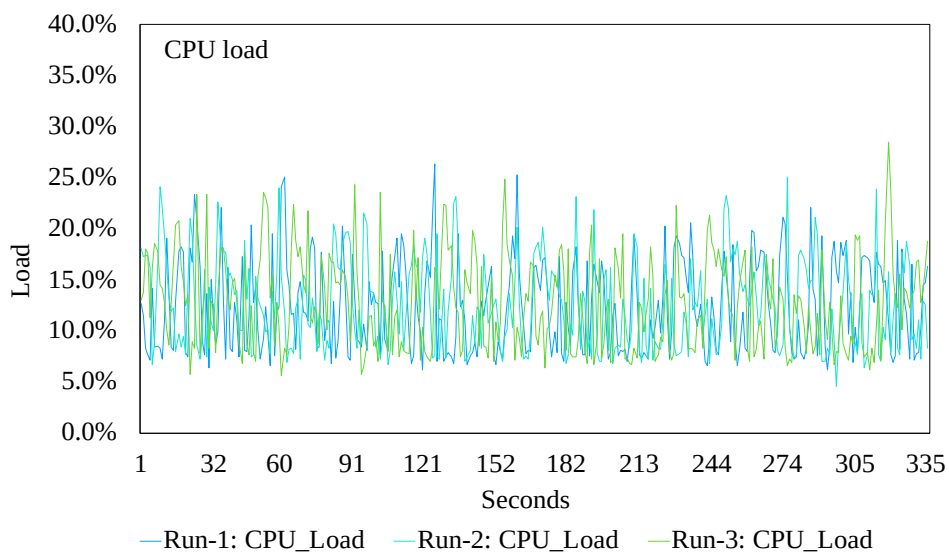


Figure 4-4. CPU load patterns for R1, R2, and R3

4.6.2. Memory Load

In terms of memory usage, not only were similarities observed, but an identical memory performance was recorded in terms of memory mode (M_{modV}), where the memory usage percentage (Mode) was concentrated at 9.50% in R1, R2, and R3. Likewise, the M_{midV} value was 9.50 in all cases and the minimum value was at 9.30% in R1, R2, and R3. The range values ranged between 1.40 and 1.50, which showed a stable pattern in memory load with only a 0.10 difference. Also, the standard deviation values were close in R1, R2, and R3. Table 4-4 summarizes these criteria values, and Figures 4-5 and 4-6 show the transcendent conformity in terms of memory usage rate each time the system's functions have been activated under regular operation conditions.

Table 4-4: Memory performance under standard operating conditions

Memory (M)		Abb.	R1	R2	R3
Pattern	Mean	M_{avgV}	9.52	9.51	9.52
	Mode	M_{modV}	9.50	9.50	9.50
	Median	M_{midV}	9.50	9.50	9.50
	Std. Deviation	M_{stdV}	0.21	0.23	0.20
Range	Range	M_{qV}	1.40	1.50	1.40
	Minimum	M_{minV}	9.30	9.30	9.30
	Maximum	M_{maxV}	10.70	10.80	10.70



Figure 4-5. Memory load for R1, R2, and R3.

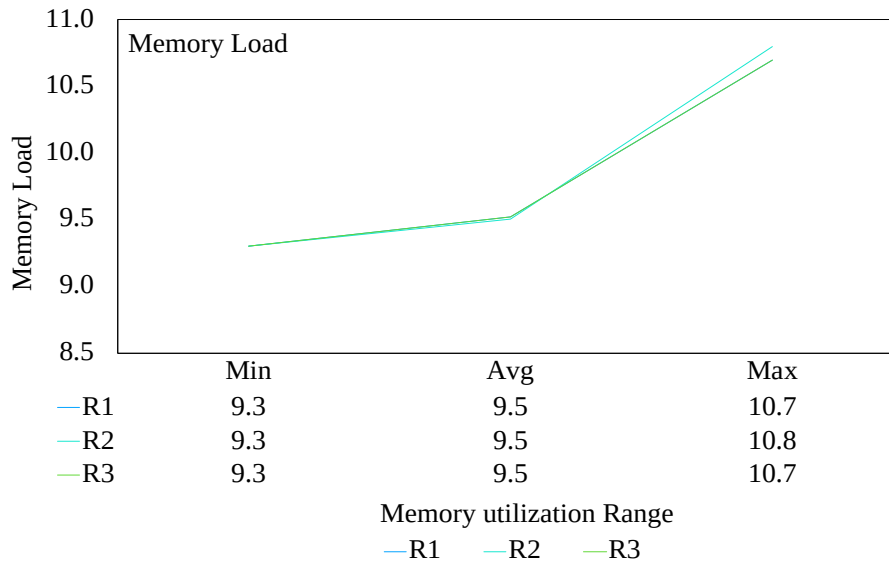


Figure 4-6. Memory load for R1, R2, and R3.

4.6.3. Tasks and Threads

In terms of the number of processes and threads, the statistical criteria results showed a remarkable convergence, as can be seen in Tables 4-5 and 4-6. The average values (N_{avgV}) of the three rounds in terms of counting alive tasks were 167.9, 168.8, and 168.1 for R1, R2, and R3, respectively. Also, the average values of executed threads were 228, 228.9, and 228.3, respectively, for R1, R2, and R3.

Also, one of the most important aspects to determine the pattern is the mode (N_{modV} and $\mathcal{G}_{modV}$) value, which has been calculated to determine the performance pattern for R1, R2, and R3. In terms of tasks count mode, the N_{modV} values were identical in all Rs cases (172 alive tasks). Also in terms of threads, the $\mathcal{G}$ values were identical (232 threads). Likewise, in terms of the N_{maxV} for R1, R2, and R3, the values were identical (173 tasks). In terms of threads number, the range ($\mathcal{G}_V$) between the highest and lowest value also was identical between R1 and R3. Therefore, the ability to define the range and pattern of the typical consumption for the system designed to perform specific functions can be seen clearly in these testbed results. Figures 4-7 and 4-8 demonstrate a significant similarity in the pattern of performance in terms of tasks and threads.

Table 4-5: Values of tasks number under standard operating conditions

Tasks No.		Abb.	R1	R2	R3
Pattern	Mean	N_{avgV}	167.9	168.8	168.1
	Mode	N_{modV}	172.0	172.0	172.0
	Median	N_{midV}	172.0	171.0	172.0
	Std. Deviation	N_{stdV}	4.5	3.6	4.2
Range	Range	N_{gV}	14.0	11.0	13.0
	Minimum	N_{minV}	159.0	162.0	160.0
	Maximum	N_{maxV}	173.0	173.0	173.0

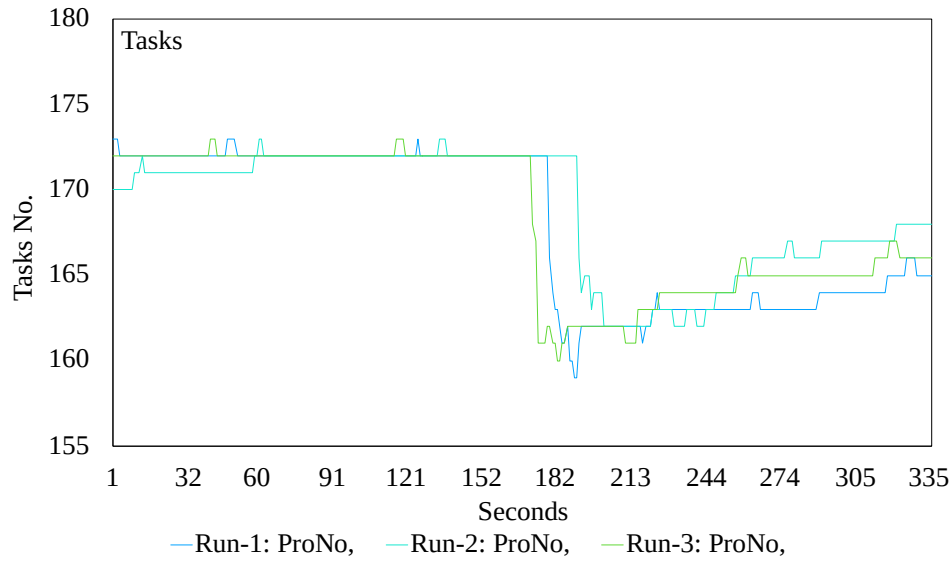


Figure 4-7. Tasks number for R1, R2, and R3

Table 4-6: Values of Threads number under standard operating conditions

Threads No.		Abb.	R1	R2	R3
Pattern	Mean	$\mathcal{G}_{avgV}$	228.0	228.9	228.3
	Mode	$\mathcal{G}_{modV}$	232.0	232.0	232.0
	Median	$\mathcal{G}_{midV}$	232.0	231.0	232.0
	Std. Deviation	$\mathcal{G}_{stdV}$	4.5	3.6	4.2
Range	Range	$\mathcal{G}_{gV}$	14.0	12.0	14.0
	Minimum	$\mathcal{G}_{minV}$	219.0	222.0	220.0
	Maximum	$\mathcal{G}_{maxV}$	233.0	234.0	234.0

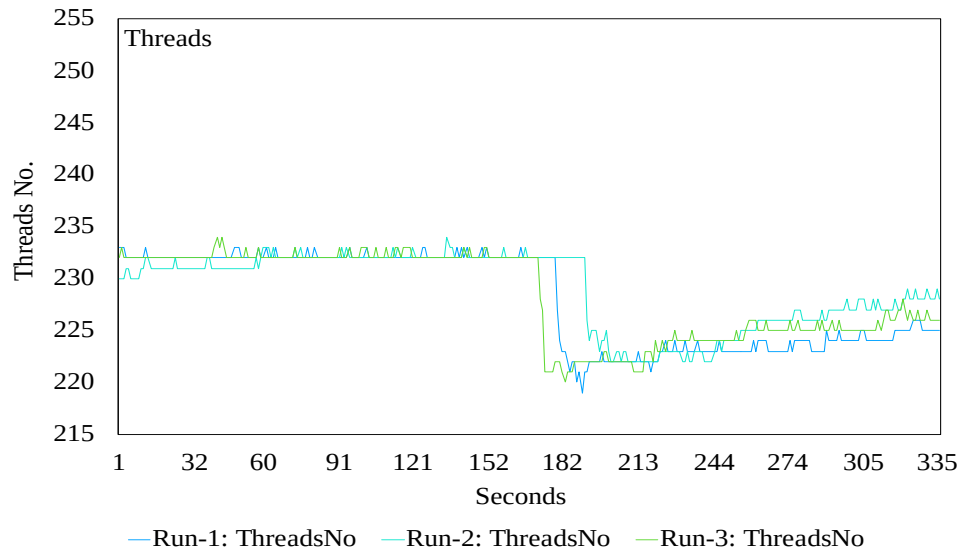


Figure 4-8. Threads number for R1, R2, and R3

4.6.4. CPU Temperature

When dealing with the ARM processor's temperature, it was necessary to take into account the ambient temperature and consider the initial temperature before experimenting. By taking into account the ambient and initial temperatures, we will avoid any misleading of these external factors, especially when conducting the attacked scenarios. After conducting the experiment and collecting the data, Table 4-7 shows the final results for R1, R2, and R3 in terms of CPU temperature. Figure 4-9 depicts the range and pattern of the processor temperature under normal operating conditions.

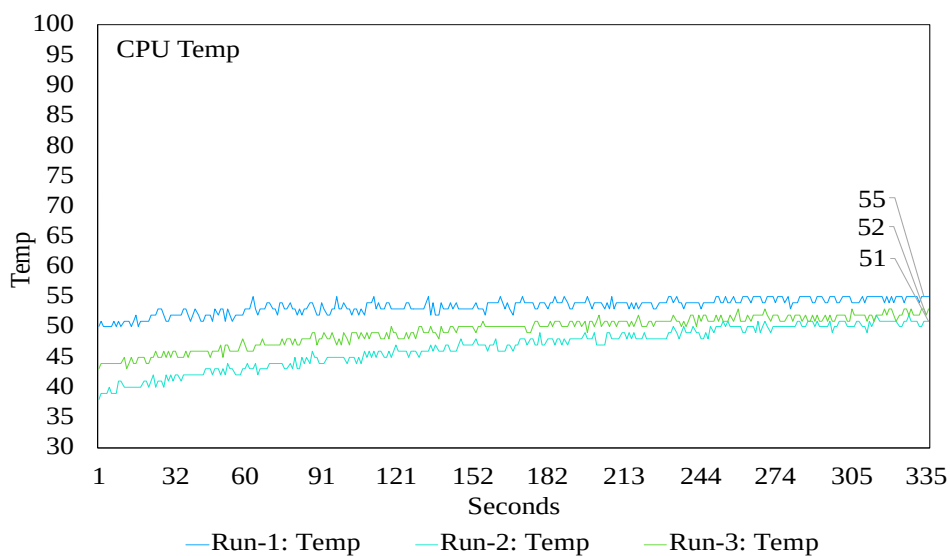


Figure 4-9. CPU temp (°C) for R1, R2, and R3

Table 4-7: CPU Temp Under Standard Operating Conditions

CPU Temp		Abb.	R1	R2	R3
Pattern	Mean	T_{avgV}	53.45	46.60	49.34
	Mode	T_{modV}	54.00	50.00	51.00
	Median	T_{midV}	54.00	47.00	50.00
	Std. Deviation	T_{stdV}	1.24	3.32	2.45
Range	Range	T_{gV}	5.00	14.00	10.00
	Minimum	T_{minV}	50.00	38.00	43.00
	Maximum	T_{maxV}	55.00	52.00	53.00
	Initial	-	50.00	38.00	43.00
	Ambient	-	23.00	21.00	23.00

Based on Table 4-7, the CPU temperatures were concentrated (T_{modV}) at 54°C, 50°C, and 51°C for R1, R2, and R3, even when the initial temperature in R2 was at 38°C, which is considered low compared to the other initial temperatures (R1 and R3), where it tended to rise and stabilize between 51°C and 54°C. Regarding the effect of the surrounding environment's temperature, the difference between the T_{modV} values and the outer temperature (ambient) in all ordinary cases was very close as the difference reached 31°C, 29°C, and 28°C for R1, R2, and R3, respectively.

4.6.5. Power Consumption Measuring

Among the testbed's parameters, the rate of power consumption was observed, where Tables 4-8 and 4-9 show a remarkable similarity and significant convergence in the rate of P in terms of V and I , with the current (I) being more important as the voltage (V) drops slightly while the current changes rapidly and the regulator struggles to maintain the 5V level. As shown in the voltage table results, the V_{modV} was 4.99v in R1 and 5v in R2 and R3, and these values represent the minimum and maximum recorded volts, which are identical in R1, R2, and R3. Also, the median (V_{midV}) values were almost identical (4.99) in R1, R2 and R3. In terms of the current, the I_r or current patterns were noticeably intertwined, as demonstrated in Figure 4-11. This pattern formed the normal range of power consumption in terms of current, ranging between 0.59A at its lowest level and 0.68A as the maximum value. Also, the I_{avgV} for R1, R2, and R3 was at $\approx 0.62A$, where similarly the I_{midV} , and I_{std} values were converging. These results describe the power consumption rate's stability under normal conditions. Tables 4-8 and 4-9 summarize these results, and Figures 4-10 and 4-11 show the power consumption patterns and their ranges.

Table 4-8: values of voltage (V) under typical operating conditions

	Volt (V)	Abb.	R1	R2	R3
Pattern	Mean	V_{avgV}	4.995	4.996	4.995
	Mode	V_{modV}	4.990	5.000	5.000
	Median	V_{midV}	4.995	4.996	4.995
	Std. Deviation	V_{stdV}	0.001	0.001	0.001
Range	Range	V_{qV}	0.010	0.010	0.010
	Minimum	V_{minV}	4.990	4.990	4.990
	Maximum	V_{maxV}	5.000	5.000	5.000

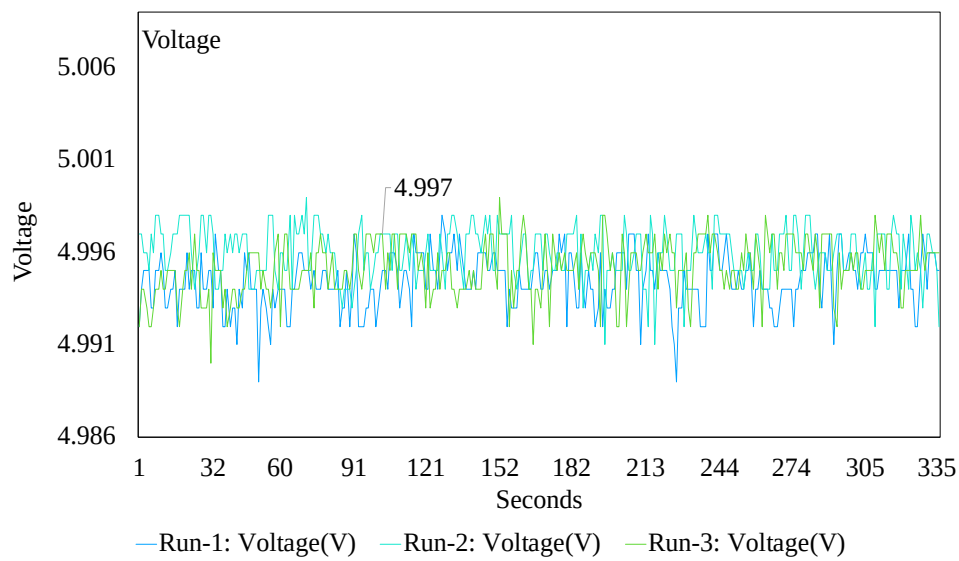


Figure 4-10. Voltage measurements for R1, R2, and R3

Table 4-9: current values (Ampere: A) Under typical operating conditions

	Current (A)	Abb.	R1	R2	R3
Pattern	Mean	I_{avgV}	0.624	0.625	0.620
	Mode	I_{modV}	0.610	0.620	0.610
	Median	I_{midV}	0.623	0.625	0.618
	Std. Deviation	I_{stdV}	0.014	0.016	0.015
Range	Range	I_{qV}	0.080	0.090	0.070
	Minimum	I_{minV}	0.590	0.590	0.590
	Maximum	I_{maxV}	0.670	0.680	0.670

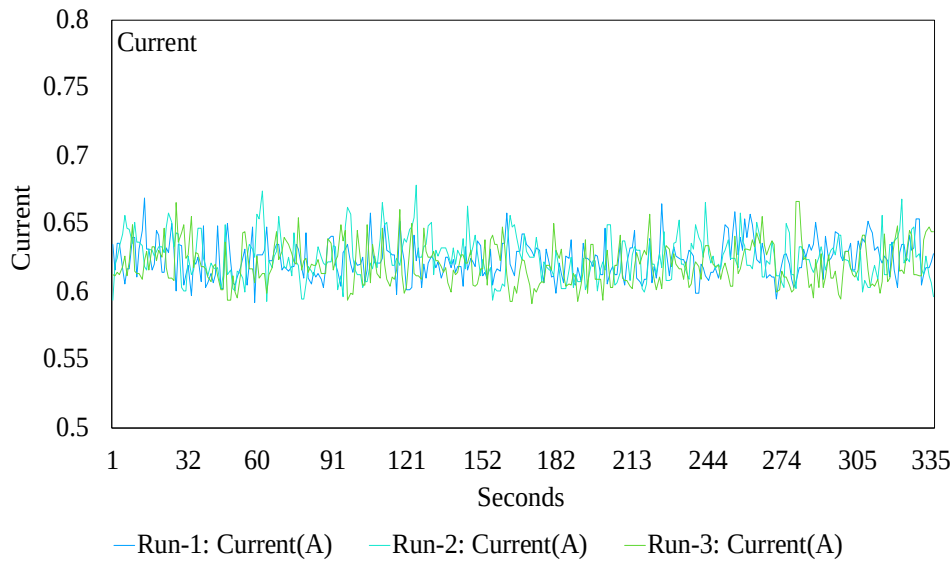


Figure 4-11. Current measurements for R1, R2, and R3.

4.6.6. Data Traffic Rate

The data traffic rate is one of the testbed parameters, and as long as the ESs are designed to perform specific functions, we assume that the data transmission rate (transferring and receiving) will be within a determinable range (RX_{gV} and TX_{gV}). Therefore, the number of received and transmitted packets per second were monitored and stored in the log files. The final results of R1, R2, and R3 in terms of the received and transmitted packets count are described in Tables 4-10 and 4-11.

Table 4-10: Received packets rate under standard operating conditions

RX Packets		Abb.	R1	R2	R3
Pattern	Mean	RX_{avgV}	4.04	4.29	5.00
	Mode	RX_{modV}	0.00	0.00	0.00
	Median	RX_{midV}	1.00	1.00	2.00
	Std. Deviation	RX_{stdV}	5.28	5.72	6.02
Range	Range	RX_{gV}	24.00	27.00	27.00
	Minimum	RX_{minV}	0.00	0.00	0.00
	Maximum	RX_{maxV}	24.00	27.00	27.00

Based on the results of the analysis criteria of received packets shown in Table 4-10, it can be concluded that the RX_{avgV} was between 4.04 and 5 packets. The normal distribution range (RX_{gV}) of the received packets rate ranged between 0 to 27 packets based on R1, R2, and R3. In general, these results show remarkable similarity, especially if we consider that the most frequent value (RX_{modV}) is 0 in R1, R2, and R3, indicating that the volume of the

received data is low and subject to the purposes for which the system was designed. Also, the RX_{midV} and RX_{stdV} values reflect significant convergence between R1, R2, and R3 in terms of received packets volume. Figure 4-12 shows the similarities in patterns of the received packets for R1, R2, and R3.

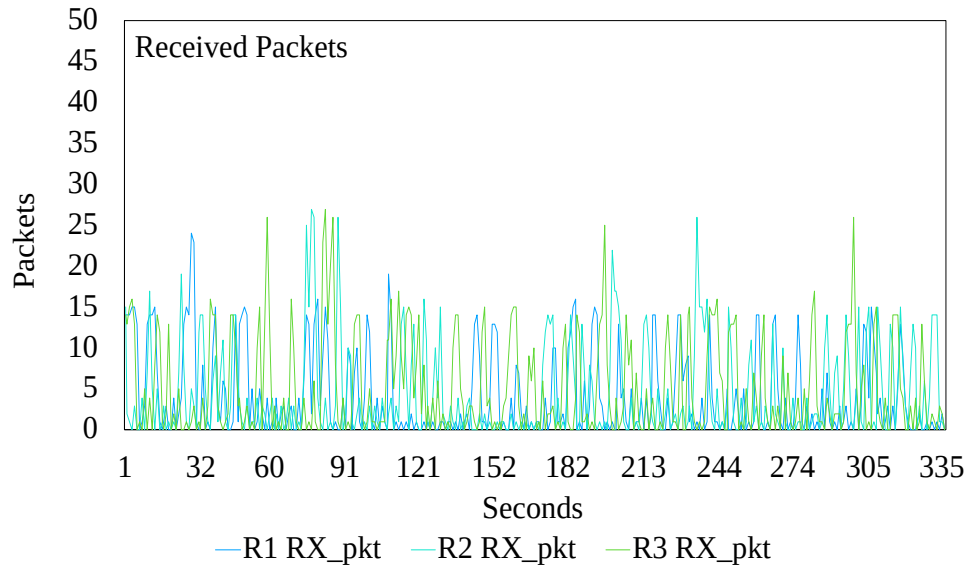


Figure 4-12. Received packets rates for R1, R2, and R3.

In terms of the transmitted packets, the TX_{modV} and TX_{minV} values were identical for R1, R2, and R3, which is 0, as shown in Table 4-11. As for the TX_{avgV} , TX_{maxV} , and TX_gV of the transmitted packets, the values were not 100 % identical, but they are close enough to shape a determinable range and pattern for the standard model. Table 4-11 summarizes the final results of the statistical criteria. Figure 4-13 depicts the similarities in patterns for R1, R2, and R3 in terms of transmitted packets.

Table 4-11: Transmitted packets rate under standard operating conditions

TX Packets		Abb.	R1	R2	R3
Pattern	Mean	TX_{avgV}	4.03	4.29	5.05
	Mode	TX_{modV}	0.00	0.00	0.00
	Median	TX_{midV}	1.00	1.00	2.00
	Std. Deviation	TX_{stdV}	5.27	5.72	6.03
Range	Range	TX_gV	24.00	29.00	27.00
	Minimum	TX_{minV}	0.00	0.00	0.00
	Maximum	TX_{maxV}	24.00	29.00	27.00

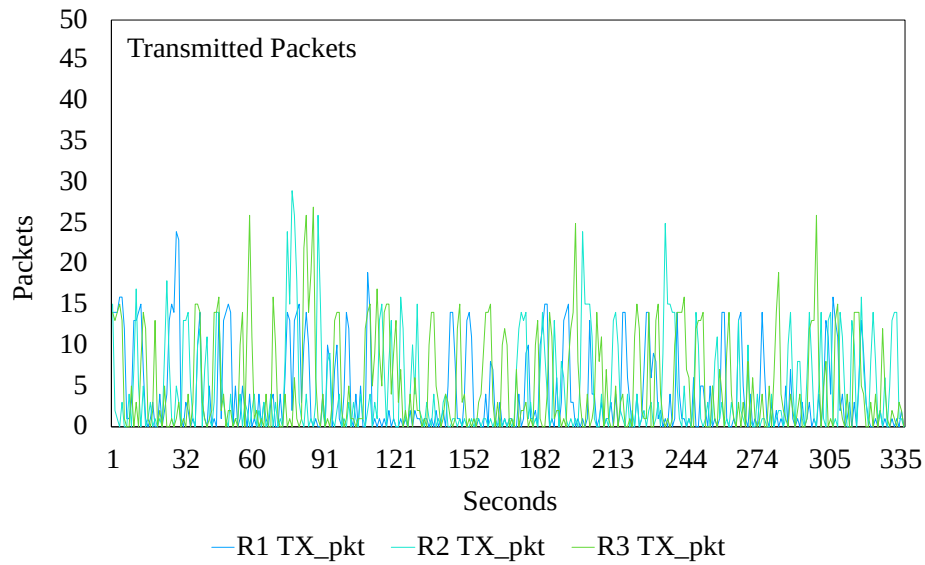


Figure 4-13. Transmitted packets rates for R1, R2, and R3

Based on the septenary tuple model of the parameters' values $\{U, M, N, \mathcal{G}, T, P, R\}$, and according to the statistical criteria results, we can say that the range and pattern of the ES's performance and its resource consumption under normal operating conditions fall within a definable range and determinable pattern. Table 4-12 shows the values of the standard model in terms of the Std_r and Std_p of the Smart PiCar implemented based on the septenary tuple model. Also, the probability of unlisted, convergent values within the normal range has been calculated by extending the maximal and minimal marginal by adding the highest subtracted value between Rs cases in each parameter for every statistical criterion to the standard range and pattern. The following table shows the determined range and pattern values of standard performance and resource consumption.

Table 4-12: values of the Generated standard model

P	Std_r	Std_p		
	Std_{rV}	Std_{avgV}	Std_{midV}	Std_{modV}
U	$3 > V > 31.9$	$12.0381 > V > 13.0863$	$11.1 > V > 13.2$	$7.5 > V > 8.1$
M	$9.3 > V > 10.9$	$9.4922 > V > 9.5396$	$V = 9.5$	$V = 9.5$
N	$156 > V > 173$	$166.9851 > V > 169.7172$	$170 > V > 173$	$V = 172$
$\mathcal{G}$	$216 > V > 235$	$227.0923 > V > 229.8511$	$230 > V > 233$	$V = 232$
R_{rx}	$0 > V > 30$	$3.0744 > V > 5.9583$	$0 > V > 3$	$V = 0$
R_{tx}	$0 > V > 34$	$3 > V > 6.0804$	$0 > V > 3$	$V = 0$
P_v	$4.99 > V > 5$	$4.993 > V > 4.9975$	$4.994 > V > 4.997$	$4.98 > V > 5.01$
P_I	$0.59 > V > 0.69$	$0.6154 > V > 0.6304$	$0.6112 > V > 0.6313$	$V = 0.61$
T	$26 > V > 58$	$39.747 > V > 60.3006$	$40 > V > 61$	$46 > V > 58$

Proving the ability to define a standard model for the ES designed to perform specific functions paves the way for the software engineer to apply the necessary restrictions to maintain an optimal resource consumption level for the prevention of any heterogeneous consumption due to illegal activities. However, we will not stop at this conclusion alone, as these results prove the correctness of the first part of the hypothesis. It must be ensured that cyberattacks are causing anomalous consumption patterns that can be distinguished from typical consumption. This approach will be validated computationally to ensure that the ES with its hardware and software layers can distinguish between regular consumption and anomalous consumption. This will be covered later (Chapter 5) by testing a random dataset of the collected data by using the Support Vector Machine (SVM) algorithm.

4.7. Attacked Cases Results

4.7.1. Denial-of-Service Attack (DoS)

According to the Department of Homeland Security official website [45], the denial-of-service (DoS) cyberattack is “a denial-of-service condition accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users.” DoS is the general description of different types of cyberattacks that tend to breach one of the security goals, which is availability. Some examples of this type of attack are distributed denial-of-service (DDoS), application-layer attacks, advanced persistent DoS, and denial-of-service as a service. Carrying out one of these types of DoS attacks can be done by using many techniques. Also, repelling these types of attacks depends on different defence techniques.

During the testbed, the Low Orbit Ion Cannon (LOIC) tool was implemented to perform a DDoS attack. From Windows virtual machine, the LOIC was used to flood the targeted ES (the victim device) with random data using TCP as the connection protocol, and port 22 was selected as the targeted port. The LOIC is an open-source tool written by C#. The victim device (the Smart PiCar) was flooded with arbitrary messages from another Windows virtual machine by using the User Datagram Protocol (UDP). After the DDoS attack was completed, we started collecting the parameter's values from the log file, and

these results reflect the DDoS attack impact on system performance. Table 4-13 summarizes the final results.

Table 4-13: Parameters Values under DoS Attack

P	Pattern				Range		
	Mean	Median	Mode	Std.D	Range	Min	Max
CPU	31.90	31.40	30.90	6.26	47.30	6.80	54.10
Mem	10.14	10.20	10.20	0.27	1.80	9.70	11.50
Tasks	181.64	184.00	171.00	9.39	33.00	166.00	199.00
Threads	241.76	244.00	249.00	9.39	33.00	226.00	259.00
Voltage	4.98	4.98	4.98	0.00	0.01	4.98	4.99
Current	0.61	0.61	0.61	0.02	0.08	0.56	0.64
Temp	61.57	62.00	64.00	2.72	10.00	55.00	65.00

Based on the results that are shown in the above table, the CPU load reached 54.1% as the maximum percentage and the most frequent value is concentrated at 30.90%. The CPU utilisation values were also widely distributed from 6.80 to 54.10%. Thus, it reached 47.30 as the range of values distribution, reflecting the magnitude of the large fluctuation in performance and instability in the pattern. In terms of CPU performance, the following chart reflects the impact of the DDoS attack on the CPU utilisation pattern compared to the typical performance. The difference between typical performance and anomalous utilisation while the system is exposed to the DoS attack can be seen clearly based on Figure 4-14 (time in seconds). Also, Figure 4-15 shows the DoS attack's impact on CPU resources compared to typical utilisation in terms of minimum, average, and maximum values.

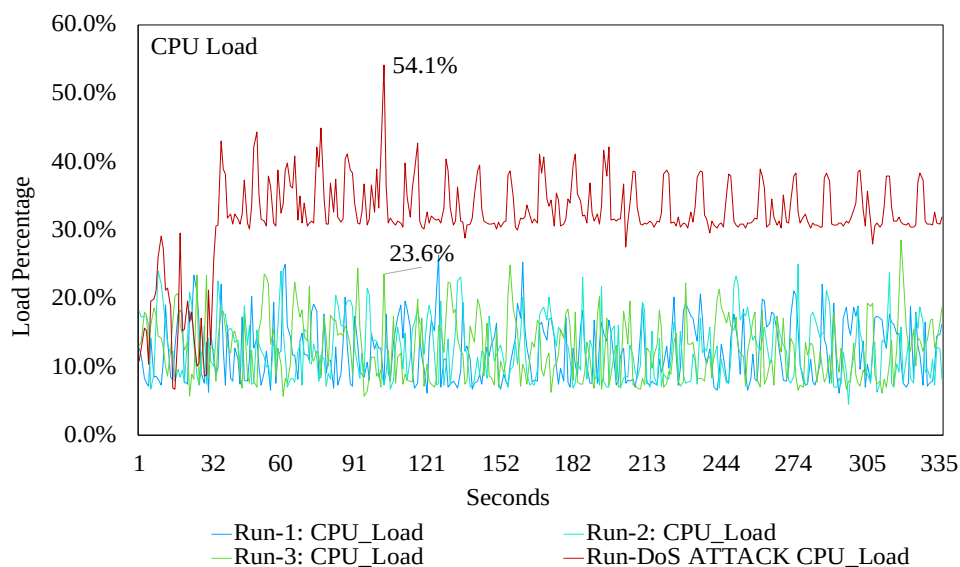


Figure 4-14. CPU load pattern DoS attack vs R1, R2, and R3

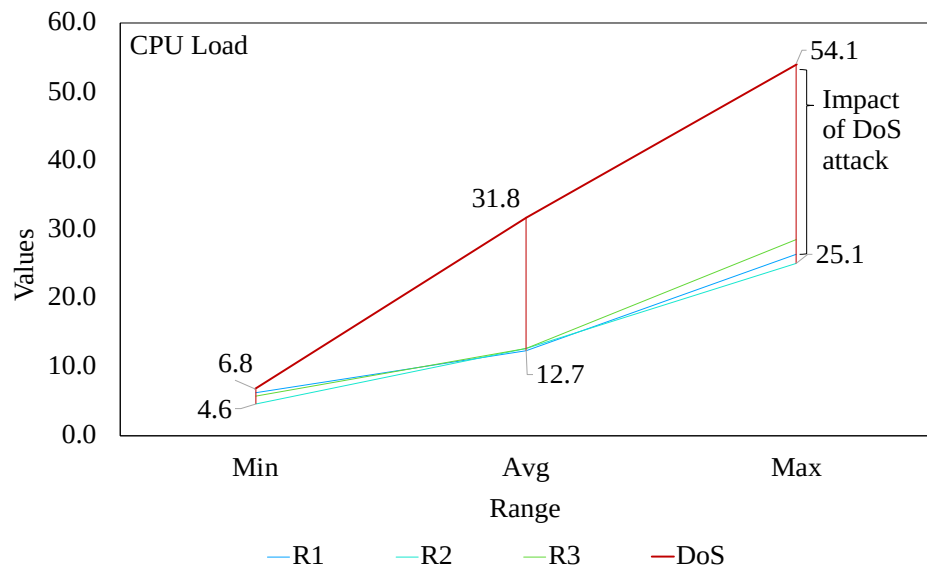


Figure 4-15. CPU range under DoS attack vs R1, R2, and R3

In terms of memory usage, the most repeated value was 10.20% (see Table 4-13) and the maximum value was 11.50%, while the minimal was 9.70%. The range of propagation or distribution of the consumption values was between 9.70% and 11.50%. These values reflect a clear difference compared to regular consumption in terms of range (M_r) and pattern (M_p). Figure 4-16 shows the impact of a DoS attack on memory resources.

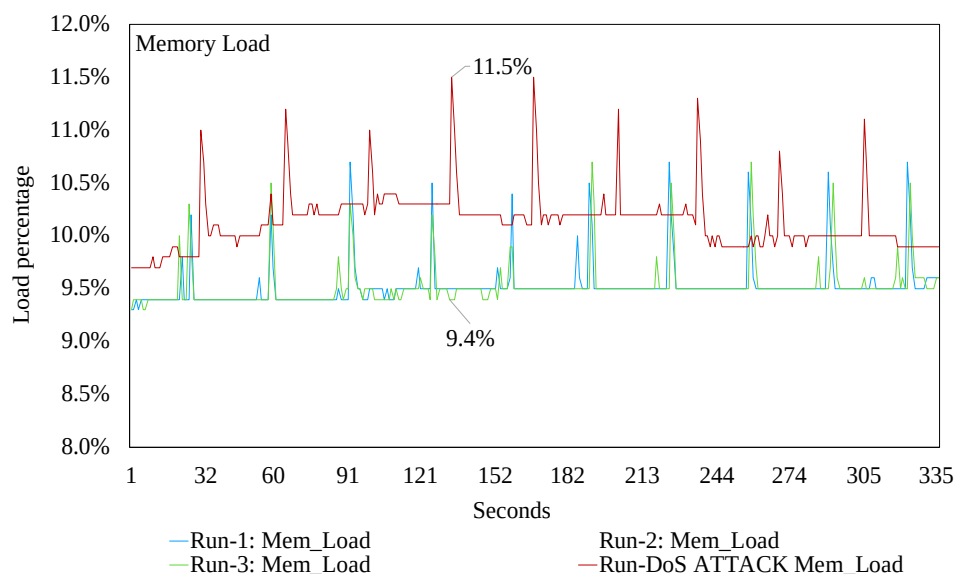


Figure 4-16. Memory load under DoS attack vs R1, R2, and R3

Tasks and threads are among the parameters whose values were collected during the testbed. These two parameters showed high accuracy in monitoring the performance of

the Smart PiCar, and even minor changes have been reflected in these parameters. Based on the values in Table 4-13, the most common value of alive tasks during the exposure of the ES to the DoS attack was 171 tasks, but the average value of alive tasks was 181.64. This was despite the concentration value or density point, which was 171 tasks per second, but due to the high fluctuation between the lowest value 166 and the highest value 199, and due to the wide distribution range of tasks number per second, which reached 30 processes as the difference between the lowest and highest value, an unbalanced and anomalous performance pattern has been formed and this is attributed to the abnormal activity.

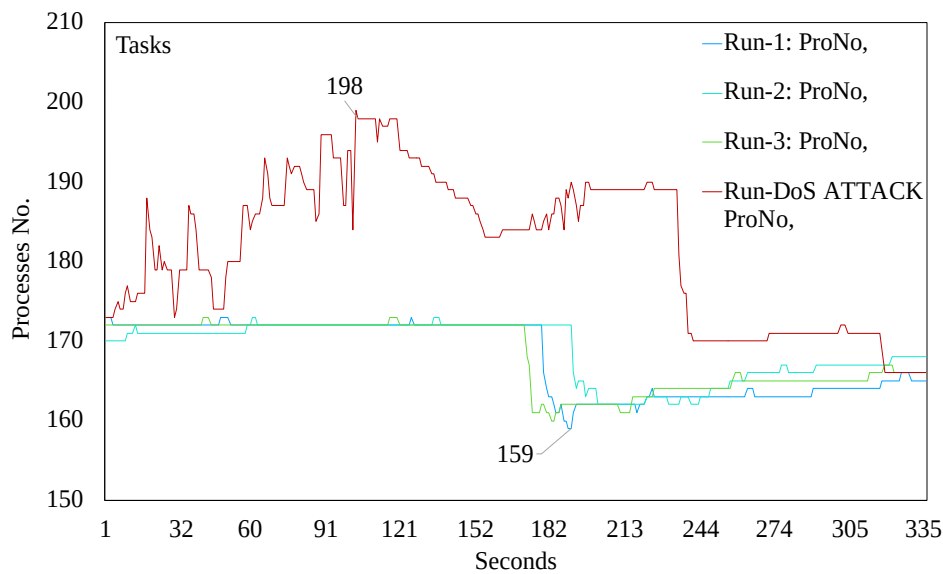


Figure 4-17. Tasks number under DoS attack vs R1, R2, and R3.

Also, it is worth mentioning that the most common value occurred and was recorded at the end of the DoS attack. While at the peak of the DoS attack, the impact caused a significant number of tasks until it reached 199 processes per second. Figure 4-17 demonstrates the anomalous performance of the Smart PiCar in terms of alive processes as a result of the DoS attack. Moreover, Figure 4-18 shows how the number of the tasks under the DoS attack diverge significantly from the N_r and N_p of R_s and Std cases, which is represented by the blue area in Figure 4-18.

Regarding the pattern of executed threads, the results did not differ from task patterns due to their relationship. The results showed that the number of executed threads at the peak of the DoS attack was 259 threads and the most frequent value was 249 threads. As with the value of the distribution range, the difference between the highest and lowest value

(33 threads) caused an abnormal and unstable performance pattern. Thus, this significant difference is considered an anomalous performance. Figures 4-19 and 4-20 show the effect that the DoS attack has had on the embedded system's performance in terms of executed threads per second. Based on Figure 4-20, we can see how the DoS attack's effect took the number of executed threads to unprecedented levels, which caused unfamiliar consumption and pattern. Thus, the threads' values have deviated significantly out of the blue area.

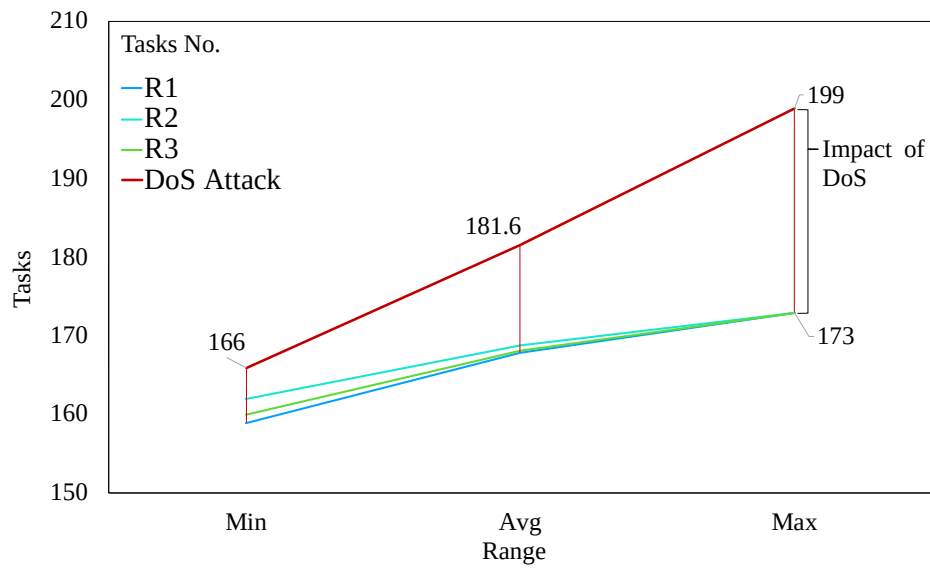


Figure 4-18. Tasks range (XgV) under DoS attack vs R1, R2, and R3

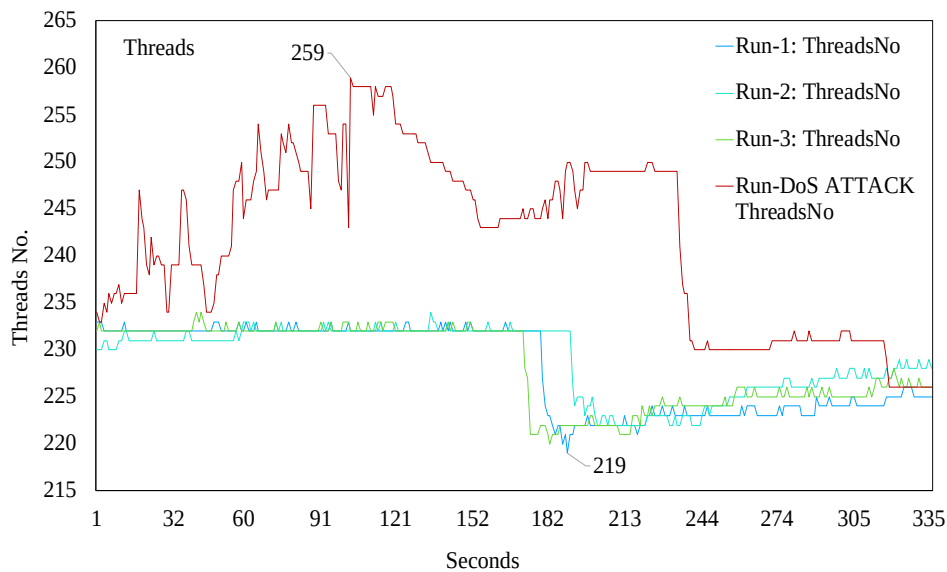


Figure 4-19. Threads pattern under DoS attack vs R1, R2, and R3.

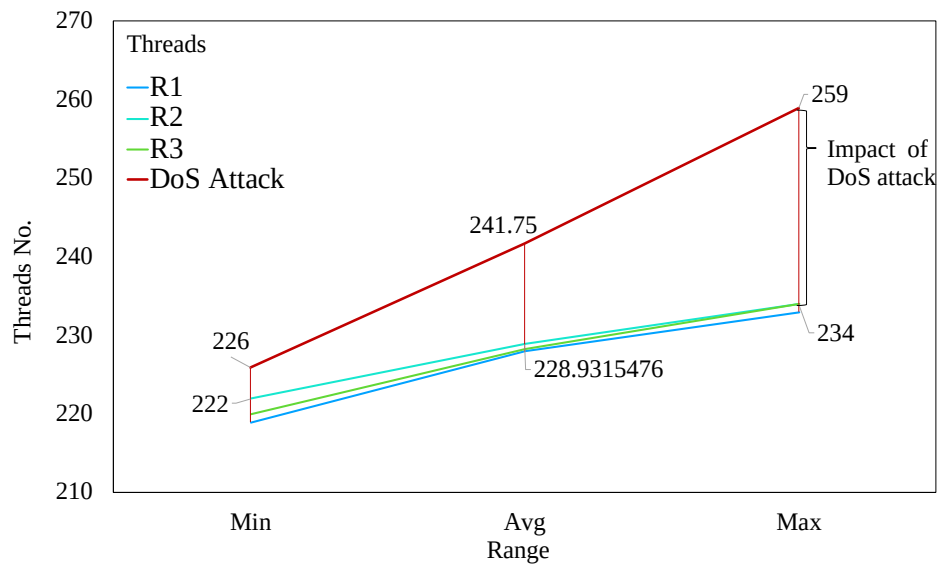


Figure 4-20. Threads range (XgV) under DoS attack vs R1, R2, and R3

Concerning voltage performance, an apparent deviation from the normal range is observed as shown in Figure 4-21. The reason for this anomalous power consumption is due to the effect of the DoS attack on the system's functions, as it was noted that the ultrasonic avoidance module was no longer functioning normally, and the connection with the administrator's device had become unstable as a result of the flooded traffic generated by the attacker.

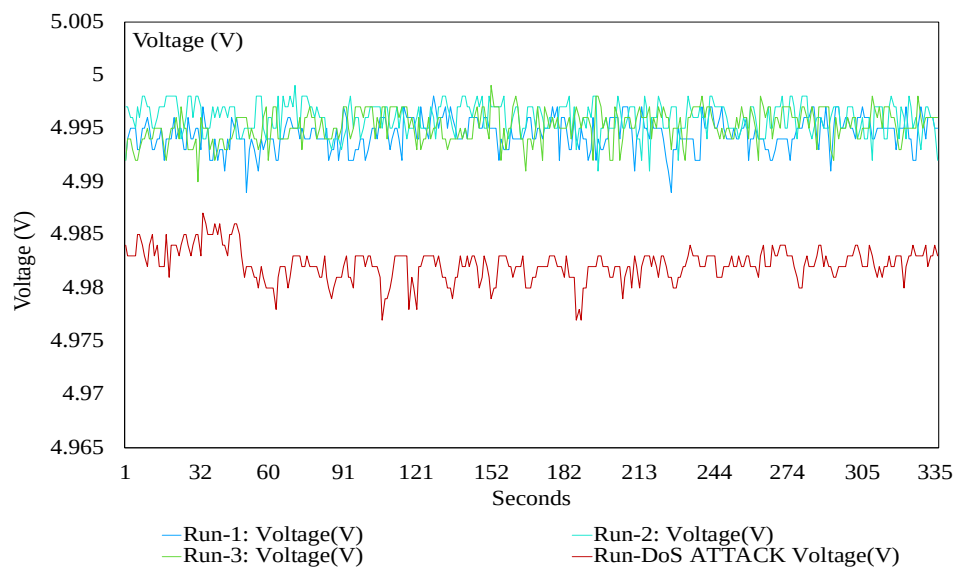


Figure 4-21. Voltage measurements under DoS attack vs R1, R2, and R3

Thus, this apparent decrease indicates the presence of an attack that disrupts the system's functions and that a significant voltage drop caused it. Accordingly, if we exclude any hardware deficiencies, we can infer the existence of an attack based on the unfamiliar consumed voltage pattern compared to the V_p in Rs cases. It was also noticed that the effect of the DoS attack was not evident in terms of the flow rate of electricity (current) except during the first few seconds of the attack, as shown in Figure 4-22. Thus, the significant interference in the current rate under conditions of attack or its absence makes this sub-parameter independently insufficient to predict and detect the attack because it did not achieve the anomalies and distinguishability principles. However, supporting this sub-parameter with other parameters' impacts will help clarify the anomalous pattern caused by the DoS attack. Figure 4-22 depicts the impact of the DoS attack in terms of current power consumption.

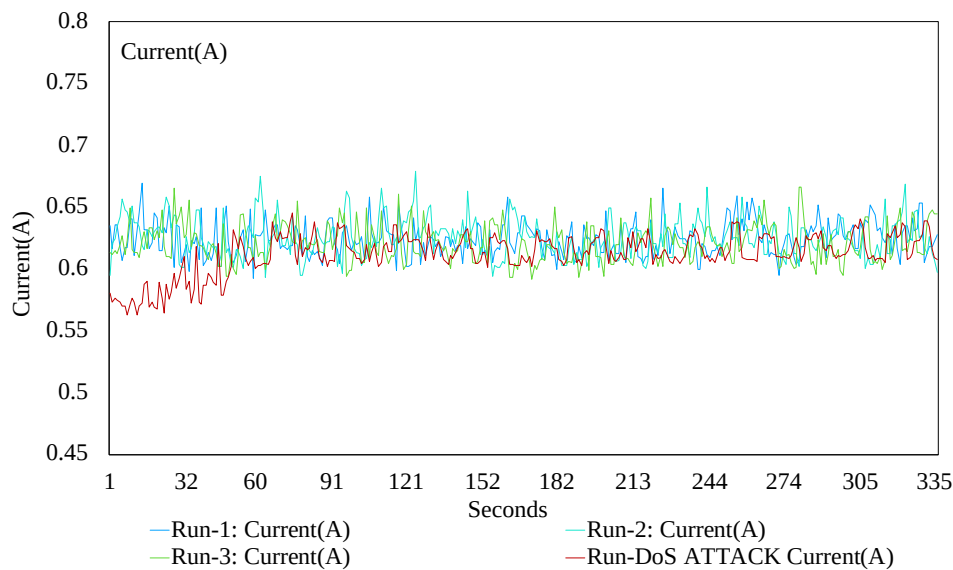


Figure 4-22. Current measurements under DoS attack vs R1, R2, and R3

The DoS attack's impact not only diminished on the direct parameters of system resources, but it impacted the temperature of the Smart PiCar processor (ARMv8). The CPU temperatures recorded abnormal values that were not observed previously under normal operating conditions. The initial temperature was 55°C, which is within the normal range, and the ambient temperature was 24°C, which was calculated to avoid any contribution by an external factor. The following figure shows the effect of the DoS attack on the processor temperature.

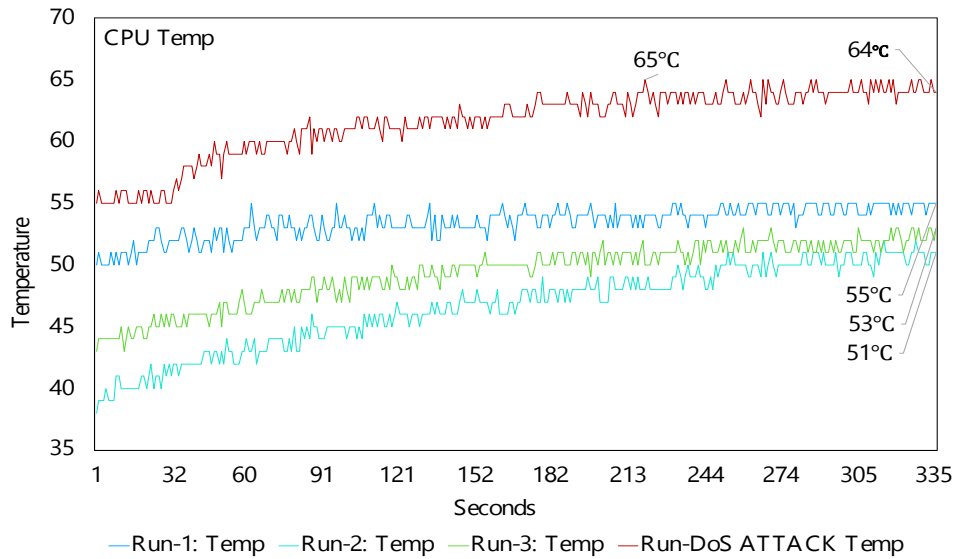


Figure 4-23. CPU Temp under DoS attack vs R1, R2, and R3

During the attack, the CPU temperature continued to increase significantly. The difference between the maximum recorded temperature and the ambient temperature reached 41°C. Thus, this is an anomalous value of CPU temperature compared to 31°C, 29°C, and 28°C for R1, R2, and R3.

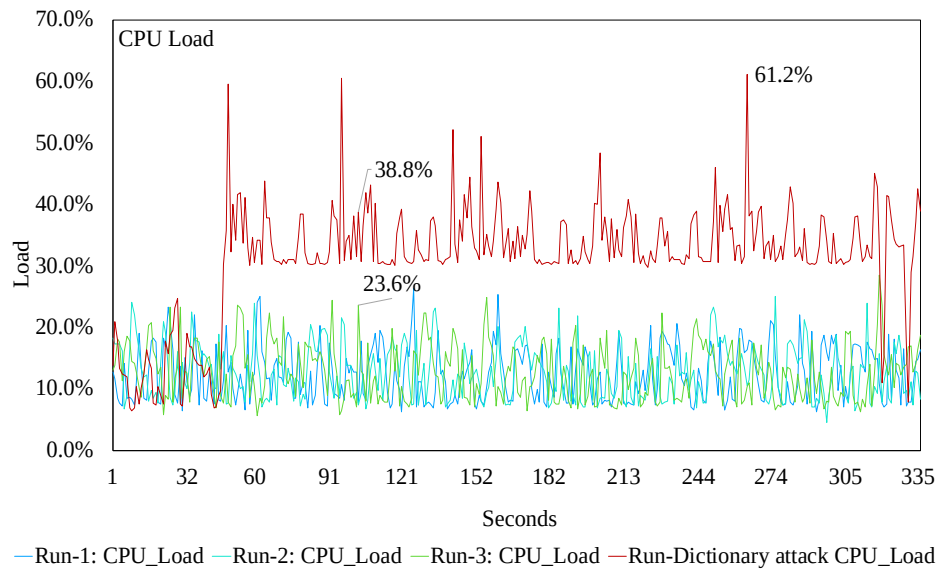
4.7.2. Password Attack (Brute-Force Attack)

According to the *Encyclopaedia of Cryptography and Security* [46], a dictionary attack describes a password-guessing technique in which the attacker attempts to determine a user's name or password by successively trying a compiled list of likely words, numbers, and symbols. In this test, "BruteDum" has been used as a brute-forcing tool. Within this tool, Network Mapper (Nmap) has been used for port scanning. After selecting a specific port, the SSH port has been selected for the attack purpose. The Hydra tool has been activated as a parallelized network logon cracker, supported with a random text password list. The initial expectation was that this type of attack would not have a monitorable effect or an indistinguishable impact. However, the obtained results after the attack was carried out are promising and auspicious for the effectiveness of the approach we are seeking to deliver. Table 4-14 summarizes the final results obtained after calculating the values of the statistical criteria for the septenary tuple model.

Table 4-14: Parameters Values under Brute-Force Attack

P	Pattern				Range		
	Mean	Median	Mode	Std.D	Range	Min	Max
CPU	31.16	31.50	30.50	9.13	54.70	6.50	61.20
Mem	9.78	9.60	9.60	0.33	1.90	9.40	11.30
Tasks	189.10	180.00	180.00	17.47	50.00	163.00	213.00
Threads	249.23	240.00	240.00	17.52	50.00	223.00	273.00
Voltage	4.99	4.99	4.99	0.00	0.01	4.99	5.00
Current	0.63	0.63	0.63	0.02	0.15	0.54	0.69
Temp	58.11	59.00	60.00	3.29	13.00	50.00	63.00

The results were as follows. In terms of CPU utilisation rate, the maximum usage was 61.20% and the most common value was 30.50. The minimum level was 6.50%. Thus, the range of distribution of values is vast, reaching 54.70. Also, the mean value is 31.16, which is close to the most repeated value. Figure 4-24 gives an impression of the effect that the password attack had on the Smart PiCar processor's performance compared to the typical patterns. Moreover, the standard deviation values of tasks and threads were significantly higher than the typical values in R1, R2, and R3. Therefore, this performance pattern of CPU utilisation diverges significantly from the standard range and pattern.

**Figure 4-24.** CPU load pattern under BF attack vs R1, R2, and R3.

The memory utilisation rate reached its highest limit at 11.30. This value had not been previously recorded under normal conditions. For the mean and mode values, the results were 9.78 and 9.60, respectively. Although these values overlapped within the normal

range Std_r of memory usage, the performance pattern appeared unfamiliar and anomalous compared to the standard pattern (Std_p), as shown in Figure 4-25. Furthermore, adding the anomalous patterns of other parameter impacts to this parameter will increase the attack recognition accuracy of detecting the existence of a password attack. Figure 4-25 depicts the impact of the password attack on memory usage.

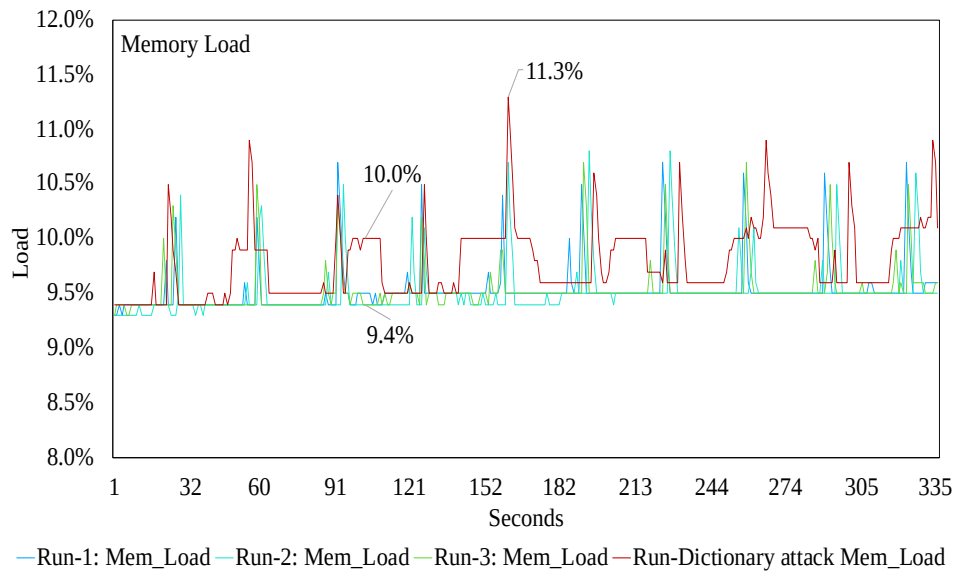


Figure 4-25. Memory load pattern under BF attack vs R1, R2, and R3

In terms of the executed number of processes and threads resulting from the password attack, the highest number of tasks reached 213 alive processes and the lowest number was 163 processes. Thereby, the attack distributed the number of the tasks into a large scale and caused an oscillating pattern. Likewise, the mode value was 180 and the mean was 189.1, which sharply deviated from the standard patterns and formed an anomalous pattern that was distinguishable. Figure 4-26 illustrates the executed task pattern under the password attack.

Regarding the pattern of executed threads, the similarity with the pattern of executed processes is clear, as shown in Figures 4-26 and 4-27. This similarity is due to their association with each other. Therefore, the tasks and threads patterns are heading in the same direction of anomalies, and these two parameters deviated from the standard pattern. Figure 4-27 shows how the threads pattern under the password attack differed from the normal range.

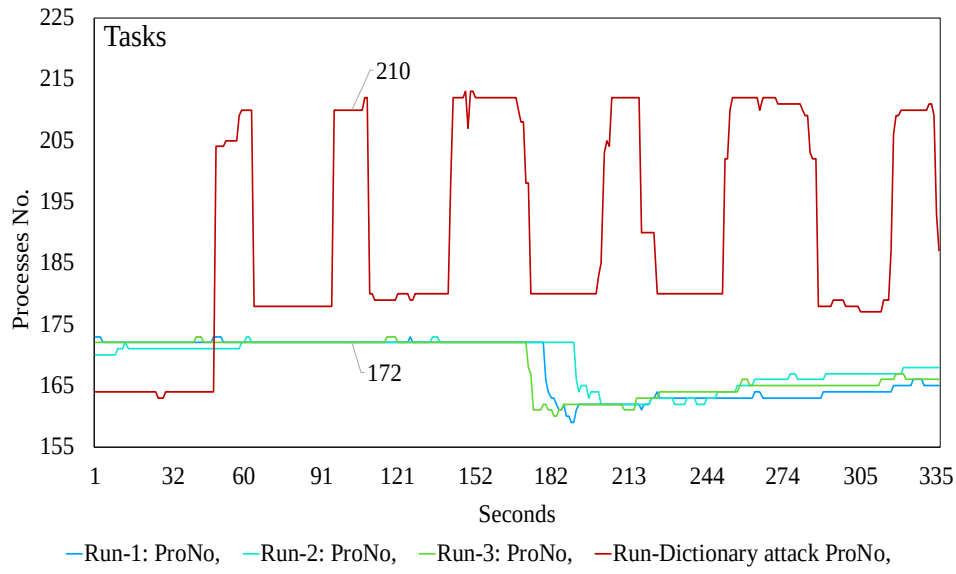


Figure 4-26. Tasks pattern under BF attack vs R1, R2, and R3

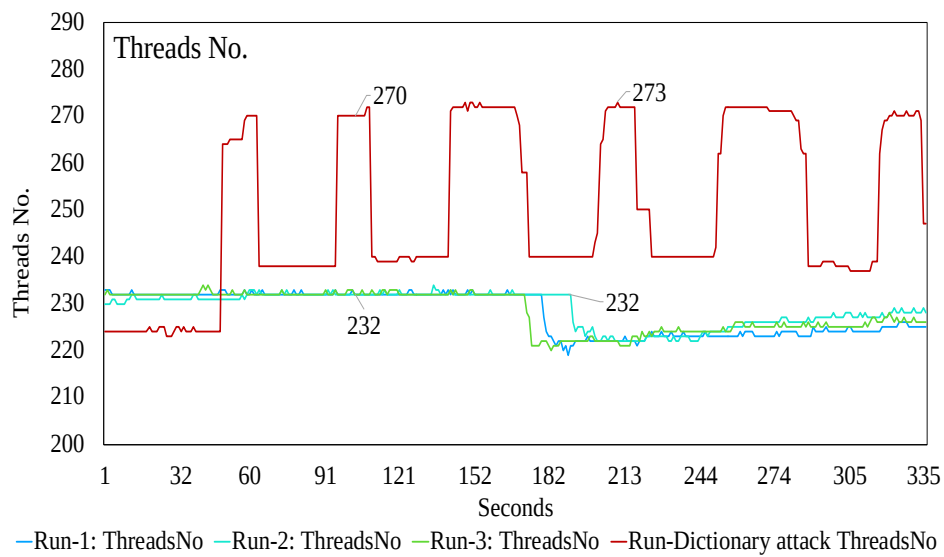


Figure 4-27. Threads pattern under password attack vs R1, R2, and R3

In terms of power consumption under the password attack, Figures 4-28 and 4-29 depict the password attack effect on the power consumption rate in terms of voltage or current. This pattern differs from the regular pattern and is similar to the impact pattern of the DDoS attack, especially in terms of voltage, which appeared decreased compared to typical patterns in R1, R2, and R3. Thus, the rate of anomalous consumption of power is a significant indicator that deserves attention. However, the decrease in voltage is not due to the cyberattack's direct impact, but instead to the attack's indirect effect on the

system's functions. Thereby, this deficiency in the system's functions has been reflected in the voltage and current patterns, indicating the existence of suspicious activities.

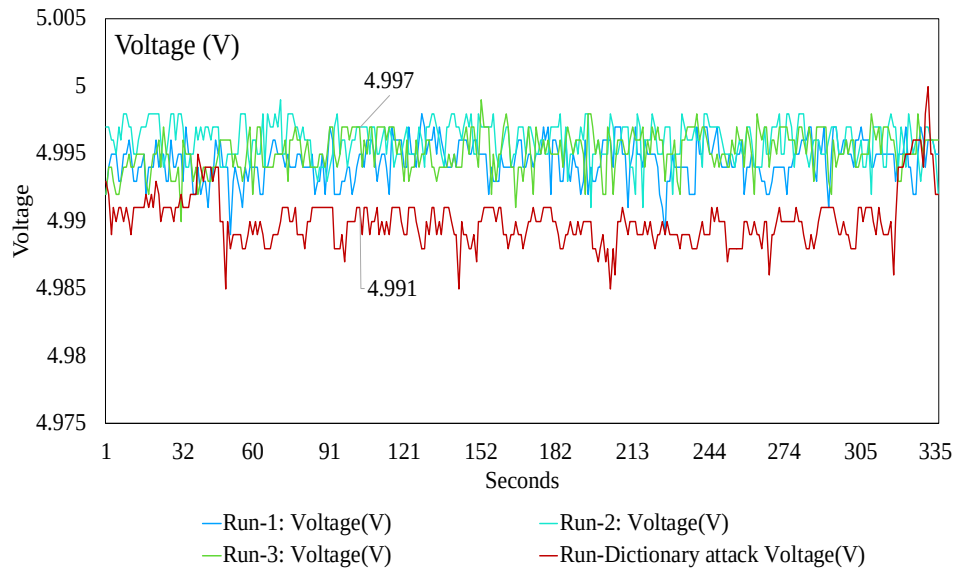


Figure 4-28. Voltage pattern under BF attack vs R1, R2, and R3

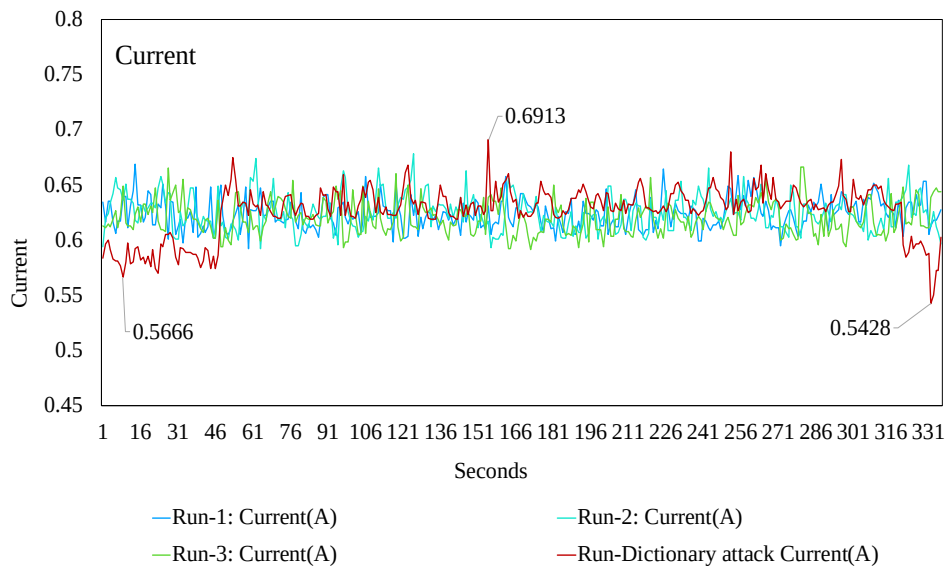


Figure 4-29. Current pattern under BF attack vs R1, R2, and R3

Regarding the effect of the password attack on CPU temperature, an increase in CPU temperature was observed. The CPU temperature under the attack differed from the typical patterns (T_p) in R1, R2, and R3. Thus, this abnormal pattern in temperature proved the existence of illegal activity that caused an increase in computing operations, which thus produced an increase in CPU temperature. Therefore, defining the pattern and range

of CPU temperature under normal operating conditions, taking into account the ambient temperature (25°C, in this scenario) and initial temperature (51°C, in this scenario) of the system, and monitoring any anomalous temperatures (63°C, as was recorded due to the attack impact) will contribute to predicting the presence of cyberattacks on the system. Figure 4-30 depicts the CPU temperature pattern under the password attack.

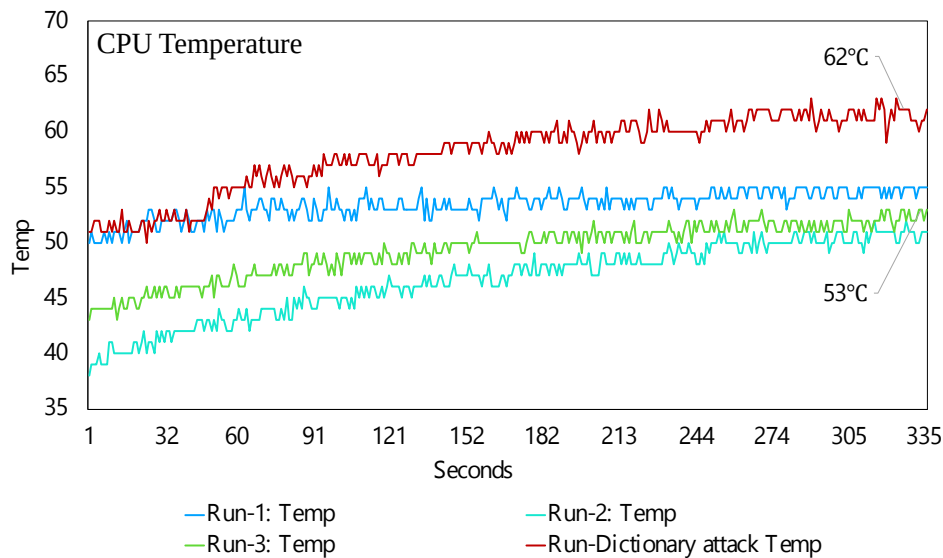


Figure 4-30. CPU temp under BF attack vs R1, R2, and R3

4.7.3. Remote Code Execution Attack (RCE)

The third attack scenario that was executed is the remote code execution attack (RCE). The RCE is an attacker's ability to gain unauthorized access to a remote device and execute malicious software. In other words, the attacker will run a local code to be executed remotely in the victim's device [47]. The following command was executed to generate this attack scenario:

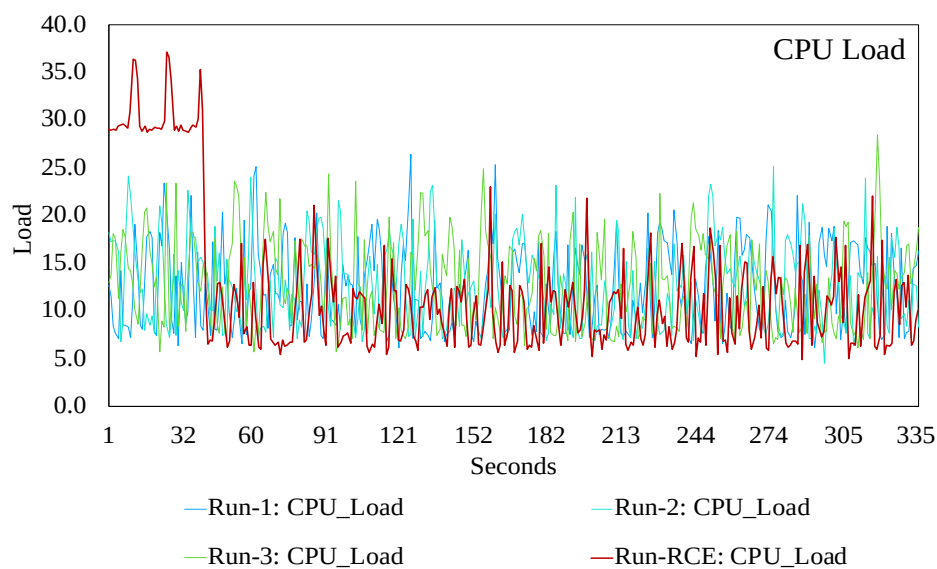
```
'sudo ssh pi@192.168.8.117 python -u - < cameraRemotly.py'.
```

As shown in this command's syntax, it consists of malicious software (*cameraRemotly.py*), written in Python language to intentionally cause damage to the Smart PiCar through its targeted IP address and disrupt one of its functions by disabling its Pi camera remotely. Table 4-15 shows the final results of the statistical criteria of the testbed's parameters under the RCE attack.

Table 4-15: Parameters Values under Remote Code Execution Attack

P	Pattern				Range		
	Mean	Median	Mode	Std.D	Range	Min	Max
CPU	12.33	10.40	6.20	7.51	32.20	4.90	37.10
Mem	9.90	9.90	9.90	0.00	0.00	9.90	9.90
Tasks	167.45	168.00	169.00	2.44	11.00	162.00	173.00
Threads	220.56	221.00	221.00	2.49	11.00	215.00	226.00
Voltage	5.00	5.00	5.00	0.00	0.01	4.99	5.01
Current	0.56	0.55	0.55	0.03	0.14	0.51	0.65
RX_pkt	3.99	1.00	0.00	5.26	27.00	0.00	27.00
TX_pkt	4.06	1.00	0.00	5.29	26.00	0.00	26.00
Temp	54.63	54.00	54.00	1.95	8.00	52.00	60.00

The most common value was 6.20% in terms of CPU utilisation, whereas the typical utilisation's mode values were between 7.5% and 7.9%. The mean value was 12.33% and the minimum and maximum values were 4.9 and 37.1, respectively, which created a wide distribution range and fluctuating performance, especially in the first few seconds of the RCE attack. Despite interference with the typical performance, a different CPU utilisation pattern had been shaped due to the RCE attack. For example, the U_{modV} values of CPU utilisation in R1, R2, and R3 was between 7.5% and 7.9%, while under RCE attack the mode value was 6.20%. Figure 4-31 illustrates the impact of the RCE attack on CPU utilisation compared to the typical patterns.

**Figure 4-31.** CPU load pattern under RCE attack vs R1, R2, and R3

As for memory usage percentage, the results that we obtained for this parameter are essential. Note that the range value is 0 and the lowest, highest, most frequent, and average values are identical (9.9%). This indicates the absence of any change in memory usage, which demands attention. The absence of change in memory usage indicates the absence of changeable activities, which indicates the presence of a defect resulting from a failure in one of the system functions. This failure can be inferred as an indicator of the presence of illegitimate activity, especially if we exclude any known manufacturer's defect. Disrupting the Pi camera function due to the RCE attack was evidently reflected in the values of this parameter. The irregular pattern of memory usage under the RCE attack and its impact on the memory usage rate compared to the typical patterns (M_p) are demonstrated in Figure 4-32.

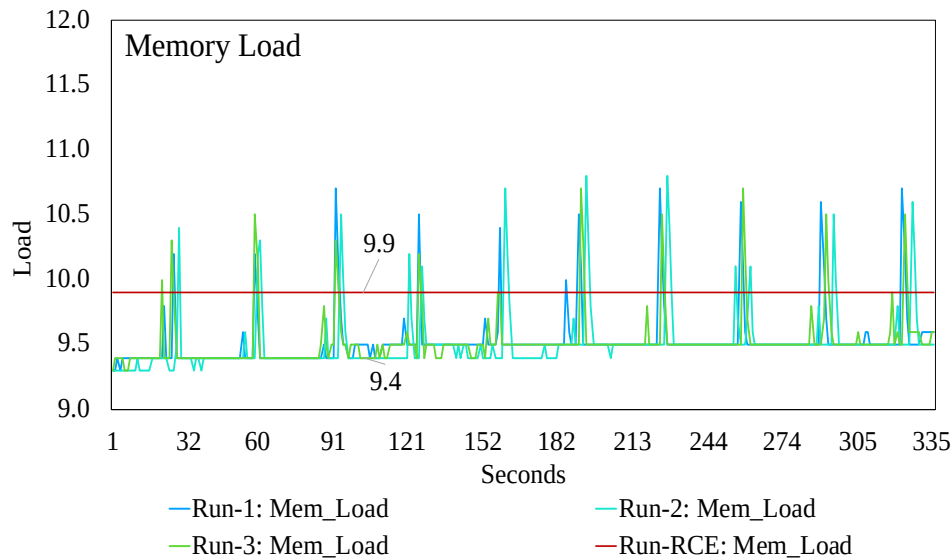


Figure 4-32. Memory load pattern under RCE attack vs R1, R2, and R3.

In terms of the number of executed processes under the RCE attack conditions, the most frequent value was 169 and the average was 167.45. The distribution range (X_{gv}) values reached 11 tasks as the difference between the lowest value (162) and the highest value (173). Figure 4-33 shows the anomalous pattern of this parameter compared to the typical performance.

Regarding the number of executed threads, the formed pattern resulting from the RCE attack is shown in Figure 4-34. This parameter's pattern was unfamiliar and deviates entirely outside the normal range, as at the beginning of the attack period the minimum

value was 215 threads, the maximum value was 226 threads, and the most frequent value (mode) was 221 threads. The following chart shows how the threads number under the RCE attack deviates from the typical patterns.

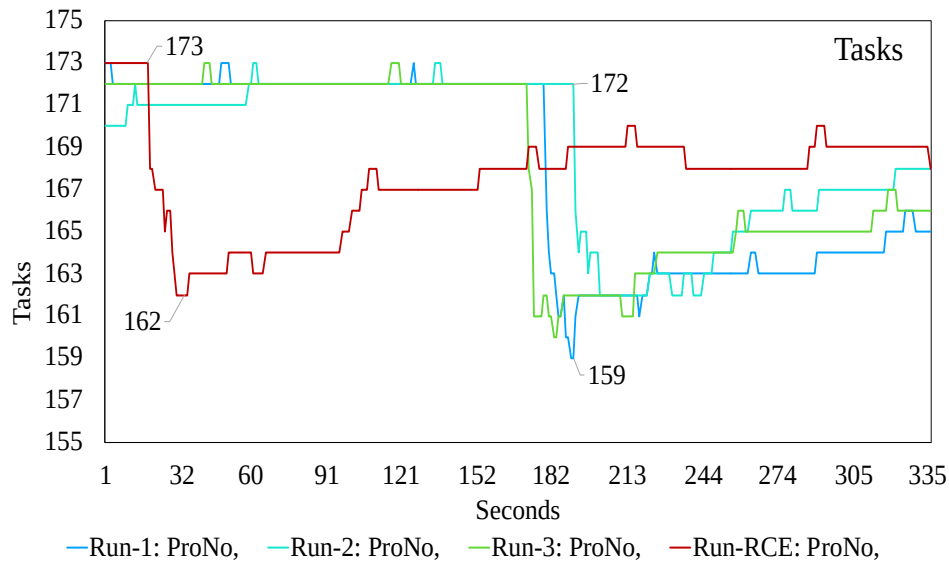


Figure 4-33. Alive tasks pattern under RCE attack vs R1, R2, and R3

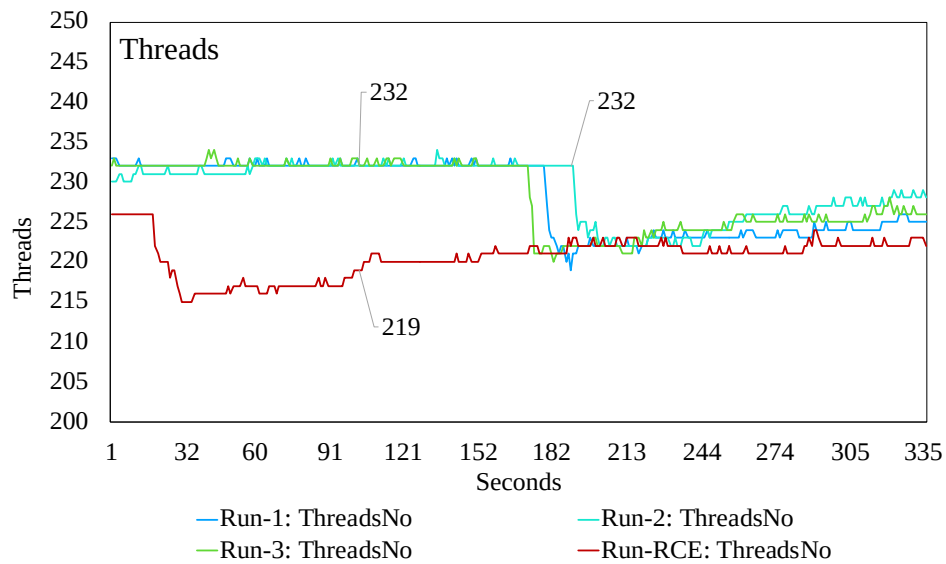


Figure 4-34. Threads pattern under RCE attack vs R1, R2, and R3

For the first time, change has appeared in both the voltage and current in terms of energy consumption. In the voltage, change has appeared in the form of an increase, while in the current it appeared in the form of a decrease. This is a crucial indication of the malfunction

of one of the system's functions, hereby detecting an attack depending on the anomalous energy consumption rate is an effective method, especially if this is done in addition to monitoring other parameters. Figures 4-35 and 4-36 show the abnormality of the power consumption and how it differed from the typical patterns.

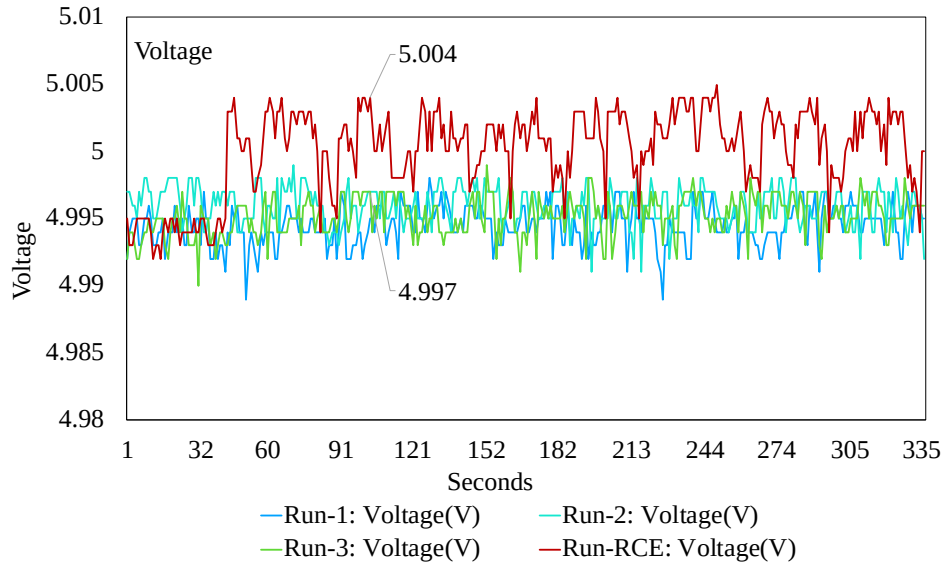


Figure 4-35. Voltage pattern under RCE attack vs R1, R2, and R3

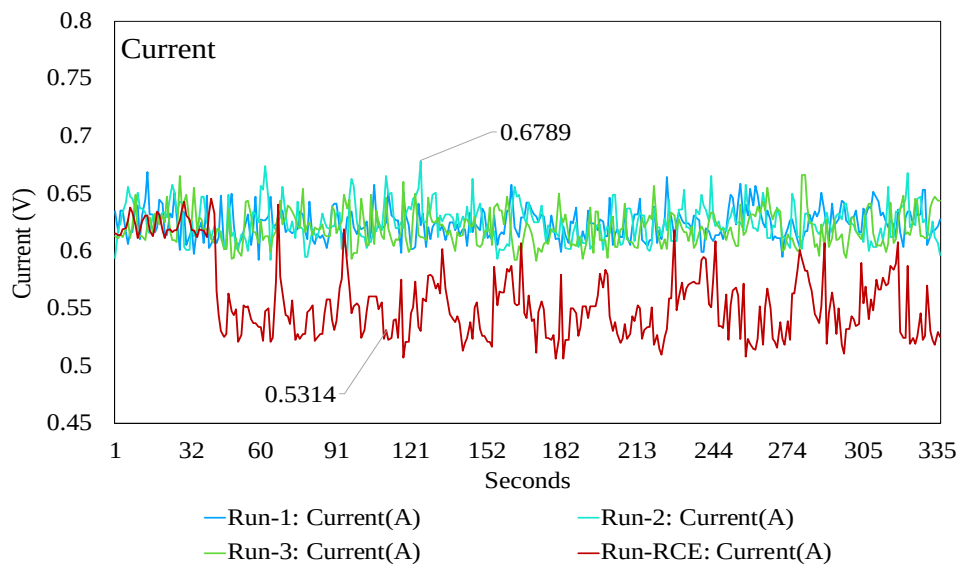


Figure 4-36. Current pattern under RCE attack vs R1, R2, and R3

In this attack scenario, transmitted and received packets have been monitored. Figures 4-37 and 4-38 show the effect of the RCE attack on the data traffic rate. Based on the analytical criteria, there was interference in the range but with a pattern difference. The

slight abnormality or anomalous pattern in transmitted and received packets will support the distinguishability between typical and anomalous traffic, especially if the other parameters' impacts have been considered. In this attack case, the impact might not be noticeable enough in this parameter as it will be in the next scenario. Furthermore, this kind of parameter might help in determining the type of attack as a network attack. For example, in a packet drop attack or blackhole attack [48], anomalous change in the expected predetermined packets volume can lead to the detection of this kind of attack based on this parameter.

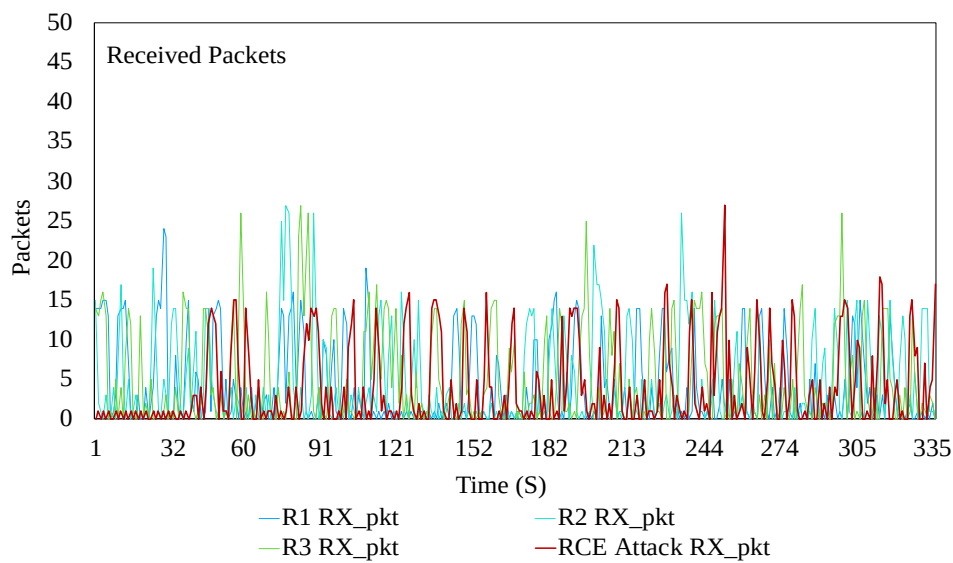


Figure 4-37. Received packets rates under RCE attack vs R1, R2, and R3.

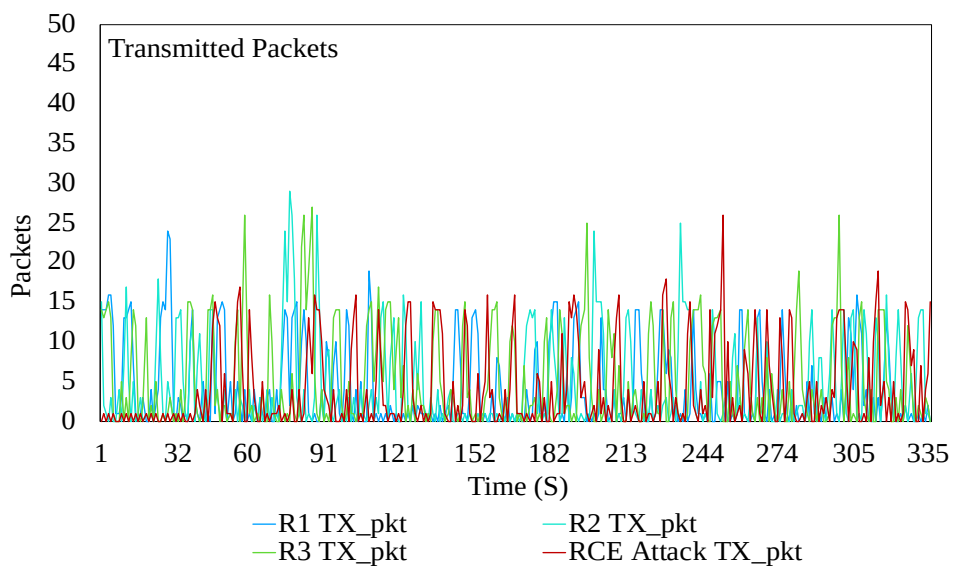


Figure 4-38. Transmitted packets rates under RCE attack vs R1, R2, and R3

Concerning CPU temperature under the conditions of this type of attack and after considering the initial (59°C) and ambient (25°C) temperatures, it is noticeable that disabling one of the embedded system's functions due to the attack was reflected by the CPU temperature. This reflection has complicated the possibility of predicting the existence of a cyberattack based on this parameter alone. Therefore, the decrease in computing operations caused a decrease in CPU load, allowed the CPU temperature to decrease. It is worth noting that this decrease placed the temperature within the range of familiar patterns (T_p). Thus, it is impossible to rely on this parameter to infer the anomalous pattern that indicates a cyberattack's existence. However, this observation is based on a relatively short period. Thus, a long operational period might show a different pattern of CPU temperature if the attack is held for a while, causing a significantly noticeable decrease due to function failure. The following figure depicts the impact of the RCE attack on CPU temperature.

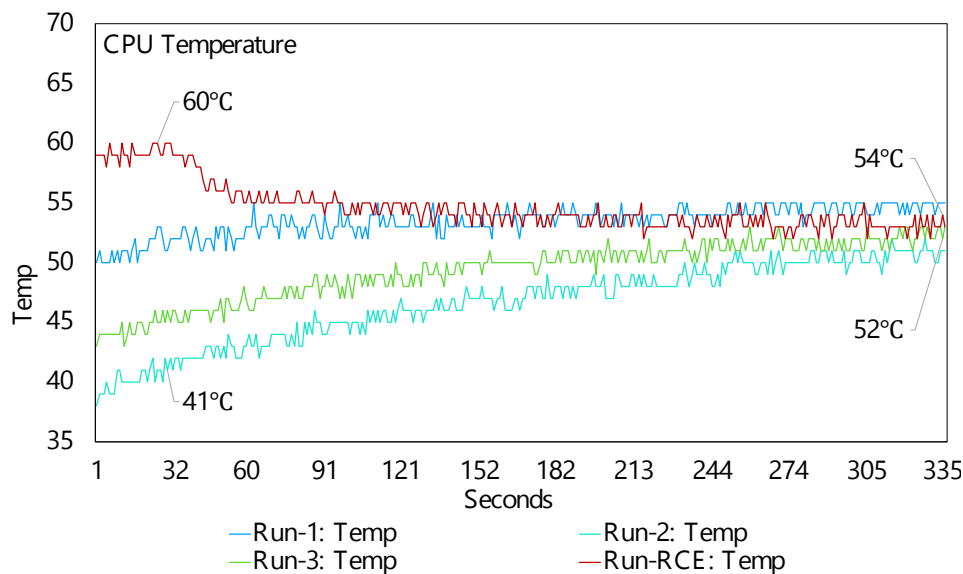


Figure 4-39. CPU temp under RCE attack vs R1, R2, and R3

4.7.4. Man-in-the-Middle Attack (MITM) Remote Command Execution

In this attack scenario, the attacker not only disabled the recording function of the equipped Pi camera, but also redirected the camera broadcast to their device by executing a remote command, which is known as a remote command execution attack. This attack type differs from the remote code execution attack, which had been executed in the previous scenario. By executing the following command in terminal:


```
'raspivid -o - -t 0 -w 960 -h 540 | cvlc -vvstream:///dev/stdin --sout
'#rtp{sdp=rtsp://:8554/}' :demux=h264'
```

The adversarial will gain unauthorized streamed video. Furthermore, the passive repetition of this illegitimate activity, without harming the system (only eavesdropping), will make the attack an advanced persistent threat (APT). During the attack period, the testbed's parameters were monitored and the final results of the analysis criteria are shown in Table 4-16.

Table 4-16: Parameters Values under MITM Attack

	Pattern				Range		
	Mean	Median	Mode	Std.D	Range	Min	Max
CPU	15.87	12.60	7.40	9.05	33.60	5.30	38.90
Mem	10.50	10.50	10.50	0.01	0.10	10.50	10.60
Tasks	171.79	173.00	173.00	1.70	10.00	167.00	177.00
Threads	239.89	241.00	241.00	1.78	10.00	235.00	245.00
Voltage	4.99	5.00	5.00	0.00	0.02	4.98	5.00
Current	0.62	0.61	0.61	0.03	0.17	0.53	0.69
RX_pkt	7.79	3.00	0.00	10.37	55.00	0.00	55.00
TX_pkt	284.29	307.00	1.00	148.68	645.00	1.00	646.00
Temp	56.15	56.00	55.00	1.34	6.00	54.00	60.00

In terms of CPU utilisation, the most common value under these conditions was 7.40%, while the mean value is 15.87%. The lowest value was 5.30% and the highest value was 38.90%. The general pattern of CPU utilisation was fluctuating and anomalous in comparison to the Std_p pattern. Figure 4-40 gives a clear vision of the CPU utilisation pattern under this attack, and it shows how the CPU performance pattern of the attacked scenario differs from the typical patterns (U_p) in R1, R2, and R3.

In terms of memory usage, a steady and high pattern of memory usage has been observed, and this steadiness is abnormal in this case. Also, the standard deviation value was 0.01 compared to 0.2 in Rs cases. The mode and mean values were stable at 10.50%. This performance pattern's steadiness appeared utterly different from the typical patterns (M_p) in Rs cases due to the MITM attack. Figure 4-41 illustrates the memory performance patterns under the attack and typical operational circumstances.

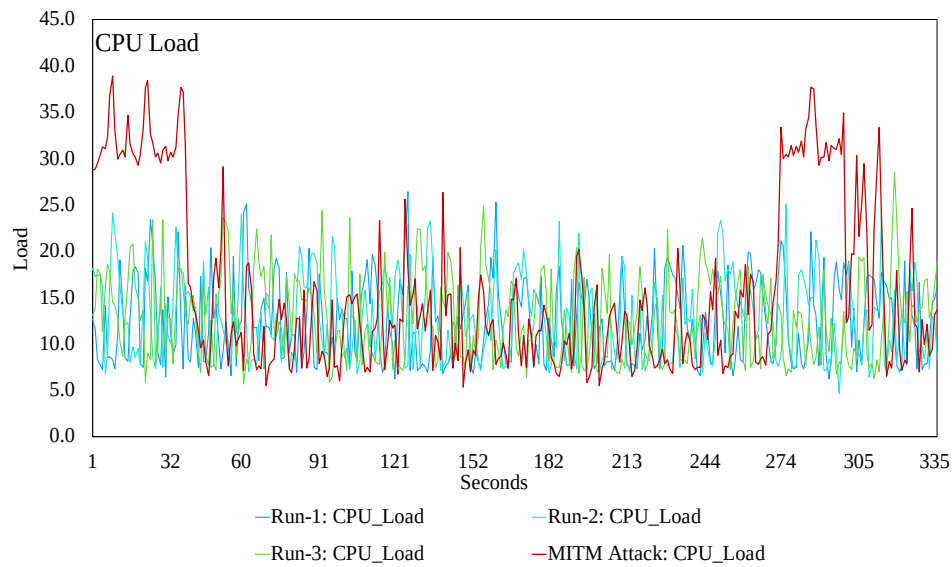


Figure 4-40. CPU load pattern under MITM attack vs R1, R2, and R3

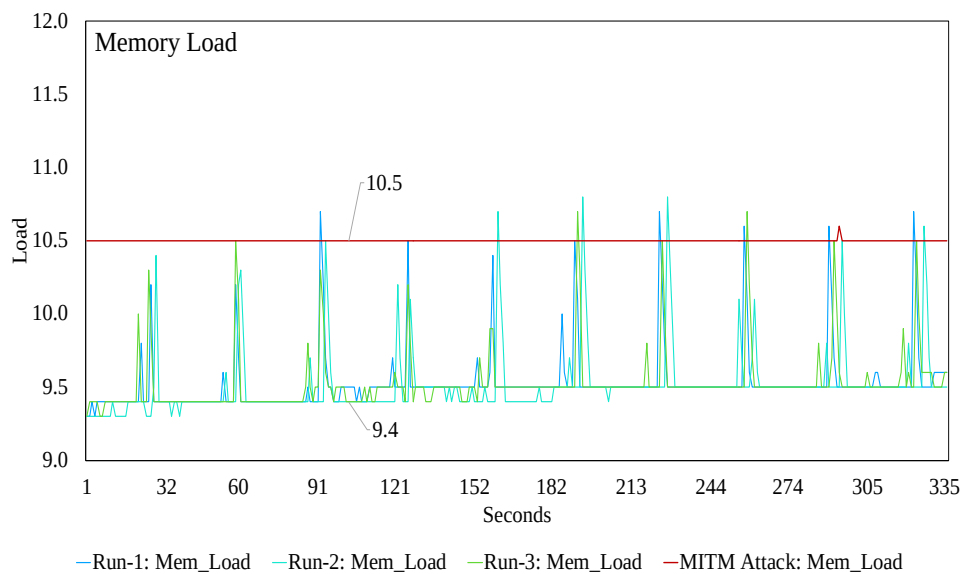


Figure 4-41. Memory load pattern under MITM attack vs R1, R2, and R3

In terms of the number of tasks executed per second, Figure 4-42 shows the pattern of the executed tasks/s, which ranged from 167 to 177 tasks/s, with 173 the most common value (mode). Although there was interference within the typical ranges (N_p), the anomalies in the executed tasks pattern under the MITM attack were sufficient to characterize the tasks pattern as an anomalous performance pattern, thus shaping an abnormal pattern with the system performance indicating the presence of an attack. Therefore, this situation

facilitates the ability to detect the attack based on the attack's impact on system performance. The following figure depicts the pattern of this parameter under the MITM attack.

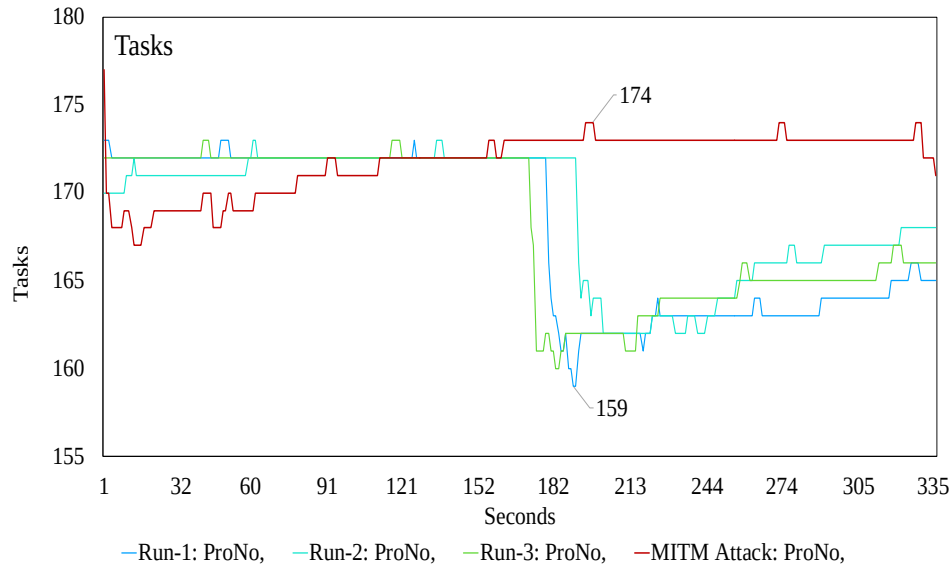


Figure 4-42. Tasks pattern under MITM attack vs R1, R2, and R3

Although there was interference within the Std_r , the abnormality in this pattern was sufficient to characterize the performance as an anomaly performance due to the presence of the MITM attack. Hence, this situation facilitates the ability of detection when making a comparison to the supposed performance.

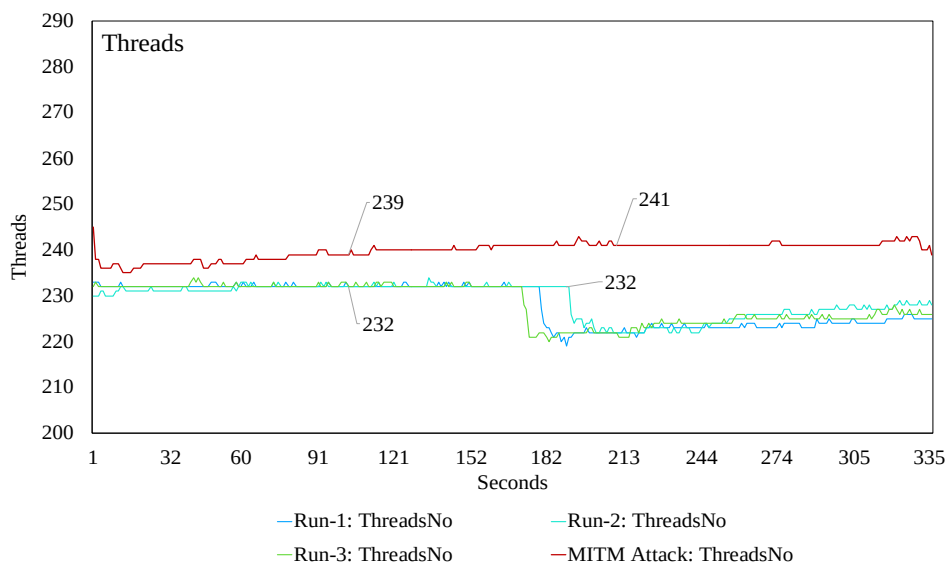


Figure 4-43. Threads pattern under MITM attack vs R1, R2, and R3

Regarding the number of executed threads, the pattern formed from the attack is shown in Figure 4-43. It was unfamiliar and deviated entirely outside the normal range ($\mathcal{G}_r$) as its minimum value was 235 threads, which is higher than the maximum value in the normal operation conditions (234 threads). The mode value was 221 threads and the maximum number of executed threads was 245. Overall, this parameter's pattern is categorized within the anomaly patterns compared to R1, R2, and R3, as illustrated in the following figure. Regarding the change in power consumption under the MITM attack conditions, it was noted that the change was more pronounced in the pattern rather than range.

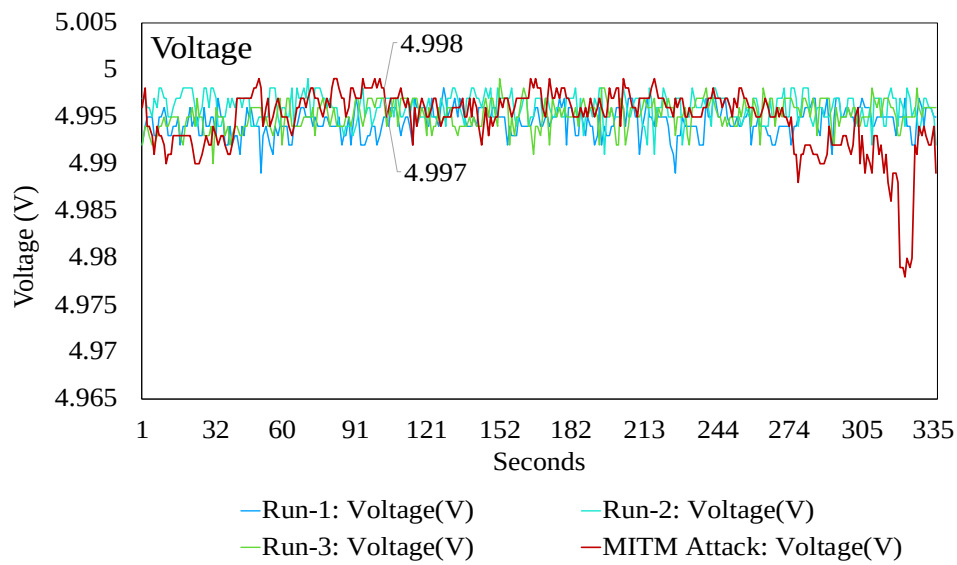


Figure 4-44. Voltage pattern under MITM attack vs R1, R2, and R3.

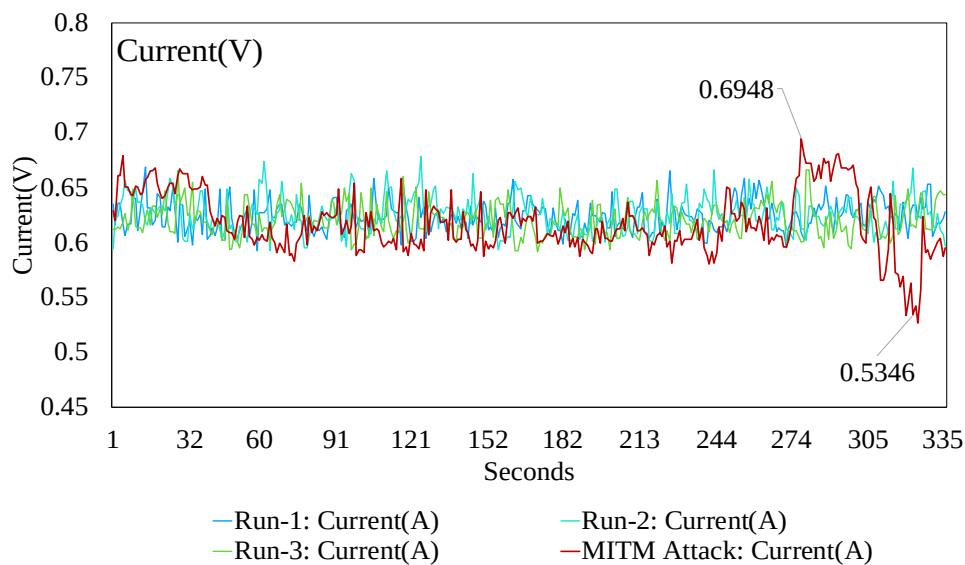


Figure 4-45. Current pattern under MITM attack vs R1, R2, and R3

The consumption rate of V and I during the attack was intertwined with the normal P_p but differently. At the end of the period, there was a sharp fluctuation due to the MITM attack's impact. In terms of voltage mode, minimum and maximum values were 5_V , 4.98_V , and 5_V , respectively. In terms of the current rate, the mode was 0.61_A and the minimum and maximum values were 0.53_A and 0.69_A , sequentially. Figures 4-44 and 4-45 demonstrate the impact of the MITM attack on this parameter P (V and I).

In terms of the data traffic rate under the circumstances of the MITM attack can be observed through Figures 4-46 and 4-47 that the patterns have changed dramatically, which confirms the presence of illegitimate activity.

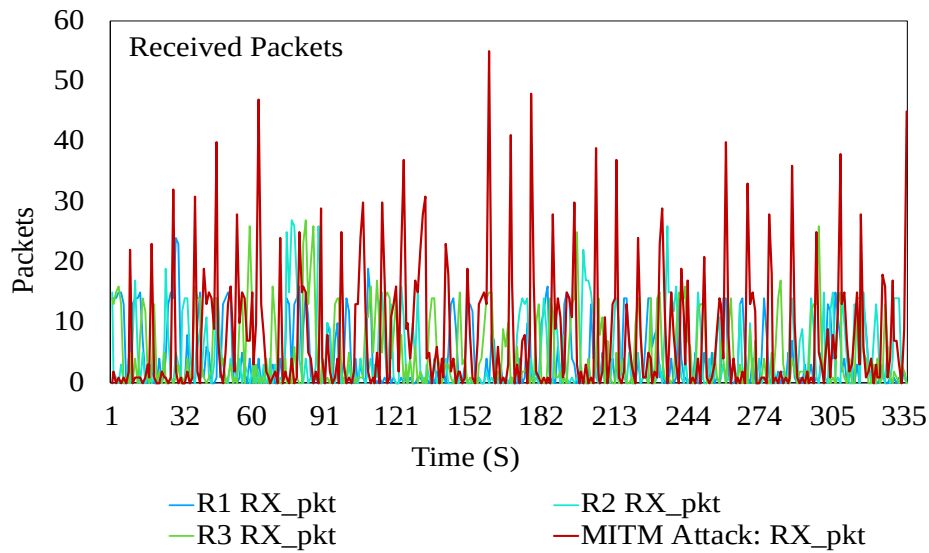


Figure 4-46. Received packets rates under MITM attack vs R1, R2, and R3

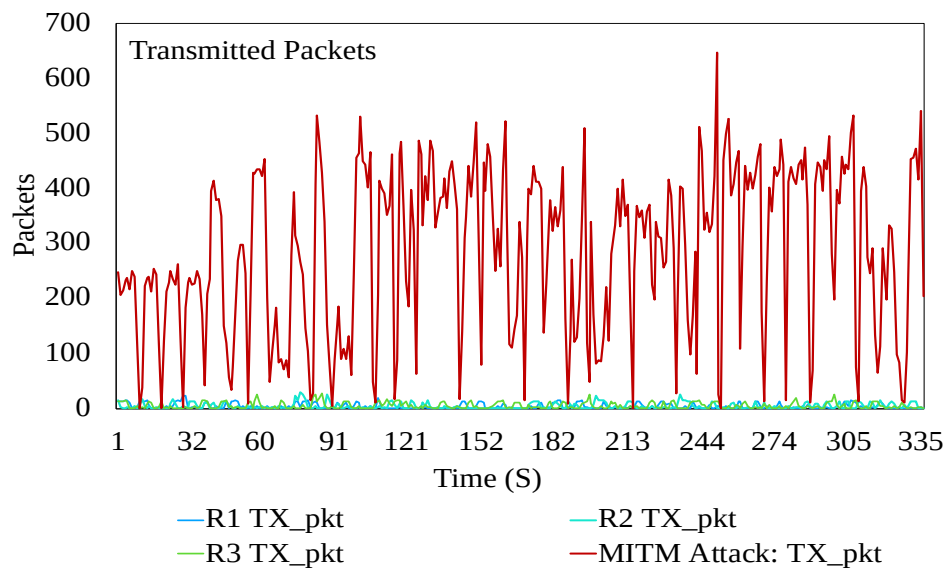


Figure 4-47. Transmitted packets under MITM attack vs R1, R2, and R3

Also, the analysis criteria (*mean*, *mode*, *median*, *std.d*, *range*, *min*, and *max*) for TX/RX packets showed a significant difference and the results deviated significantly outside the normal standard range (Std_r), as well as in the pattern (Std_p), especially in terms of transmitted packets number. The mean value of the transmitted packets under the conditions of this type of attack was 284.29 packets, while the TX_{avgV} in Rs cases was between 4 to 5 packets/s, which is considered an enormous amount of data compared to the typical transmission rates (TX_r and TX_p) in Rs cases, proving undoubtedly the existence of unauthorized activities.

Regarding the CPU temperature pattern under the attacker's influence (as the attacker redirects the camera back to his device), the temperatures were close to the typical ranges but relatively anomalous in the pattern. The most common temperature was 55°C, the maximum was 60°C, the minimum was 54°C, and the average value was 56.15°C. In the first and last seconds of the attack, the CPU temperature increased for a short period, forming a different pattern from the usual pattern. Altogether, adding this parameter pattern to other parameters' impacts will enable the detection of the cyberattack's presence. Figure 4-48 summarizes the CPU temperature pattern in this attack scenario compared to other typical patterns. The initial temperature was 55°C and the ambient temperature was 25°C.

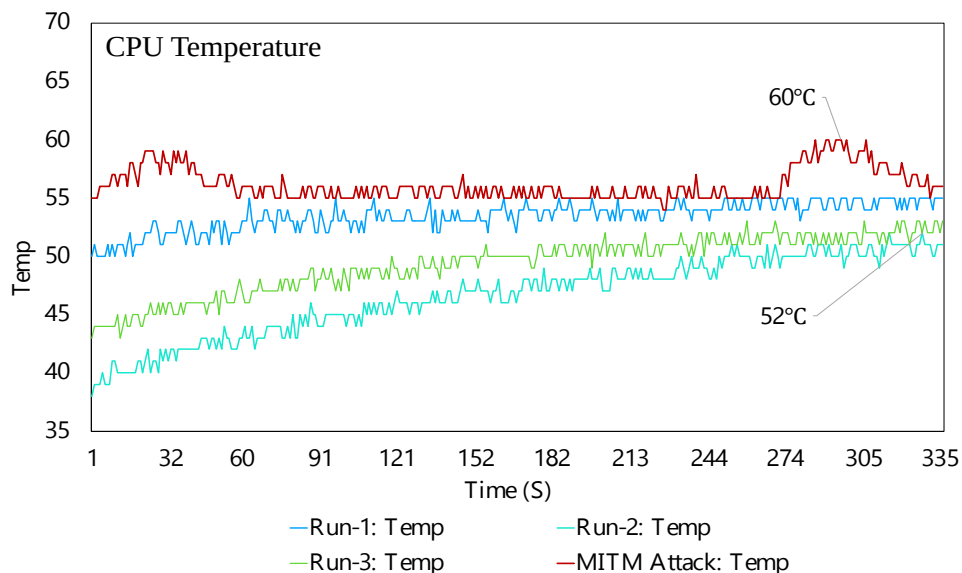


Figure 4-48. CPU temp under MITM attack vs R1, R2, and R3

4.8. Detection Latency

In terms of detection latency, to find out the estimated time to detect the attack based on the proposed approach, the time-series of two attacked scenarios have been revised: DoS and password attack, and relevant insights have been presented. Based on the results shown in Table 4-26, and Table 4-27, the DoS attack was executed at 00:26:25, and the anomalous pattern started to form at 00:26:26.

Table 4-17: Timestamps During Dos Attack

T. Stamp	Temp	CPU	Mem	Tasks	Threads	RX	TX
00:26:16	60	19	10.3	167	228	11	12
00:26:17	60	17.1	10.3	167	227	12	10
00:26:18	61	22	10.3	167	228	11	10
00:26:19	60	23.3	10.3	167	227	11	11
00:26:20	60	21.6	10.3	167	227	12	10
00:26:21	60	17.3	10.3	167	228	11	10
00:26:22	59	17.7	10.3	167	227	11	19
00:26:23	61	17.9	10.3	167	227	11	13
00:26:24	60	16.9	10.3	167	227	11	10
00:26:25	60	16.3	10.3	167	227	13	11
00:26:26	62	65.4	11.3	167	227	1449	700
00:26:27	60	47.4	11.9	261	326	4737	2974
00:26:28	60	23.9	11.9	267	327	2308	1575
00:26:29	60	21.3	11.9	267	327	1675	930
00:26:30	60	17.6	11.9	267	328	28	30

Time-series of DoS attack

00:26:24	Normal Pattern.
00:26:25	The attack was launched.
00:26:26	The threshold of anomalies, (first outlier values).
00:26:27	Anomalous pattern formation

Also, at 00:16:16s, the password attack was executed, and at 00:16:18s, the anomalous pattern began to appear. Therefore, detecting attacks based on this approach is an efficient method. However, the formation of the anomalous pattern is also related to other factors that might have an influence, i.e., the type of attack, the architecture of the operating system, and the computing capabilities of the ES.

Table 4-18: Timestamps during Password attack

T. Stamp	Temp	CPU	Mem	Tasks	Threads	RX	TX
00:16:08	55	7.1	9.9	172	232	2	2
00:16:09	55	6.8	9.9	172	232	1	0
00:16:10	56	7.9	9.9	172	233	2	2
00:16:11	56	8.5	10.3	172	232	1	1
00:16:12	55	10.6	10.7	173	233	2	2
00:16:13	56	8.1	10.3	173	233	1	0
00:16:14	56	7.5	9.9	173	233	2	1
00:16:15	57	13	9.9	173	234	1	0
00:16:16	56	13	9.9	173	233	1	1
00:16:17	57	14.6	9.9	173	233	15	12
00:16:18	57	47	10.3	173	233	216	211
00:16:18	57	5.6	10.3	205	265	2	2
00:16:19	57	7.9	10.3	203	263	1	0
00:16:20	55	10.4	10.3	203	263	2	1
00:16:21	57	7.2	10.3	203	263	1	0

Time-series of Password attack

00:16:15	Normal Pattern.
00:16:16	The attack was launched.
00:16:18	The threshold of anomalies, (first outlier values).
00:16:18	Anomalous pattern formation

Returning to the starting point from which we started (the hypothesis of the study) and based on our final results, we can confirm the validity of the hypothesis where cyberattacks against embedded systems can be detected according to our proposed approach. By delivering this approach, we have paved the way for software engineers to augment OS robustness by adding a protective layer to prevent cyberattacks based on a new perspective, which is the statistical analysis of the septenary tuple model. More details about the results of the experiment are discussed in the discussion chapter.

4.9. Conclusion

Embedded systems differ from typical computer systems given that they are designed to perform specific functions. In this context, we proposed a new security approach for detecting cyberattacks based on the recognition of anomalous resource consumption and performance patterns of an embedded system. In particular, a septenary tuple of a parameter

model, consisting of CPU utilisation, memory load, tasks, threads, data traffic rate, temperature, and power consumption, is presented as the detection mechanism. The data has been collected through the repetitive operation of a test model, i.e., Smart PiCar, where the collected data has been analysed in terms of seven statistical criteria, i.e., mean, median, mode, standard deviation, range, minimum, and maximum. The final result illustrated there exists a pattern of resource consumption and performance of embedded systems that can be defined as a standard pattern due to a distinctive feature (ESs are dedicated to performing specific functions), providing a baseline on which the pattern of normal states of an embedded system can be determined and utilized as a reference profile to detect anomalous patterns.

In contrast, the anomalous patterns of the Smart PiCar performance under different cyberattacks (denial-of-service, password, remote code execution, and man-in-the-middle) have clearly appeared and been observed. These anomalous patterns differ from the typical normal pattern.

The experimental results prove the efficacy of the ARCD approach. Thus, this approach enables software engineers to improve the OS layer of the ESs. By creating a recognition mechanism against cyberattacks based on resource consumption and performance patterns, the OS layer of an ES could secure regular consumption and respond to cyberattacks once an anomalous pattern occurs.

Furthermore, the raw data enabled us to develop a machine learning model by using the support vector machine algorithm to determine the prediction accuracy percentage in terms of separating anomalous patterns from typical patterns, forming our future task. The outcomes of computational validation based on machine learning algorithms will be presented in the next chapter, including an architecture framework facilitating this approach adoption for software engineers.

4.10.References:

1. Papp D., Ma Z., Buttyan L. Embedded systems security: Threats, vulnerabilities, and attack taxonomy. 2015 13th Annual Conference on Privacy, Security and Trust, PST 2015. IEEE; 2015; : 145–152. Available at: DOI:10.1109/PST.2015.7232966
2. Vahid F., Givargis T. Embedded System Design: A Unified Hardware/Software Approach. 1999; : 103.
3. Pham Van P Van., Binh NN. Embedded System Architecture Design and Optimization at the Model Level. International Journal of Computer and Communication Engineering. 2012; 1(4): 345–349. Available at: DOI:10.7763/ijcce.2012.v1.87
4. Marwedel P. Embedded System Design. Cham: Springer International Publishing; 2018. Available at: DOI:10.1007/978-3-319-56045-8 (Accessed: 15 August 2019)
5. Radoglou Grammatikis PI., Sarigiannidis PG., Moscholios ID. Securing the Internet of Things: Challenges, threats and solutions. Internet of Things. Elsevier B.V.; 2018; 5: 41–70. Available at: DOI:10.1016/j.iot.2018.11.003
6. Wang W., Zhang X., Hao Q., Zhang Z., Xu B., Dong H., et al. Hardware-Enhanced Protection for the Runtime Data Security in Embedded Systems. Electronics. 2 January 2019; 8(1): 52. Available at: DOI:10.3390/electronics8010052 (Accessed: 8 September 2019)
7. Chai H., Zhang G., Zhou J., Sun J., Huang L., Wang T. A Short Review of Security-Aware Techniques in Real-Time Embedded Systems. Journal of Circuits, Systems and Computers. 12 February 2019; 28(02): 1930002. Available at: DOI:10.1142/S0218126619300022 (Accessed: 8 September 2019)
8. Riahi Sfar A., Natalizio E., Challal Y., Chtourou Z. A roadmap for security challenges in the Internet of Things. Digital Communications and Networks. Elsevier Ltd; 2018; 4(2): 118–137. Available at: DOI:10.1016/j.dcan.2017.04.003
9. Habibzadeh H., Nussbaum BH., Anjomshoa F., Kantarci B., Soyata T. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustainable Cities and Society. Elsevier; October 2019; 50(June): 101660. Available at: DOI:10.1016/j.scs.2019.101660
10. Humayed A., Lin J., Li F., Luo B. Cyber-Physical Systems Security - A Survey.

- IEEE Internet of Things Journal. 2017; 4(6): 1802–1831. Available at: DOI:10.1109/JIOT.2017.2703172
11. Ravi S., Kocher P., Lee R., McGraw G., Raghunathan A. Security as a new dimension in embedded system design. Proceedings of the 41st annual conference on Design automation - DAC '04. New York, New York, USA: ACM Press; 2004. p. 753. Available at: DOI:10.1145/996566.996771
 12. Bodei C., Chessa S., Galletta L. Measuring security in IoT communications. Theoretical Computer Science. Elsevier B.V.; 2019; 764: 100–124. Available at: DOI:10.1016/j.tcs.2018.12.002
 13. Hameed S., Khan FI., Hameed B. Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review. Journal of Computer Networks and Communications. 10 January 2019; 2019: 1–14. Available at: DOI:10.1155/2019/9629381
 14. Ali S., Al Balushi T., Nadir Z., Hussain OK. Risk Management for CPS Security. springer. Cham: Springer International Publishing; 2018. pp. 11–33. Available at: DOI:10.1007/978-3-319-75880-0_2 (Accessed: 15 August 2019)
 15. Aloheel A., He H., Shaw C., Khan MA. Analytical Review of Cybersecurity for Embedded Systems. IEEE Access. 2021; 9: 961–982. Available at: DOI:10.1109/ACCESS.2020.3045972
 16. Mukherjee B., Heberlein LT., Levitt KN. Network intrusion detection. IEEE Network. May 1994; 8(3): 26–41. Available at: DOI:10.1109/65.283931
 17. Vikram A., Mohana. Anomaly detection in Network Traffic Using Unsupervised Machine learning Approach. 2020 5th International Conference on Communication and Electronics Systems (ICCES). IEEE; 2020. pp. 476–479. Available at: DOI:10.1109/ICCES48766.2020.9137987
 18. Singh S., Banerjee S. Machine Learning Mechanisms for Network Anomaly Detection System: A Review. 2020 International Conference on Communication and Signal Processing (ICCSP). IEEE; 2020. pp. 0976–0980. Available at: DOI:10.1109/ICCSP48568.2020.9182197
 19. Vic Barnett TL. Outliers in statistical data. 3rd Editio. Wiley; 1994. Available at: <https://www.wiley.com/en-us/Outliers+in+Statistical+Data%2C+3rd+Edition-p-9780471930945>

20. Cook AA., Misirli G., Fan Z. Anomaly Detection for IoT Time-Series Data: A Survey. *IEEE Internet of Things Journal*. 2020; 7(7): 6481–6494. Available at: DOI:10.1109/JIOT.2019.2958185
21. Moustafa N., Hu J., Slay J. A holistic review of Network Anomaly Detection Systems: A comprehensive survey. *Journal of Network and Computer Applications*. Elsevier Ltd; February 2019; 128(October 2018): 33–55. Available at: DOI:10.1016/j.jnca.2018.12.006
22. Tao X., Peng Y., Zhao F., Zhao P., Wang Y. A parallel algorithm for network traffic anomaly detection based on Isolation Forest. *International Journal of Distributed Sensor Networks*. 27 November 2018; 14(11): 155014771881447. Available at: DOI:10.1177/1550147718814471
23. Seo J., Lee S. Abnormal Behavior Detection to Identify Infected Systems Using the APChain Algorithm and Behavioral Profiling. *Security and Communication Networks*. 2018; 2018. Available at: DOI:10.1155/2018/9706706
24. Feinstein L., Schnackenberg D., Balupari R., Kindred D. Statistical approaches to DDoS attack detection and response. *Proceedings DARPA Information Survivability Conference and Exposition*. IEEE Comput. Soc; 2003. pp. 303–314. Available at: DOI:10.1109/DISCEX.2003.1194894
25. Latif S., Zou Z., Idrees Z., Ahmad J. A Novel Attack Detection Scheme for the Industrial Internet of Things Using a Lightweight Random Neural Network. *IEEE Access*. 2020; 8: 89337–89350. Available at: DOI:10.1109/ACCESS.2020.2994079
26. Chen C-L., Chen H-C. A resource utilization measurement detection against DDoS attacks. 2016 9th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI). IEEE; 2016. pp. 1938–1943. Available at: DOI:10.1109/CISP-BMEI.2016.7853035
27. Ding M., Xiong Z., Yu J. Anomaly Detection Based on Job Monitoring Metrics in Distributed System. 2018 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC). IEEE; 2018. pp. 182–186. Available at: DOI:10.1109/SPAC46244.2018.8965641
28. Prakash J., Sankaran S., Jithish J. Attack detection based on statistical analysis of smartphone resource utilization. 2019 IEEE 16th India Council International

-
- Conference, INDICON 2019 - Symposium Proceedings. IEEE; 2019; (1): 2019–2022. Available at: DOI:10.1109/INDICON47234.2019.9030310
29. Gulenko A., Wallschlagel M., Schmidt F., Kao O., Liu F. Evaluating machine learning algorithms for anomaly detection in clouds. 2016 IEEE International Conference on Big Data (Big Data). IEEE; 2016. pp. 2716–2721. Available at: DOI:10.1109/BigData.2016.7840917
30. Shabtai A., Kanonov U., Elovici Y., Glezer C., Weiss Y. “Andromaly”: a behavioral malware detection framework for android devices. *Journal of Intelligent Information Systems*. 6 February 2012; 38(1): 161–190. Available at: DOI:10.1007/s10844-010-0148-x
31. Liu S., Chen Y., Trappe W., Greenstein LJ. ALDO: An Anomaly Detection Framework for Dynamic Spectrum Access Networks. *IEEE INFOCOM 2009 - The 28th Conference on Computer Communications*. IEEE; 2009. pp. 675–683. Available at: DOI:10.1109/INFCOM.2009.5061975
32. Agrawal B., Wiktorski T., Rong C. Adaptive real-time anomaly detection in cloud infrastructures. *Concurrency Computation*. New York, NY, USA: ACM; 25 December 2017; 29(24): e4193. Available at: DOI:10.1002/cpe.4193
33. Lazri K., Laniece S., Zheng H., Ben-Othman J. AMAD: Resource Consumption Profile-Aware Attack Detection in IaaS Cloud. 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing. IEEE; 2014. pp. 379–386. Available at: DOI:10.1109/UCC.2014.48
34. Cherkasova L., Ozonat K., Mi N., Symons J., Smirni E. Automated anomaly detection and performance modeling of enterprise applications. *ACM Transactions on Computer Systems*. 14 November 2009; 27(3): 1–32. Available at: DOI:10.1145/1629087.1629089
35. Hayes MA., Capretz MA. Contextual anomaly detection framework for big sensor data. *Journal of Big Data*. 27 December 2015; 2(1): 2. Available at: DOI:10.1186/s40537-014-0011-y
36. Schnorr LM., Legrand A., Vincent J-M. Detection and analysis of resource usage anomalies in large distributed systems through multi-scale visualization. *Concurrency and Computation: Practice and Experience*. October 2012; 24(15): 1792–1816. Available at: DOI:10.1002/cpe.1885

37. Fortier PJ., Michel HE. Introduction. Computer Systems Performance Evaluation and Prediction. Elsevier; 2003. pp. 1–38. Available at: DOI:10.1016/B978-155558260-9/50001-1
38. Edgar TW., Manz DO. Instrumentation. Research Methods for Cyber Security. Elsevier; 2017. pp. 321–344. Available at: DOI:10.1016/B978-0-12-805349-2.00013-3
39. Fortier PJ., Michel HE. Hardware Testbeds, Instrumentation, Measurement, Data Extraction, and Analysis. Computer Systems Performance Evaluation and Prediction. Elsevier; 2003. pp. 305–330. Available at: DOI:10.1016/B978-155558260-9/50010-2
40. psutil documentation, psutil , 2009-2021. [Online]. Available: URL. Available at: <https://psutil.readthedocs.io/en/latest/> (Accessed: 25 April 2021)
41. Love R. Linux Kernel Development. 3rd edn. Addison-Wesley Professional; 2010. p. 33.
42. The Linux man-pages project, hkernel.org doc man-pages 2021. Available at: <https://www.kernel.org/doc/man-pages/> (Accessed: 25 April 2021)
43. Frequency management and thermal control, Raspberry Pi Foundation,. Available at: <https://www.raspberrypi.org/documentation/hardware/raspberrypi/frequency-management.md> (Accessed: 25 April 2021)
44. Python 3.9.4 documentation,python.org,2021. 2021. Available at: <https://docs.python.org/3/> (Accessed: 25 April 2021)
45. ,Understanding Denial-of-Service Attacks, us-cert.cisa.gov, November 04, 2009. 2020. Available at: <https://us-cert.cisa.gov/ncas/tips/ST04-015> (Accessed: 25 April 2021)
46. Biswas S., Chellappa R. Encyclopedia of Cryptography and Security. van Tilborg HCA, Jajodia S (eds.) In the Tree Where the Double Sex Sleeps. Boston, MA: Springer US; 2011. 38–38 p. Available at: DOI:10.1007/978-1-4419-5906-5
47. Biswas S., Sohel M., Sajal MM., Afrin T., Bhuiyan T., Hassan MM. A Study on Remote Code Execution Vulnerability in Web Applications. International Conference on Cyber Security and Computer Science. 2018; (October): 1–8.
48. Fazeldehkordi E., Akanbi OA., Study A., Attack H. A Study of Black Hole Attack

Solutions. Elsevier; 2016. Available at: DOI:10.1016/C2015-0-04114-4

**CHAPTER 5: ATTACK-DETECTION ARCHITECTURAL
FRAMEWORK BASED ON ANOMALOUS PATTERNS OF
SYSTEM PERFORMANCE AND RESOURCE UTILISATION**

CHAPTER 5: ATTACK-DETECTION ARCHITECTURAL FRAMEWORK BASED ON ANOMALOUS PATTERNS OF SYSTEM PERFORMANCE AND RESOURCE UTILISATION

Abdulmohsan Alooseel¹, Saba Al-Rubaye (IEEE Member)¹, Argyrios Zolotas (Senior Member, IEEE)¹, Carl Shaw²

¹School of Aerospace, Transport and Manufacturing (SATM), Cranfield University

²Cerberus Security Laboratories Ltd, UK.

5.1. Abstract

This chapter presents a unique security approach for detecting cyber-attacks against embedded systems (ESs). The proposed approach has been shaped within an architectural framework called anomalous resource consumption detection (ARCD). The approach's detection mechanism detects cyber-attacks by distinguishing anomalous performance and resource consumption patterns from a pre-determinable reference model. The defence mechanism of this approach acts as an additional layer of protection for ESs. This technique's effectiveness was previously evaluated statistically, and in this chapter, we tested this approach's efficiency computationally by using the support-vector machine algorithm. The datasets were generated and collected based on a testbed model, where it was run repeatedly under different operation conditions (normal cases (Rs) versus attacked cases). The executed attack scenarios are (1) denial-of-service (DoS), (2) brute force (BF), (3) remote code execution (RCE), and man-in-the-middle (MITM). A septenary tuple model, which consists of seven determinants that are analysed based on seven statistical criteria, is the core of the detection mechanism. The prediction accuracy in terms of classifying anomalous patterns compared to normal patterns based on the confusion matrix revealed promising results, proving this approach's effectiveness, where the final results confirmed very high prediction accuracies in terms of distinguishing anomalous patterns from the typical patterns. Integrating the ARCD concept into an operating system's functionality could help software developers augment the existing security countermeasures of ESs. Adopting the ARCD approach will pave the way for software engineers to build more secure operating systems in line with the embedded system's capabilities, without depleting its resources.

5.2. Introduction

5.2.1. Embedded Systems and Cybersecurity Challenges

The enormous expansion of the applications of ESs in many different domains highlights the urgent need to secure these systems against cyber-attacks; the consequences of not doing so might be catastrophic for individuals, companies, organizations, and governments[1], [2], [3], [4], [5], [6]. The resource limitations of ESs impose tight constraints on computing capacity [7][8]. The limited processing capability and the limited energy of the ESs block the implementation of high-level security measures, as in conventional computer systems [9], [10], [11], [12], [6], [13]. Therefore, the capabilities of ESs face the significant challenge of meeting advanced security solution requirements. Marwedel [13] shed light on many tight constraints on ES resources, particularly for SoCs; these limitations are hindering the implementation of advanced security solutions. Therefore, the ESs must be designed with resource-awareness [14]. These constrained capabilities have made the applicability of conventional security mechanisms for ESs impossible [15]. The processing gaps, battery gaps, and costs are at the top of the security challenges list [13]. The high barrier of constraints on computational capability, storage, power, and other aspects of ESs characteristics are complicating the implementation of advanced security solutions, making it difficult to maintain data confidentiality through encryption and key management, as mentioned by Liu et al. [16], [17], [18].

Neglecting security countermeasures at the early stages of ES design increases the number of unprotected entry points, which can result in unauthorized access to the system. As many ESs are battery-powered, and as long as the enhancement of security solutions might sacrifice part of the power sources, it is crucial to at minimum reduce the amount of power consumption with lightweight and efficient solutions [17]. Running robust encryption on ESs with their constrained resources is a critical challenge [19], [20]. Thus, the inability of ESs to handle intensive cryptographic calculations on SoCs is due to their limited resources, giving rise to the need for suitable solutions [14].

Ali et al. [21] stated that “the major point of concern is due to the limited resources”; thus, complicated requirements such as higher computational capability and lower power consumption impose serious challenges for the implementation of effective and efficient

security solutions. Traditional advanced security solutions in this field offer impractical solutions, considering the ESs' abilities. The best security solutions must consider the capabilities of software and hardware in the early stages of design; in addition, adopting the "security by design" concept is recommended to avoid unexpected modification costs. Furthermore, we have previously published a comprehensive analytical study of all aspects related to the cybersecurity of ESs [22].

Therefore, I would like to emphasize this study's main motivation, which is the lack of compatible security solutions in line with ES capabilities. As long as ESs are exposed to the same security threats as multitasked computer systems but with significant limitations for handling advanced security solutions as effectively as conventional systems, and as long as ESs have the same generic security goals (confidentiality, integrity, and availability) as conventional systems, the implementation of efficient security solutions in line with ES capabilities remains a critical challenge. Therefore, there is an urgent need for efficient security solutions [22], [17]. Efficient and compatible security solutions for ESs are necessary because of their decisive roles in a diverse array of domains. In this chapter, we are presenting a new security architecture framework (ARCD), bridging the gap by contributing to this aspect of ES cybersecurity. The ARCD approach derives its rationale in detecting cyber-attacks from the ability to define a comparable reference performance pattern for the ES; this is due to its functions' determinability. After that, the anomalous pattern (if it exists and is observable during the attack presence) will be used as an indicator to detect the attack, activate an autonomous response, and warn the system administrator.

Based on what has been addressed in this introduction, it has become apparent that one of the most distinctive features of the ES is that ESs are dedicated to performing specific functions, which distinguishes them from conventional systems. Accordingly, we assume that these systems have identifiable performance patterns, and in the event of a cyber-attack, these systems may form abnormal patterns in terms of performance and resource consumption. Therefore, we have reached the linkage point between the main research topic "cybersecurity of ESs" and the purpose of adopting machine learning (ML) methods, where we seek to calculate the prediction accuracy for classifying typical patterns against anomalous patterns that were monitored during the system's exposure to various cyber-attacks. The collected data values were previously evaluated statistically.

Therefore, to complete the validation of the approach, we created training models followed by test models for the datasets to find the predictive accuracy ratio based on selected parameters, which represent the features of datasets in the ML context. Also, the relevant studies to the concept of this approach have been addressed in Chapter 4.

5.2.2. Machine Learning for ES Cybersecurity

Machine learning, as described by Zhang, is “a subset of artificial intelligence, which builds (sic) a mathematical model based on sample data, known as ‘training data,’ in order to make predictions or decisions without being explicitly programmed to perform the task” [23]. The exploitation of ML algorithms in the field of cybersecurity is drawing many researchers in this direction, as it is taking security countermeasures to a new level. Concepts such as anomaly-based detection, recognition strategies, and network traffic pattern analysis have been intensively discussed in many studies [24–28] . Therefore, adopting artificial intelligence (AI) concepts, and ML algorithms in particular, contribute to the development of innovative and effective security solutions that differ from known traditional solutions such as anti-virus software, firewalls, and encryption. The domains of anomaly detection implementations are endless, as they can be implemented across many applications such as network traffic, resource utilisation, behavioural profiling, statistical analysis, and machine learning algorithms. The following table summarizes some relevant studies to the proposed approach.

Table 5-1: Summary of the related studies

Ref	Anomaly Detection Domains	Deliverables
[29]	Android devices	Behavioural malware detection framework.
[30]	Network Anomaly Detection Systems (NADSs)	Holistic review
[31] [32]	Machine Learning concepts, and Machine Learning algorithms	A Novel Attack Detection Scheme, and Machine Learning algorithms evaluation
[33]	Network Traffic	A Proposed parallel network traffic anomaly detection algorithm
[34] [35]	Resource utilisation, or resources usage.	A novel DDoS detection scheme, and analysis methodology
[36]	statistical analysis	A detection-response prototype

[37]	Behavioral Profiling	Attack Pattern Chain algorithm (APChain) and a behavioral profiling algorithm
[38] [39]	Cloud infrastructures, and IaaS Cloud	A scalable model for automatic anomaly detection, and a system designed for detecting an abusive use of dynamic virtual machine migration
[40]	Dynamic Spectrum Access Networks	A framework for detecting unauthorized spectrum usage
[41]	Distributed Systems	An anomaly detection approach
[42]	Internet of Things (IoT)	A Survey of Anomaly Detection for IoT
[43]	Enterprise application	A novel framework for automated anomaly detection
[44]	Big sensor data	Contextual framework

However, ML as a branch of artificial intelligence is a forked domain, and its algorithms and applications are divergent. ML methods can be placed into many categories based on dataset nature or desired purpose (clustering, classifying, regression), or according to the implications of influencing factors, such as environment, object, event, or intended action or decision. According to Zhang, ML can be categorized into two main roots: (1) Euclidean structured data learning and (2) non-Euclidean structured data learning [23]. Based on these two roots, ML methods can be classified into six different types of learning, as illustrated in the following figure (Fig. 5-1). Supervised learning, semi-supervised learning, and unsupervised learning are classical learning approaches. The algorithms of the classical learning methods are based on computational statistic concepts. According to the nature of the dataset, the supervised learning methods are suitable when the datasets are labelled, and they can be pre-categorized into groups. The semi-supervised learning method can be divided into three classes: (1) Self-training, by using its own predictions to teach itself; (2) co-training, by using the co-training setting and use their own predictions to teach themselves; (3) active learning, based on an active or participatory role in determining which data points it will be asked to label by an expert or teacher [23].

The semi-supervised method can be adopted when the datasets are partially labelled. Each of these methods has its own algorithms for learning and prediction based on different mathematical equations. The supervised learning methods can be used for classification

or regression, while the unsupervised methods can be used for clustering or association, where the features are unknown in early stages.

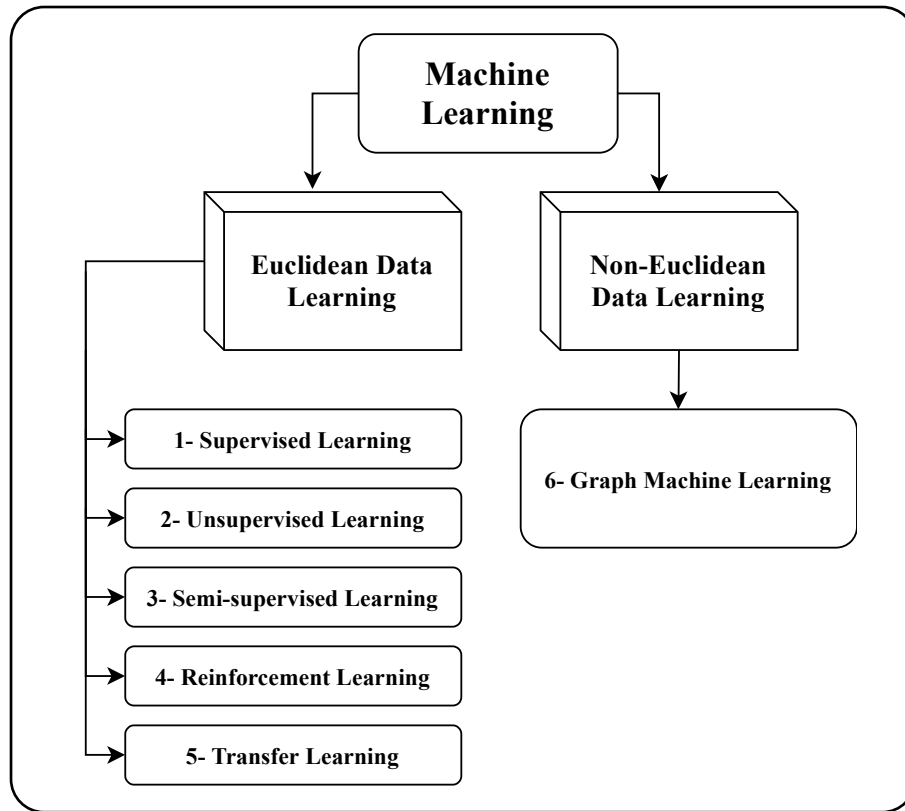


Figure 5-1. Machine Learning roots.

The fourth and fifth machine learning types based on Euclidean data learning are reinforcement learning and transfer learning. The concept of reinforcement learning is to learn by interacting with an environment, event, or object. A repeated response to a specific event or object within the surrounded environment will enhance the machine's ability to learn. The reinforcement learning method can be used in a dynamic environment by feeding the learning system with feedback based on the interaction experience. The transfer learning method can be applied to transfer knowledge from the source domain to the target domain [23]. The second root of the ML tree is graph machine learning, which is a sub-category of the non-Euclidean structured data learning root. With this method, the machine will learn based on training samples of the structure of a graph. Typically, the main purpose of using ML is to establish a regressor or classifier through the training group of a dataset and then to evaluate the performance through a test model with a test dataset. Thus, the two main tasks of ML are classification of discrete data and prediction

of continuous data [23]. In the machine learning discussion context, there is an essential term that must be referred to, namely “pattern recognition.” A pattern, as described by Watanabe [45], is the “opposite of chaos (sic); it is an entity, vaguely defined, that could be given a name.” Pattern recognition aims to classify or to cluster a dataset into classes based on their distinctive features, using one of the following four typical approaches: (1) template matching, (2) statistical classification, (3) syntactic or structural matching, or (4) neural networks [23].

In this study, we are applying machine learning method to design a classifier, or predictor model to separate the anomalous patterns from the typical patterns of ES performance. Since the ESs are dedicated to performing specific functions, we assume that they consume their resources in a determinable pattern; thus, we can define a standard performance pattern acting as a reference model; in addition, we assume that during the ES attack, an observable anomalous pattern in resource consumption and performance might be monitored. Thus, our suggested security approach is to detect cyber-attacks based on discriminating anomalous patterns in comparison to a predetermined standard pattern, which can be identified in the early design stages extracted from typical performance patterns. Based on the dataset features and purpose of applying machine learning algorithms, the classification algorithms are the most appropriate algorithms, as we are trying to calculate the prediction accuracy percentage in terms of separating anomalous patterns values from the typical pattern values. Therefore, using classification algorithms for machine learning will prove the validity and efficiency of this technique, or the opposite, depending on the prediction accuracy percentage.

The remainder of this chapter is organized as follows. Section 5.3 addresses the machine learning role in the cybersecurity of ESs and presents the approach hypothesis. Section 5.4 presents our case study design, with explanations of normal operating conditions and attack scenario cases. Statistical classification results are evaluated and presented in section 5.5. The support-vector machine (SVM) algorithm implementation and prediction accuracy results are explained and discussed in section 5.6. Section 5.6 illustrates the architectural framework for approach adoption. Finally, the conclusion and future works are summarized in section 5.8.

5.3. Applying The Machine Learning Method for ARCD Approach Validation

5.3.1. Approach Hypothesis

We conceptualized a research hypothesis, as follows: “In ESs, which are designed to perform specific functions, performance and resource consumption are within a determinable pattern. Thus, an anomalous pattern (if it exists and is identifiable) can be exploited in comparison to a pre-identifiable reference pattern as an indicator to detect cyber-attacks.” In the ML context, defining a standard pattern means labelling its parameter values as the standard consumption and categorizing any outlier values from the normal range, or typical patterns as abnormal values that belong to an anomalous pattern. Based on the ARCD approach, we do not focus on the impact of the attack on the system’s functions but instead focus on the changes in system performance and resource consumption, regardless of the type, method, or surface of this attack—in other words, we detect attacks based on anomalous pattern recognition, which is comparable to a pre-definable reference pattern model.

To test the validity of the hypothesis, we designed a realistic experiment as a case study, using the Smart PiCar (manufactured by SunFounder) as a testbed, reflecting a real-life example of an ES application. The Smart PiCar is designed to carry out reconnaissance missions within a specific geographical area. It was equipped with a recording camera and ultrasound avoidance module. The following figure demonstrates the assembled and configured Smart PiCar.

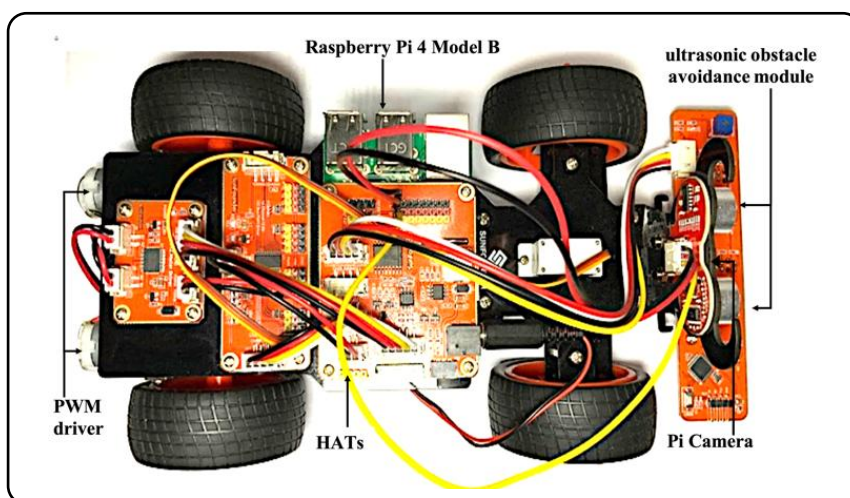


Figure 5-2. Assembled Smart PiCar as a testbed.

5.3.2. Machine Learning Algorithm Selection

MATLAB [46], [47], a numeric computing environment platform, was used to train and test the datasets; in particular, we used the classification learner app. The datasets have been examined against twenty-four different algorithms based on six different training models. These models are (1) decision trees, (2) discrimination analyses, (3) naive Bayes classifiers, (4) support-vector machines, (5) nearest neighbour classifiers, and (6) ensemble classifiers. The support-vector machine algorithms, along with several other algorithms (such as fine K-nearest neighbour), revealed the highest accuracy percentages in terms of classification, based on the data training sessions. The quadratic support vector machine (QSVM) algorithm was the most accurate algorithm overall, based on the prediction accuracy percentage; accordingly, the test models have been generated.

The SVM algorithm was initially proposed by Vapnik et al. [48], [49]; it is based on the Vapnik–Chervonenkis (VC) theory [50], which is related to the statistical learning theory [51], [52]. The SVM algorithm concept involves finding a hyperplane to classify the datasets into classes based on their features. The hyperplane acts as a separator and falls in the middle of a margin, and the margin represents the maximum possible width between two classes supported by support vectors; the support vectors are the closest data points to the hyperplane. The following figure depicts the concept of the SVM algorithm.

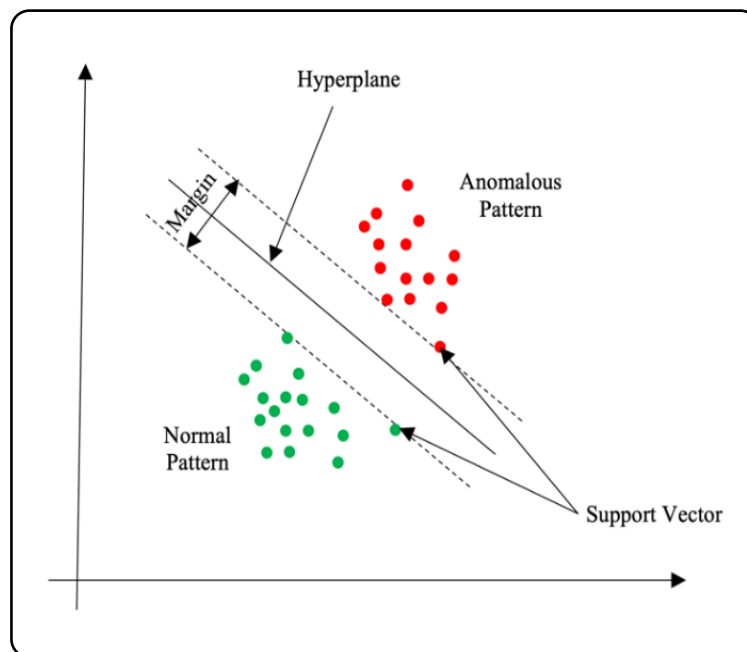


Figure 5-3. The support vector machine algorithm principle.

5.4. Case Study Design

This section is divided into two parts. The first part describes the normal operating conditions of the Smart PiCar as an example of CPS applications, with its structure, components, and functions. Based on running the Smart PiCar repeatedly, the parameters' values have been collected to evaluate the possibility of determining a reference pattern. If the PiCar shows consistency in its performance and resource consumption, we will be able to generate a standard performance pattern act as a reference model; otherwise, defining a reference model will not be possible. The second part explains a set of different attack scenarios that have been executed against the testbed (PiCar) to study ES behaviour under these circumstances. If anomalous patterns are observed, and the ability to determine a standard pattern is confirmed, we will develop our approach by merging these two findings and then delivering an architectural framework to facilitate the adoption of this approach.

5.4.1. Normal Conditions

The Smart PiCar was assembled and programmed for reconnaissance purposes. It was equipped with a built-in camera and ultrasonic avoidance module to ensure constant movement and avoid collision with obstacles. In terms of the embedded processing unit, a Raspberry Pi 4 Model B was embedded to take over the computational tasks. During the test period, system performance and resource consumption were monitored, based on seven parameters:

- I. Resource consumption:
 - CPU utilisation.
 - Memory load.
 - CPU temperature.
 - Power consumption in terms of:
 - Voltage.
 - Current.
 - V(D) and V(D-).
- II. System performance:
 - Alive processes count.
 - Executed threads count.
 - Rate of transmitted and received data.

The terms resource consumption and system performance have been shortened to resource consumption performance (RCP) for the rest of this chapter. The proposed

approach does not address how the system performs its functions but instead focuses on how it consumes its resources, considering the cyber-attack as an external factor. Regarding the operating condition, the system functions were operated three times repeatedly and separately, and all the data was evaluated statistically. The statistical classification results are discussed in section 5-5. The three rounds of typical operation were labelled as R1, R2, and R3 and grouped based on modified features, such as dataset-1 and dataset-2, to be tested against different random datasets where their values were collected under attack circumstances.

5.4.2. Attacked Case Scenarios

5.4.2.1. Denial of Service Attack

The first generated attack scenario is the denial-of-service (DOS) attack. The DoS attack was accomplished by flooding the smart PiCar with directed arbitrary data traffic using the low orbit ion cannon (LOIC) tool. While the Smart PiCar was being attacked, the testbed's parameters were observed, and their values were collected and stored.

5.4.2.2. Password Attack

The second attack scenario is the password attack; some of these techniques include the brute force attack and the dictionary attack. In order to generate the attack, several tools were used. BruteDum was used as a brute-forcing tool, and for port scanning, the Nmap tool was used as the network mapper. The Hydra framework as a parallelized network logon cracker was activated, and it was supported with a random text password list. The password list contained some of the most common and random meaningful words. As in the previous attack scenario, the parameters' patterns were observed, and their values collected and stored.

5.4.2.3. Remote Code Execution and Malicious Software

In the third attack scenario, malicious software was executed remotely as a remote code execution attack. The malicious code is designed to disrupt the Smart PiCar's function by disabling the PiCamera remotely. The expected impact of this attack on the hardware and software performance patterns of the Smart PiCar were observed during the attack

period. The testbed's parameter values were collected and stored to be added to the datasets.

5.4.2.4. Man-In-The-Middle Attack by Executing Command Remotely

Unlike the previous attack, in this type of attack, the attacker redirects the camcorder recording to their device and gains unauthorized access to a live camera broadcast. To carry out this type of attack, the attacker executes the following command remotely against the victim's device:

```
"raspivid -o - -t 0 -w 960 -h 540 | cvlc -vv stream:///dev/stdin --sout '#rtp{sdp=rtsp://:8554/}' :demux=h264."
```

The expected impact on system performance patterns was monitored in terms of test parameters. Finally, the parameters' values under these circumstances were collected to be added to the dataset for computational validation.

5.5. Statistical Classification Method Results

As we are dealing with real numbers (values of specific parameters), not imaginary values, the principles of real analysis, which is a branch of mathematical analysis and statistics, have been adopted. Based on the research hypothesis (section 5.3.1), we analysed the collected data according to several statistical criteria (mean, median, mode, standard deviation, range, minimum, and maximum). To evaluate the possibility of defining a standard pattern of system performance and resource consumption under different operational conditions, the above statistical criteria were calculated to define the range and pattern of the RCP, whether in typical or attacked cases.

Based on the statistical criteria results, we determined that the system performs its functions in a similar pattern in terms of performance and resource consumption each time when operated and has an identifiable pattern in a form that can be identified, and a standard performance pattern has been defined accordingly (Chapter 4, Sec 4.6). To test the second part of the approach hypothesis, we generated different attack scenarios to determine if the system was behaving irregularly in terms of its RCP; thus, anomalous

patterns might be formed; these anomalous patterns are supposedly distinguishable in comparison to the standard generated pattern. The analysis results proved the validity of what we assumed, as the system showed abnormal performance patterns in all cases while exposed to a cyber-attack. The following table summarizes the statistical classification results.

Table 5-2 presents a summary of the statistical classification analysis. These results are what encouraged us to measure the prediction accuracy in distinguishing anomalous patterns from the normal typical pattern by using machine learning algorithms. Some statistical parameters, such as the minimum and the maximum, were calculated to determine the range of the RCP. The other criteria, such as the mode and mean, were calculated to find out the pattern of the RCP, where it was observed that the performance and resource consumption rates might be within the limits of the normal range, but at a different pattern. One of the most accurate and reliably applied statistical criteria are the mode values of threads count.

By looking at Table 5-2, the mode value columns show that, in most cases, the significant similarities reached the point of congruence in the typical performance pattern (Rs) cases. We can recognize the anomalous patterns in the system's performance during a cyber-attack by looking to the same criterion. For example, we noticed that the mode values of the threads count for the R1, R2, and R3 cases were identical (232 threads).

In contrast, when the system was subjected to a cyber-attack, the mode values were 249, 240, 221, and 241 threads for each of the DoS, brute force (BF), remote code execution (RCE), and man-in-the-middle (MITM) attacks, respectively. The results were similar for the rest of the statistical results applied within the testbed parameters. The statistical classification method showed encouraging results, the approach efficiency defining a standard pattern and distinguishing between typical performance patterns and anomalous patterns.

The significant similarity often reached identical limits in terms of the performance and resource consumption rate and under normal operating conditions proved the possibility of determining a standard reference pattern. In contrast, the anomalous patterns of the system while being exposed to different attack scenarios confirmed that it is possible to

detect attack existence through the anomalous patterns caused by abnormal levels of performance and resource consumption.

For an overall evaluation at a glance, two graphs (5-4 and 5-5) have been generated. Looking at the left side of Figure 5-4 or 5-5, we notice the significant similarities in the system's performance patterns in the R1, R2, and R3 cases. On the other hand, by looking at the right side of Graphs 5-4 and 5-5, we can see the system's performance pattern anomalies more clearly while the system is under attack. For example, in Graph 5-4, the system performance pattern was abnormal in the case of a DoS or brute-force attack. Likewise, in Graph 5-5, anomalous patterns were inconsistent with the conventional patterns that were formed during the RCE and MITM attacks. Therefore, defining the regular performance pattern as a reference model for the system's performance and then monitoring any deviation from it to predict the presence of suspicious activity is an effective mechanism for ESs dedicated to performing specific functions. Based on this compelling mathematical evidence, it is possible to test the validity and feasibility of the proposed security approach computationally through machine learning algorithms.

Table 5-2: Statistical classification Results

CPU Utilisation						Threads Number						Current					
	Mean	Mode	Range	Min	Max		Mean	Mode	Range	Min	Max		Mean	Mode	Range	Min	Max
R1	12.39	7.9	20.2	6.2	26.4	R1	228	232	14	219	233	R1	0.62	0.61	0.08	0.59	0.67
R2	12.68	7.7	20.5	4.6	25.1	R2	228.9	232	12	222	234	R2	0.63	0.62	0.09	0.59	0.68
R3	12.74	7.5	22.8	5.7	28.5	R3	228.3	232	14	220	234	R3	0.62	0.61	0.07	0.59	0.67
DoS	31.9	30.9	47.3	6.8	54.1	DoS	241.8	249	33	226	259	DoS	0.61	0.61	0.08	0.56	0.64
BF	31.16	30.5	54.7	6.5	61.2	BF	249.2	240	50	223	273	BF	0.63	0.63	0.15	0.54	0.69
RCE	12.33	6.2	32.2	4.9	37.1	RCE	220.6	221	11	215	226	RCE	0.56	0.55	0.14	0.51	0.65
MIMT	15.87	7.4	33.6	5.3	38.9	MIMT	239.9	241	10	235	245	MIMT	0.62	0.61	0.17	0.53	0.69
Memory Load						Temp						RX Packets					
	Mean	Mode	Range	Min	Max		Mean	Mode	Range	Min	Max		Mean	Mode	Range	Min	Max
R1	9.52	9.5	1.4	9.3	10.7	R1	53.45	54	5	50	55	R1	4.04	0	24	0	24
R2	9.51	9.5	1.5	9.3	10.8	R2	46.6	50	14	38	52	R2	4.29	0	27	0	27
R3	9.52	9.5	1.4	9.3	10.7	R3	49.34	51	10	43	53	R3	5	0	27	0	27
DoS	10.14	10.2	1.8	9.7	11.5	DoS	61.57	64	10	55	65	RCE	3.99	0	27	0	27
BF	9.78	9.6	1.9	9.4	11.3	BF	58.11	60	13	50	63	MIMT	7.79	0	55	0	55
RCE	9.9	9.9	0	9.9	9.9	RCE	54.63	54	8	52	60						
MIMT	10.5	10.5	0.1	10.5	10.6	MIMT	56.15	55	6	54	60						
Tasks Number						Voltage						TX Packets					
	Mean	Mode	Range	Min	Max		Mean	Mode	Range	Min	Max		Mean	Mode	Range	Min	Max
R1	167.9	172	14	159	173	R1	4.99	4.99	0.01	4.99	5	R1	4.03	0	24	0	24
R2	168.8	172	11	162	173	R2	5	5	0.01	4.99	5	R2	4.29	0	29	0	29
R3	168.2	172	13	160	173	R3	5	5	0.01	4.99	5	R3	5.05	0	27	0	27
DoS	181.6	171	33	166	199	DoS	4.98	4.98	0.01	4.98	4.99	RCE	4.06	0	26	0	26
BF	189.1	180	50	163	213	BF	4.99	4.99	0.01	4.99	5	MIMT	284.3	1	645	1	646
RCE	167.5	169	11	162	173	RCE	5	5	0.01	4.99	5.01						
MIMT	171.8	173	10	167	177	MIMT	4.99	5	0.02	4.98	5						

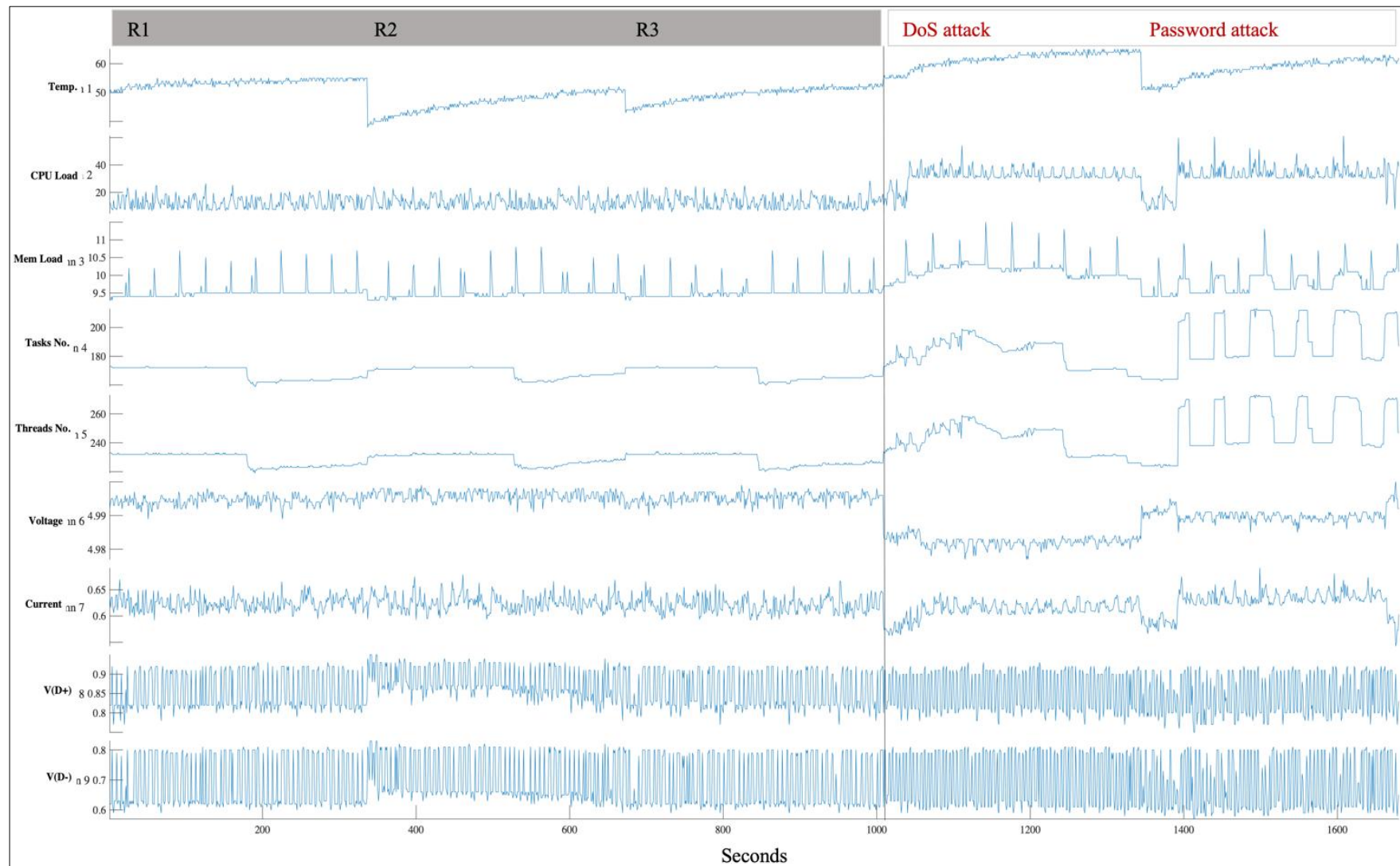


Figure 5-4. Typical patterns (Rs) vs. anomalous patterns (DoS and BF)

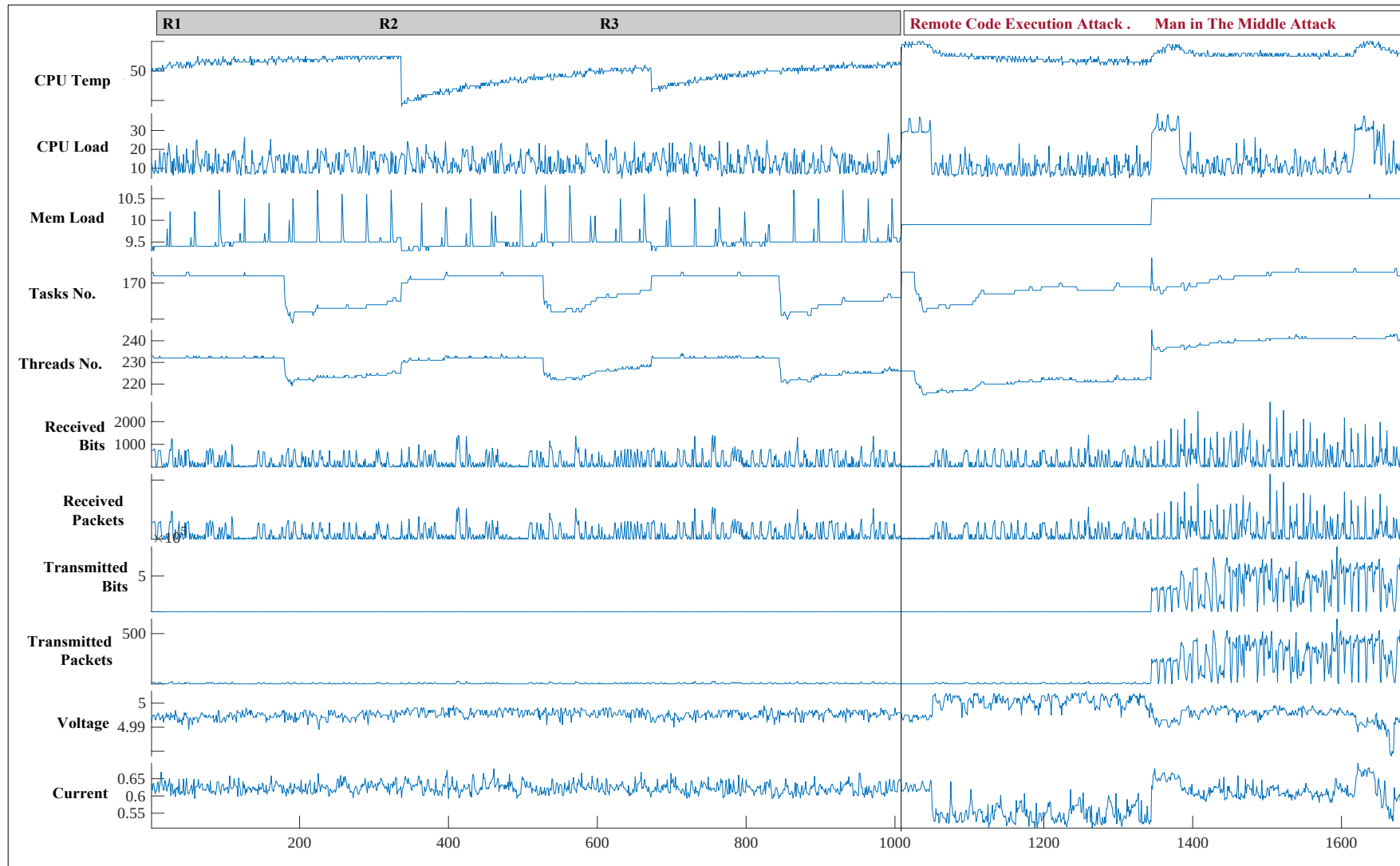


Figure 5-5. Typical patterns (Rs) vs. anomalous patterns (RCE and MITM).

5.5.1. Machine Learning: Data Normalisation, Modelling Requirements and Attack Prediction

Three main components are mandatory for successful machine learning modelling and for accurate computational statistic results. These components are (1) the data, (2) the features, and (3) the algorithm. In this work, we have 24,528 observations that have been generated and collected under different operation conditions. The collected data has been extracted and stored by executing Python code that has been written for this purpose. These datasets represent the performance and resource consumption values of specific parameters and variables that express the features of the dataset. The last component is the algorithm, which is addressed and determined in section 5.3.2.

5.5.2. Data Preparation and Testing

For data preparation (DP), the datasets have been grouped or labelled into multi groups. The dataset values of the R1, R2, and R3 cases were grouped into one group and labelled with -1 as the response. Rs cases represent the typical RCP pattern, which was generated by running the Smart PiCar three times under normal conditions. For the attacked cases, the dataset values of the Smart PiCar's performance under DoS attack were labelled with 1 as the response. Likewise, the values of the performance and resource consumption of the PiCar under the brute force attack were labelled with 2 as the response. Also, the collected data under the RCE and MITM attacks were labelled with 3 and 4 respectively, which represents the third and fourth attack scenarios. The purpose of labelling the datasets is to determine the response variable, which is mandatory for the creation of trained models based on the supervised learning method.

The unbalanced data or misclassification cost factor was taken into account during the data normalization step. The datasets were classified asymmetrically to simulate reality, where the normal pattern is usually the default or the dominant situation (has more observations) and the exception is the anomalous performance pattern. The following table summarizes the classes of the datasets.

Table 5-3: case classification and response

Cases		Response / Label
Normal Cases (Typical Performance)	R1	-1
	R2	
	R3	
Attack Cases	DoS	1
	BF	2
	RCE	3
	MITM	4

5.5.3. Machine Learning Modelling

Determining the data features will contribute to defining its patterns; the data features will act as predictors in the ML context, and these features or predictors are the parameters of the testbed in the experimentation context. The datasets are classified according to the predictors' value patterns. The features and predictors of the datasets are listed in the following table.

Table 5-4: dataset features

P		Features / Predictors
Parameters / Predictors	p1	CPU Temp.
	p2	CPU Utilisation
	p3	Memory Load
	p4	Task Number
	p5	Thread Number
	p6	Received Bits
	p7	Received Packets (RX)
	p8	Transmitted Bits
	p9	Transmitted Packets (TX)
	p10	Voltage (V)
	p11	Current (A)
	p12	D+(V)
	p13	D-(V)

After defining the features of the data, we can move on to generate trained and test models for pattern classification, and then measure the prediction accuracy. To generate the trained models, we started with trained multiclass models, using the classification learner app in MATLAB, which classifies the datasets into three classes based on their performance and resource consumption patterns (normal patterns versus anomalous patterns). We started with data loading, and then defined its variables (predictors), to be used for classification. In the first training session, to generate the first trained model, we

selected datasets 1 and 3, as shown in Table 5-5. Datasets 1 and 3 consist of 9 predictors and 15,120 observations. Likewise, for the second trained model, datasets 2 and 4 were loaded for a new training session. The datasets of this session consist of 18,480 observations, 11 predictors, and three classes, as shown in Table 5-5. After completing the training session by testing the datasets against 24 different algorithms based on six different machine learning methods, we selected the QSVM algorithm as the most accurate algorithm for prediction.

Table 5-5: dataset classification

Data group	Cases	Features	Observations
Dataset 1	R1, R2, and R3	9 features	9072
Dataset 2	R1, R2, and R3	11 features	11088
Dataset 3	DoS and BF attacks	9 features, p6–p9 excluded	6048
Dataset 4	RCE and MITM attacks	11 features, p12–p13 excluded	7392
Dataset 5	Random selection	Based on the category	6048–18480

Based on the trained models (1 and 2), models 3 and 4 were generated as the test models. The test models 3 and 4 were generated without their trained data. For the test session, dataset 5 has been created, which is a random selection from other datasets, in addition to new data. Also, in dataset 5, the class labelling (response) was excluded from the datasets, because we are in the testing phase, not the training stage. The following Table (5-6) summarizes the details of the trained and test models.

Table 5-6: trained and test models

Model		Datasets	Features	Classes	Observations
Trained Models	Model 1	Datasets 1 and 3	9	3	15120
	Model 2	Datasets 2 and 4	11	3	18480
Prediction Results		Prediction Correctness Percentage		Misclassification percentage	
Test Model	Model 3	99.880 %		0.1190 %	
	Model 4	100 %		0 %	

5.6. Classification Results: Analysis and Validation

5.6.1. Confusion Matrix Results

Based on the confusion matrix results, the final results showed very high prediction accuracies in terms of distinguishing anomalous RCP patterns from the typical patterns, where the correct prediction has been calculated within the True Positive Ratio (TPR), while the misclassification or (incorrect prediction) has been calculated within the False Negative Ratio (FNR). The accuracy percentage of the prediction is ranged between 100% and 98.8% as the lowest percentage.

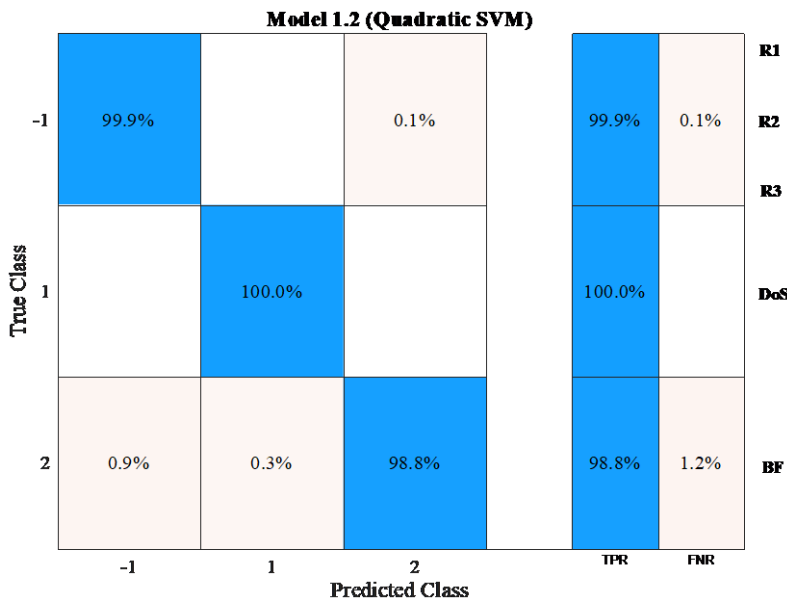


Figure 5-6. Confusion matrix 1 (Rs cases vs. attack cases).

As shown in Fig. 5-6, the prediction accuracy in identifying the classic pattern as a standard pattern was 99.9%. The false negative ratio (FNR) percentage was only 0.1%, and this misclassification (0.1%) percentage was classified incorrectly as an anomalous pattern belonging to the BF attack pattern. Regarding the prediction accuracy of the anomalous pattern under the DoS attack, 100% was reached, without any errors. Also, under the BF attack, the true positive ratio (TPR) percentage was 98.8%, and the FNR, which is the misclassification cost, was 1.2%. According to the results, 0.9% of the dataset was incorrectly considered to belong to the typical patterns, and 0.3% of the dataset was considered to belong to the DoS attack pattern. With regard to the third and fourth attack scenarios, based on the second confusion matrix results in Fig. 5-7, the

prediction accuracy of the typical pattern (Rs cases) reached 100%; in addition, all the anomalous patterns resulting from the attack's existence were identified to be 100% and classified correctly without any errors based on the TPR and FNR percentages. Therefore, increasing the monitored features count helps to make the prediction more precise; the features number of test model 2 was 11 features, compared to 9 features in test model 1.

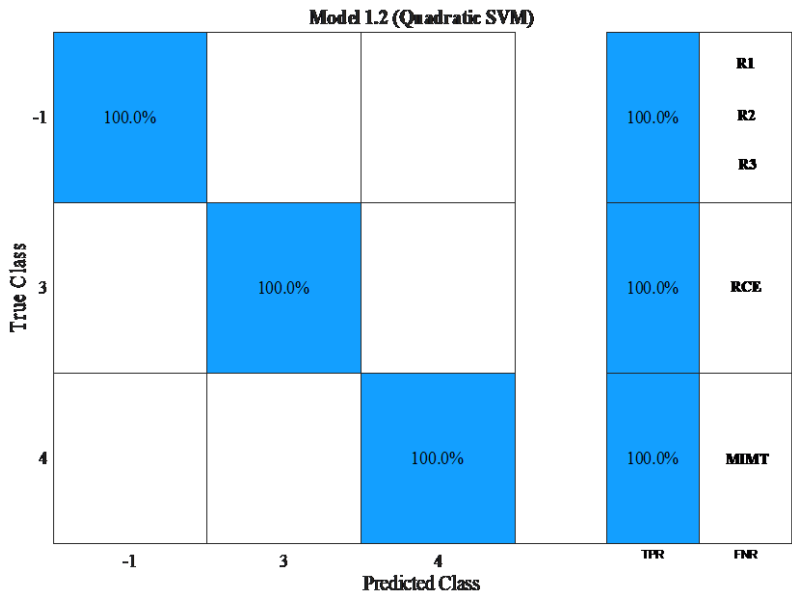


Figure 5-7. Confusion matrix 2 (Rs cases vs. attacked cases).

Overall, detecting a cyber-attack by comparing the in-progressed pattern to a predetermined reference pattern is a very effective method. Also, it is worth noting that the ability to distinguish anomalous patterns from the standard performance pattern is affected by the number of parameters (predictors), as it is not possible to detect the anomalous patterns accurately based on one predictor. Thus, relay through one parameter or predictor is not a reliable technique: the more parameters, the more accurate the prediction. However, to avoid extensive computing, some sub-parameters that have not shown any changes despite different operating conditions have been excluded in the proposed architectural framework, such as D+(V) and D-(V). In the remaining part of this section, the results for each predictor will be explained in more detail.

5.6.2. Effect of Predictors

The predictor most impacted by the attack has the most obvious effect in shaping the anomalous pattern. The effectiveness of the predictors varied in terms of the level of their

deviation from the typical pattern. Therefore, the combination of these predictors is what contributed to making the anomalous pattern more apparent. In addition, it was observed that the significant deviation of one predictor compared to another predictor will not only lead to the detection of the anomalous pattern, thus detecting the attack existence, but may also contribute to determining the type of attack. We will address this point in more detail while reviewing the results of the predictors individually.

5.6.2.1. CPU Utilisation

In terms of the CPU utilisation, the ability to discriminate between the typical patterns (reference patterns) of the RCP versus the anomalous RCP is clearly shown in figures 5-8 and 5-9. The impacts of the DoS and BF attacks on the PiCar's performance were classified accurately, based on the QSVM algorithm. Under the DoS and BF attack conditions, the differentiation between the standard and anomaly patterns appeared with two different characteristics. First, in terms of the range, which is the deviation from the standard regular consumption range (Rs cases); second, in terms of the pattern. In some cases, the RCPs were within the normal range; however, the RCPs appeared differently in terms of the pattern. For example, as shown in Fig. 5-9, the RCP of the Smart PiCar under the RCE and MITM attacks overlap within the typical range, but due to its anomalous pattern, the attack is still detectable and distinguishable based on the QSVM algorithm.

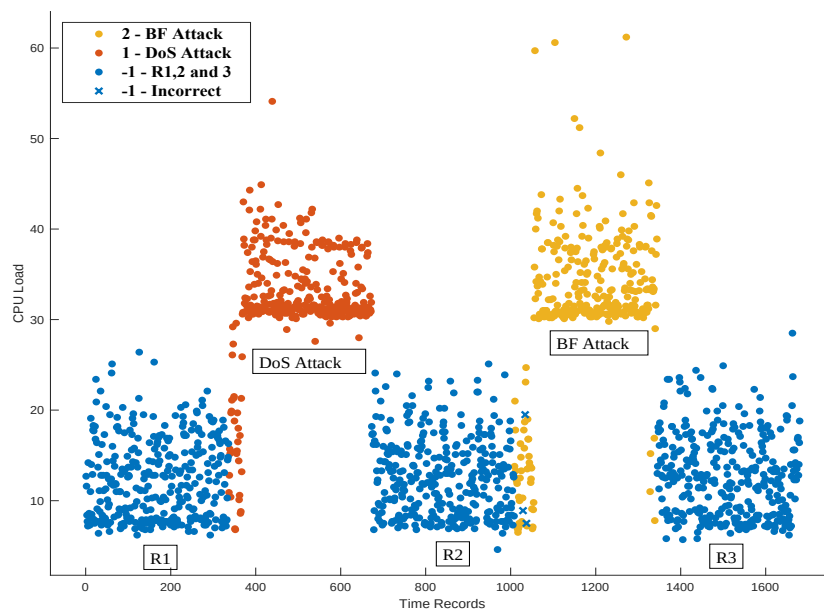


Figure 5-8. CPU pattern classification (Rs cases vs. DoS and BF).

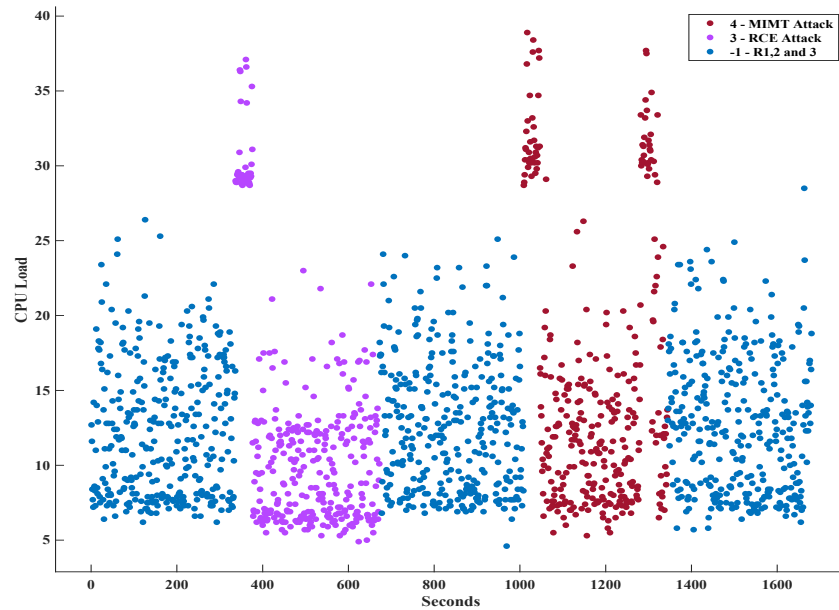


Figure 5-9. CPU pattern classification (Rs cases vs. RCE and MITM).

5.6.2.2. Memory Load

In terms of memory load, as shown in Figures 5-10 and 5-11, the memory usage in R1, R2, and R3 were identical in terms of the most frequent value (mode), which was concentrated at 9.50% (Table 5-2). The general trait of memory usage in Rs cases was consistent and steady, in a manner that can be determined and defined as the reference pattern; whereas, under the cyber-attack circumstances, the memory usage pattern was anomalous in a manner that can be easily detected in comparison with the typical memory pattern.

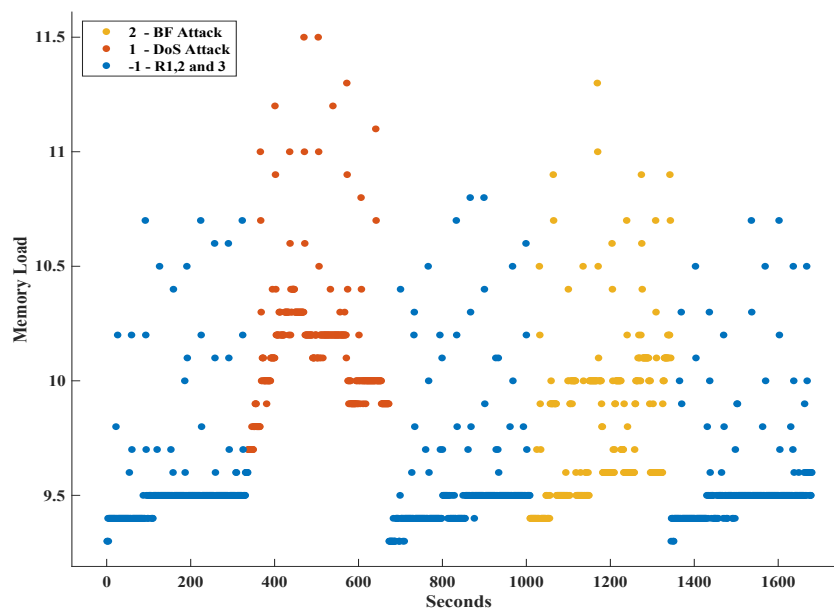


Figure 5-10. Memory pattern classification (Rs cases vs. DoS and BF).

Even though the memory usage rates under the cyber-attacks overlapped within the normal range of memory usage (Figures 5-10 and 5-11), the anomalous pattern enabled us to detect the attacks due to the distinguishability of these patterns.

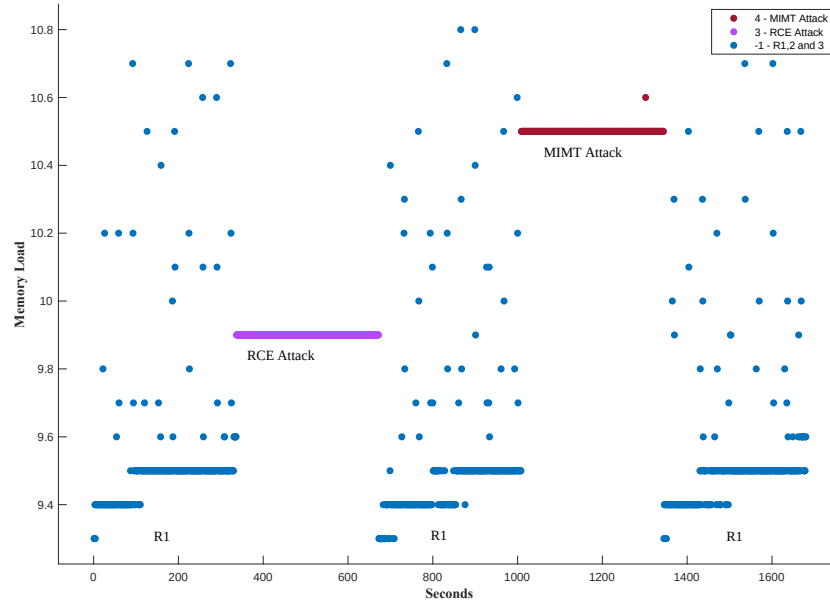


Figure 5-11. Memory pattern classification (Rs cases vs. RCE and MITM).

5.6.2.3. Tasks count

In terms of the executed processes count, the Rs case mode values were concentrated at 172 processes per second, and as the mode value is identical in R1, R2, and R3 (Table 5-2), this proves the ability to define a standard range and pattern for the RCP for the Smart PiCar. In contrast, the alive process patterns under all attack cases have been classified accurately as anomalous patterns, as shown in Figures 5-12 and 5-13. In Fig. 5-12, the range and pattern of the executed processes under the BF attack case shaped an abnormal pattern that departed from the normal range and pattern. Likewise, under the DoS attack, the executed process pattern was anomalous, but slightly overlapped with the typical pattern.

In the cases of RCE and MITM attacks (Fig. 5-13), there was more interference, but due to their anomalous patterns in terms of alive task count (Table 5-2), it was still possible to separate them using the QSVM algorithm, especially after taking into account the role of other predictors and features with regard to highlighting the anomaly. Based on that, it

becomes certain that the ability to detect the existence of cyber-attacks is a consequence of the executed tasks' irregular behaviour. This is done by defining a reference pattern of the performed tasks under normal operating conditions and then using anomalous patterns of executed processes as an indicator referring to the existence of the attack.

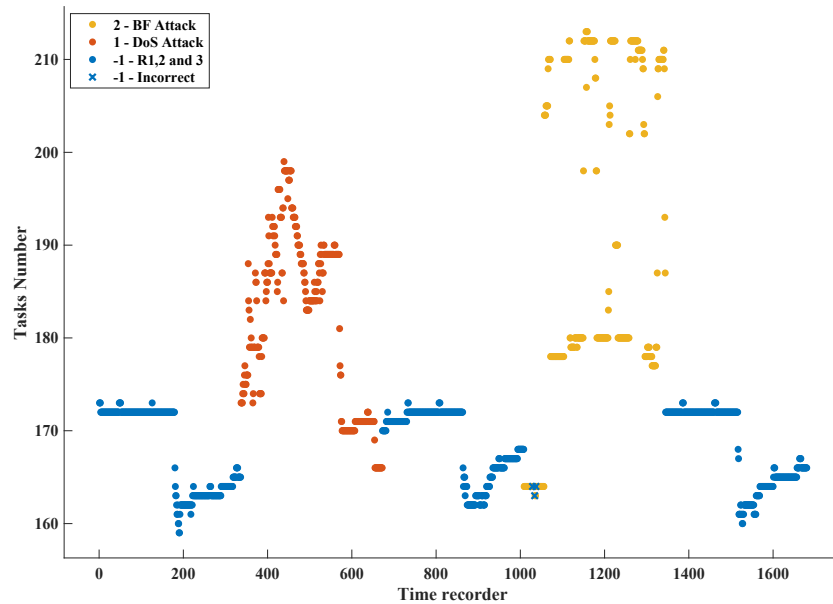


Figure 5-12. Task pattern classification (Rs cases vs. DoS and BF).

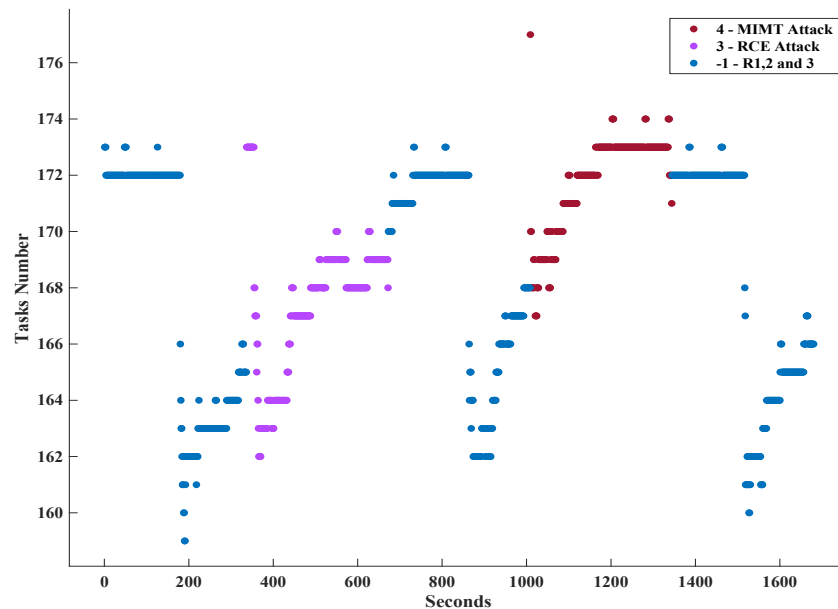


Figure 5-13. Task pattern classification (Rs cases vs. RCE and MITM)

5.6.2.4. Thread count

Regarding the executed threads, in the R1, R2, and R3 cases, the thread count was within a specified area (Fig. 5-14) and consistent pattern (Fig. 5-15). The number of executed

threads under normal conditions was identifiable (232 threads, Table 5-2). Thus, it can be defined as a standard performance pattern. On the other hand, the anomalous thread pattern under attack scenarios appeared on the RCP of the Smart PiCar. As shown in Figure 5-14, the pattern of executed threads under the DoS and BF attacks seemed to be anomalous. It spread more inconsistently across the Fig.14 axis compared to the usual performance pattern, which concentrated in a specific area.

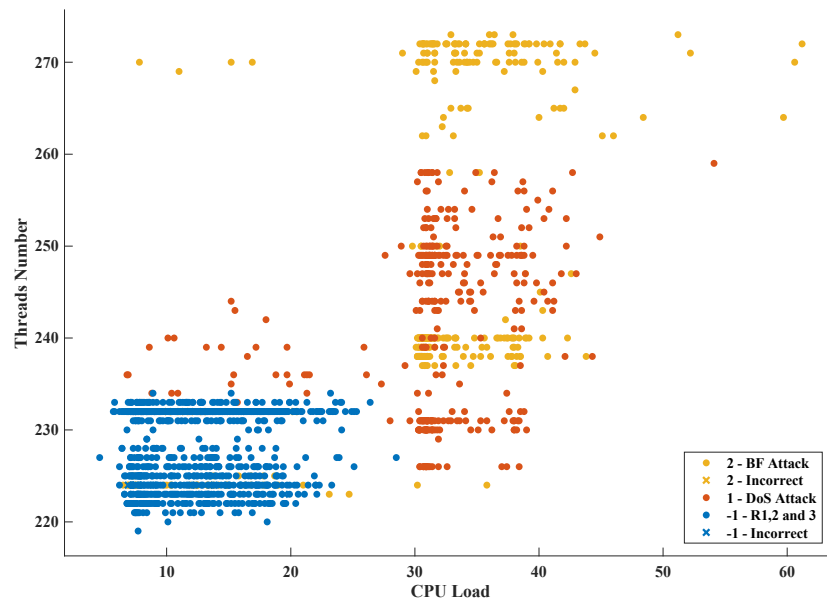


Figure 5-14. Thread pattern classification (*Rs* cases vs. DoS and BF).

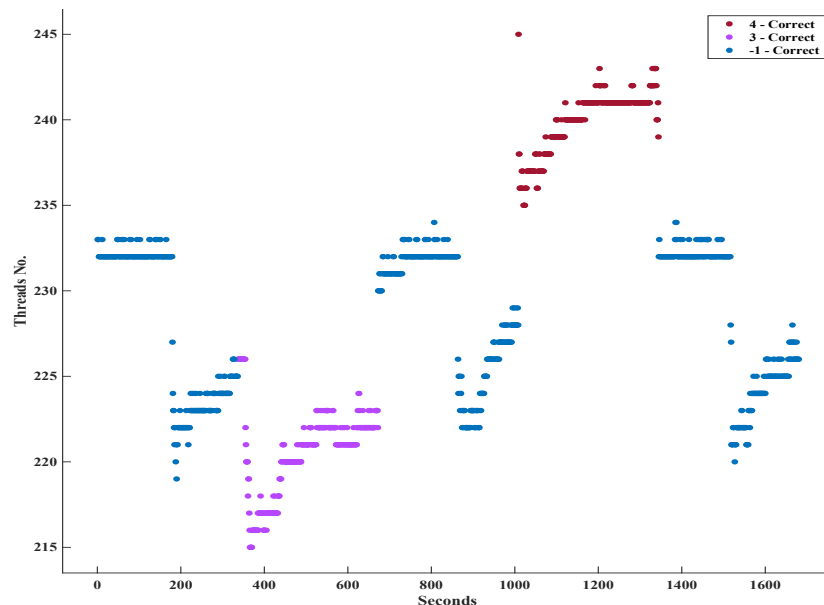


Figure 5-15. Thread pattern classification (*Rs* cases vs. RCE and MITM).

Also, Fig. 5-15 shows the pattern of thread count under normal operating conditions and its consistency compared to the Smart PiCar's behaviour under attack cases (RCE: purple dots, and MITM: burgundy dots). Therefore, the QSVM algorithm classifies the attack cases from non-attack cases efficiently. It was also noted that the QSVM algorithm classifies the irregular behaviour of the Smart PiCar under the MITM attack due to its complete deviation from the normal range. Whereas the MITM attack was detected because it deviated from the normal range, the other attack (RCE) was marked by its anomalous patterns despite being partially within the normal range. Moreover, the executed thread count in DoS, BF, and MITM cases reached unprecedented numbers, as shown in Table 5-2; also in the RCE attack case, the thread count significantly decreased in terms of the mode value compared with R1, R2, and R3 (see Table 5-2).

5.6.2.5. CPU temperature

The role played by the temperature of the CPU (ARMv8), as one of the data features in terms of distinguishing attack case patterns compared to the typical patterns, was valuable and meaningful, because it helped with the recognition of abnormal patterns resulting from the cyber-attacks. As shown in Figures 5-16 and 5-17 and Table 5-7, under normal operating conditions, the CPU temperature ranged from 38°C to 55°C. In contrast, the maximum CPU temperature in the presence of a cyber-attack reached values that were not previously recorded under normal conditions, such as 65°C, 63°C, and 60°C. This was after taking into consideration the ambient temperature and the initial temperature (Table 5-7).

Table 5-7: CPU temperature (°C)

Case	Initial	Maximum	Ambient	Diff.	Mode
R1	50	55	23	32	54
R2	38	52	21	31	50
R3	43	53	23	30	51
DoS attack	55	65.00	24	41	64
Brute-Force	51	63.00	25	38	60
RCE attack	59	60.00	25	35	54
MITM	55	60.00	25	35	55

The elevations in the CPU temperature during the attack periods indicate unconventional levels of CPU temperature. Based on the results of Table (5-7), it was noted that the

differences between the maximum temperatures and the ambient temperatures in R1, R2, and R3 were 32°C, 31°C, and 30°C respectively. In comparison, this difference turned to 41°C, 38°C, 35°C, and 35°C under attack conditions. The unusual maximum CPU temperatures support the anomaly-detection technique more closely.

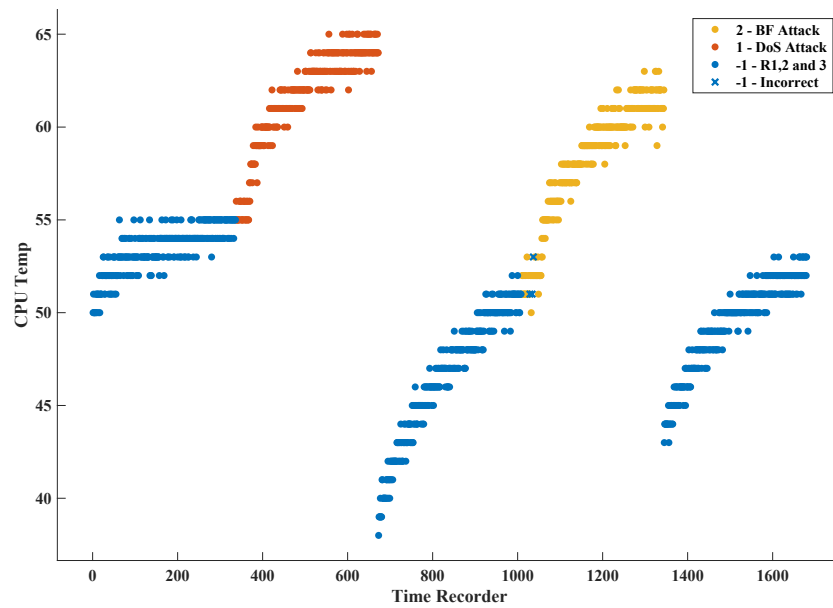


Figure 5-16. CPU temp. pattern classification (*Rs* cases vs. DoS and BF).

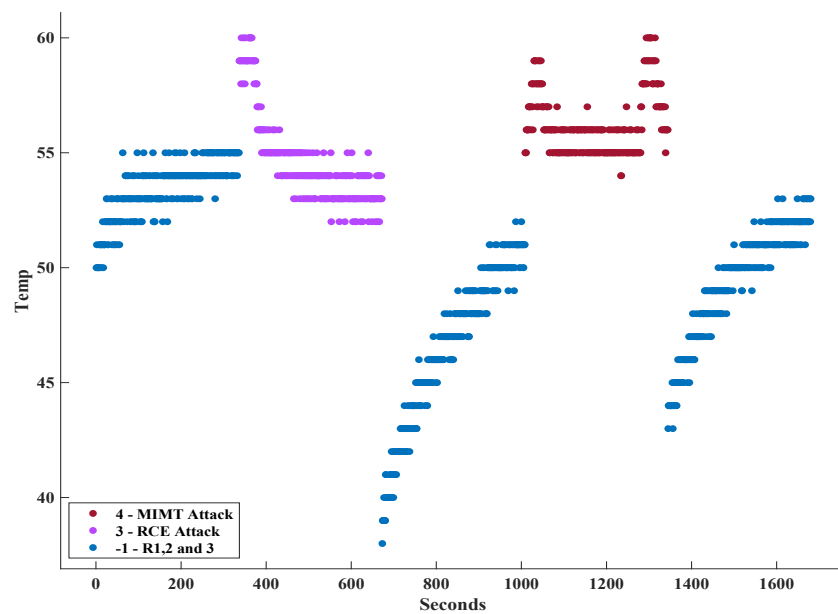


Figure 5-17. CPU temp. pattern classification (*Rs* cases vs. RCE and MITM).

As explained previously, ESs are designed to perform specific functions. Thus, it is to be expected that the ESs consume their resources and perform their functions in an identifiable pattern and in a manner that will be steadily reflected by the CPU temp. Thereby, any anomaly in terms of pattern or any divergence in terms of range compared to the standard pattern performance will indicate the presence of illegal activity, which requires an immediate response.

5.6.2.6. Power consumption

Turning to the power consumption rate as one of the predictors added to the training model, we note from Figures 5-18 and 5-19 that the voltage patterns of the smart PiCar under normal conditions (Rs cases) reflected a consistent power consumption pattern. Furthermore, this pattern can be identified and defined as a standard pattern, due to its significant similarities in R1, R2, and R3. On the other hand, the RCP of the Smart PiCar under the DoS attack, BF attack, and RCE attack caused abnormal patterns that have given the QSVM algorithm the ability to predict anomalous patterns more accurately and distinguish them from the patterns of the typical operations. It was also noticed through Fig. 19 that the power consumption under the MITM attack scenario was within the normal range, but at a different rate and an irregular pattern, and here the role of other features supports the ability to recognize the abnormality of the voltage pattern under attack circumstances.

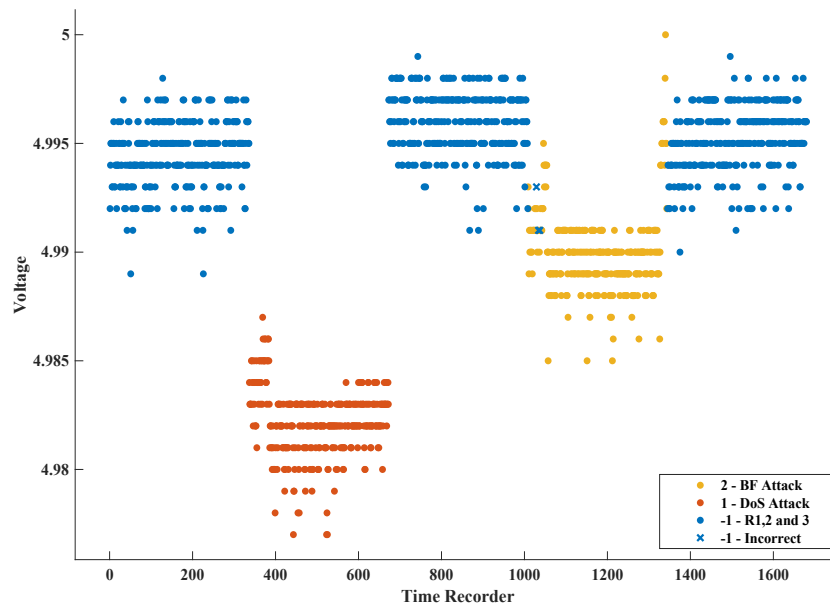


Figure 5-18. Voltage pattern classification (Rs cases vs. DoS and BF).

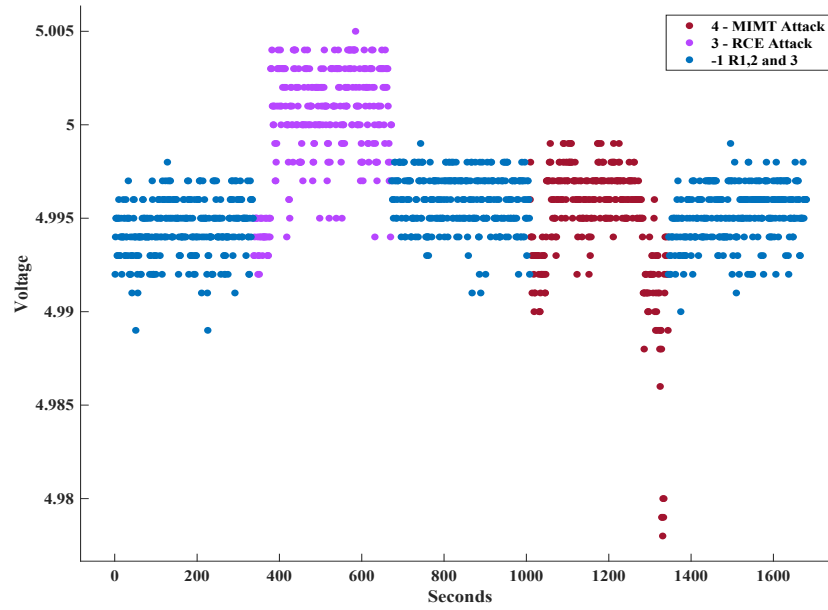


Figure 5-19. Voltage pattern classification (*Rs* cases vs. RCE and MITM).

In terms of the current pattern, as shown in Figures 5-20 and 5-21, the typical operating modes formed a consistent pattern. While under the attack cases, the current-voltage consumption rate patterns varied in each cyber-attack type. Therefore, this feature enhanced the QSVM algorithm's ability to recognize the cyber-attacks due to their anomalous effects on power consumption, whether voltage or current. In turn, this enhances the effectiveness of the proposed approach for detecting and responding to attacks.

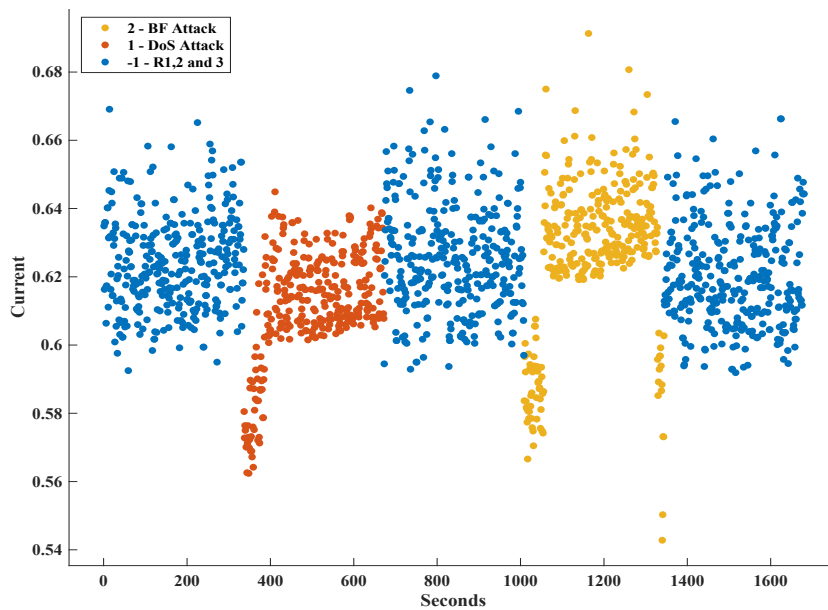


Figure 5-20. Current pattern classification (*Rs* cases vs. DoS and BF).

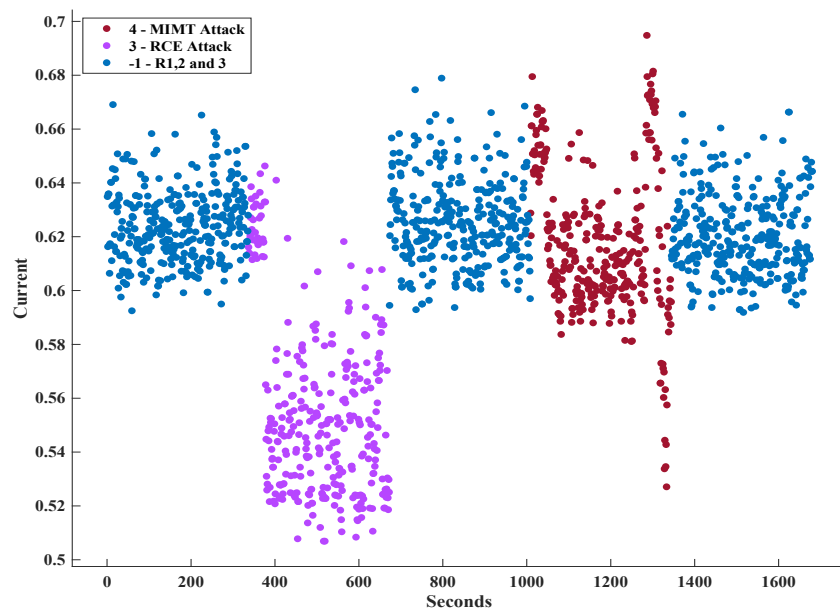


Figure 5-21. Current pattern classification (Rs cases vs. RCE and MITM).

5.6.2.7. Received & Transmitted Packet Rate

The rates of received and transmitted packets have been added to the second trained model (as data features) and to the second test model (as predictors). By looking at Figures 5-22 and 5-23, it was noticed that the QSVM algorithm greatly benefited from these predictors in detecting the anomalous pattern of the RCP, under the MITM attack in particular.

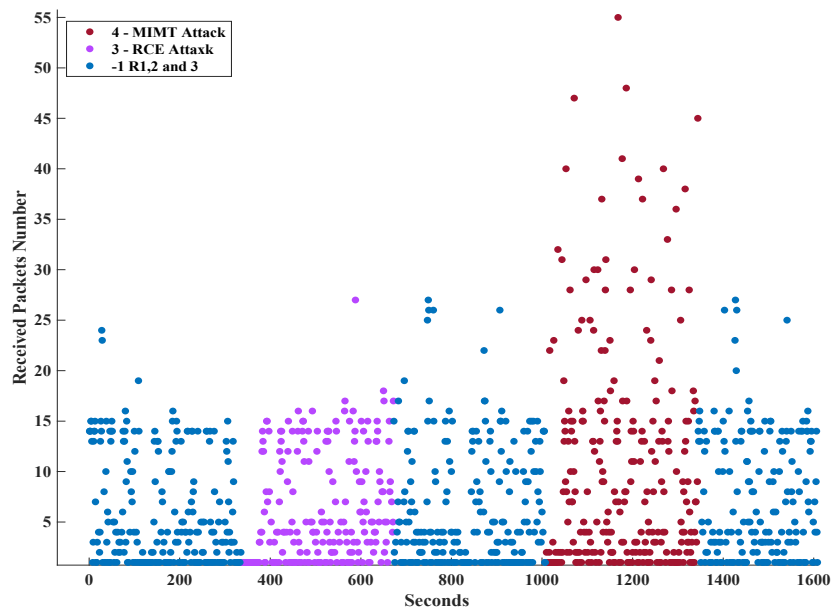


Figure 5-22. RX-rate pattern classification (Rs cases vs. RCE and MITM).

The RX and TX rates under the MITM attack circumstances reached unprecedented values that enabled the QSVM algorithm to detect the anomaly. Furthermore, the abnormal change in this particular feature, or predictor, will help to detect irregular patterns, detect attack presence, and determine the type of attack as a networked attack. In other words, the unjustified rate of received and transmitted packets indicates a networked attack incident, and this is what has been proven based on these results, both statistically and computationally.

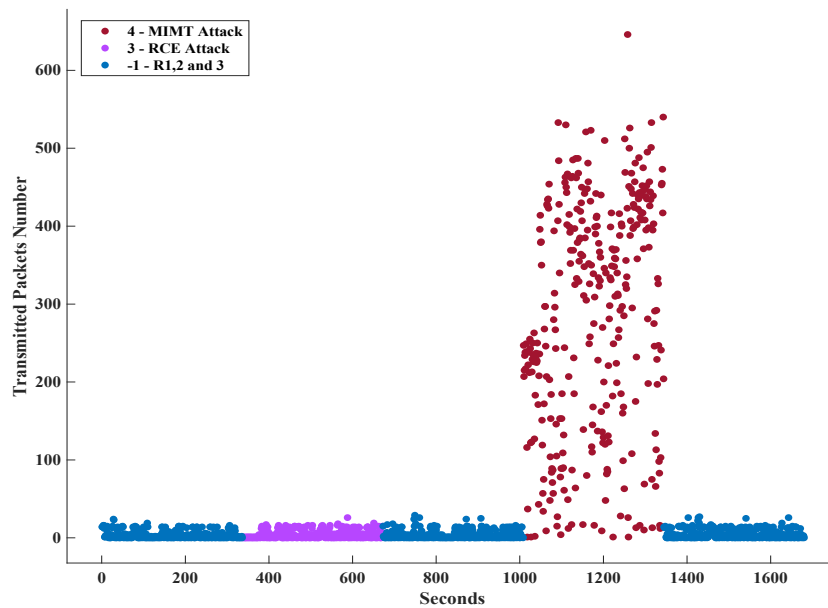


Figure 5-23. TX-rate pattern classification (Rs cases vs. RCE and MITM).

In addition, the average of received and transmitted packets while the system was running was consistent in a way that can be defined as a standard pattern; this will enable us to identify the presence of a networked attack, such as the blackhole attack. In the blackhole attack, the adversary will intentionally breach the data integrity by dropping the received or transmitted packets. Therefore, defining the supposed rate of received and transmitted packets based on specifiable system functions will help to detect any anomalies from the predefined standard pattern or any deviation from the typical range. As a side note, the received and transmitted packets were added after excluding the D+/D-(V) features and predictors, which were observed to be unchanged and had no contribution to the identification of abnormal patterns, as was the case with the other parameters and attributes. Throughout different types of attacks, these results compellingly proved the effectiveness of this technique for detecting cyber-attacks due to anomalies in RCP

patterns, taking into consideration the ability to determine a standard pattern from the TX and RX rates.

5.7. Architectural Framework of The Anomalous Resource Consumption Detection (ARCD) Approach

After proving the validity of the proposed approach in detecting cyber-attacks, in this section, we address the steps required to facilitate the adoption of this approach for software engineers and operating system designers. The architectural framework (Fig. 5-24) of the ARCD approach has been built in line with the multiple layers feedback framework of ES cybersecurity (MuLFESC) [22], where steps 1 to 4 take place in parallel with layers 1 to 3, and step 5, which is the detection mechanism, will be implemented in line with layers 3 to 5. Finally, steps 6 and 7 need to be considered in line with layers 7 to 9.

5.7.1. Determining The Components:

Defining the system's components is an essential step toward defining the ideal performance pattern and defining the functions that the system will perform. Also, determining the system's application domain will be positively reflected in the prediction of the nature of potential security risks. In our case study, the components of the CPS consist of the physical components that represent the physical parts of a smart car, in addition to the computational part. The physical components consist of:

- Hardware attached on top (Robot HAT),
- Pulse width modulation (PCA9685 PWM Driver x 1),
- Motor driver (TRA9118A x 1),
- Ultrasonic obstacle avoidance module x 1,
- DC gear motor x 2,
- Servo motor x 1,
- Power supply, in addition to the body components of the physical structure.

For the computational part, the Raspberry Pi 4 Model B+ was attached to the Smart PiCar to steer its functions, as the embedded system.

5.7.2. Determining The Functions:

Defining the “function” or “functions” for which the system is designed is a fundamental and major step. The determination of system functions is closely related to the recognition of the supposed typical performance. As mentioned earlier, the ESs are dedicated to performing specific functions (sensing, computing, controlling, opening or closing valves, switching, sending and receiving signals, and influencing outcomes in the real world through physical processes), which distinguishes them from conventional multitasked systems. This unique feature makes ESs stand out from traditional computers and enabled us to develop this security approach to protect them. ESs are limited in capabilities due to their nature, which requires them to be small, easy to integrate, inexpensive, portable, and installed in remote sites in harsh conditions, where their energy source is often limited. All these limitations make the application of advanced security solutions effectively impossible. On the other hand, the fact that this type of system is by nature designed to perform specific functions enabled us to use this characteristic to develop this security approach for detecting cyber-attacks.

In our case study, the system functions can be determined as follows: (1) performing reconnaissance tasks in a specific area and making the Smart PiCar move autonomously while maintaining its continuous movement by (2) attaching and enabling an ultrasound module to avoid obstacles and finally, (3) activating an attached recording camera to capture the surrounding area. These are the functions that the CPS was designed to perform.

5.7.3. Identifying The Typical Pattern:

Defining the typical, expected, and optimal performance patterns is a fundamental step, and it can be made based on the repeated operation of the CPS’s functions and by then collecting specific parameter values, which represent the system’s performance and resource consumption. Then, these values are analysed statistically by applying the septenary tuple model, which consists of seven statistical criteria: minimal, maximal, range, median, mean, mode, and standard deviation on the collected parameter values, and these parameters are: (X): CPU utilisation (U), memory load (M), CPU temp. (T), power consumption (P), task count (N), thread count (Θ), and rates of received and

transmitted packets (R), where X refers to a parameter. The CPS must be operated repeatedly under ideal operating conditions (no malfunctions, or presence of cyber-attacks). The collected values must be analysed statistically to determine the pattern and the range of each round's performance. To determine the typical ranges (Std_r) of each parameter, the minimal (X_{minV}), maximal (X_{maxV}), and range (X_{gV}) values need to be calculated, and to determine the standard pattern (Std_p), the following values need to be calculated: the median (X_{midV}), mean (X_{avgV}), mode (X_{modV}), and standard deviation (X_{stdV}). Based on (1) the arithmetic mean, we can determine the average performance and resource consumption for each testbed parameter. Based on the (2) mode value, we can determine the most frequent value recorded while the system performs its functions. Thus, we can know the central tendency or density point value and determine the performance and resource consumption patterns. Based on the (3) median value, we can find the middle number in a sorted list of values. Also, the (4) standard deviation criterion will be applied to measure how spread-out the numbers are.

To define the typical range of the RCP, we need to calculate three mathematical criteria—these criteria as follows: (5) maximum value, which is the highest value among the dataset collected during a completed operation cycle in which the system performed all its functions. (6) The minimum value, which is the lowest value recorded while the system was performing its functions. Finally, the distribution range of the values is determined by subtracting the maximum value and the minimum value.

In our case, the Smart PiCar was turned on three times in a row ($R1, R2, R3$), and the values of each parameter (X) = $\{U, M, N, \mathcal{G}, T, P, R\}$ were collected for each run, in which all system functions were performed completely. After analysing these parameters statistically according to the septenary tuple model, the results revealed a significant similarity that often reached the point of congruence, thus proving the possibility of defining a standard performance pattern.

In the machine learning context, whenever the patterns of operation in normal conditions show great congruence or convergence in terms of performance and resource consumption, there is less need for data training based on the supervised learning method. Conversely, whenever the patterns of operation under normal operating conditions have diverged, the greater the need for more data training sessions to reach the optimal standard

pattern. Therefore, the required training overhead is mainly dependent on the level of convergence or variance in operating patterns under normal conditions.

In contrast, the required training overhead to distinguish the generated standard pattern derived from typical operations versus anomalous patterns depends on the level of anomaly. The greater the anomaly from the standard pattern, the easier it is to detect the attack, and therefore the need to train the data based on the supervised learning method decreases. The lower the level of anomaly, the greater the need for more data training sessions to accurately define the detection threshold without confusion and to prevent a false positive case.

5.7.4. Generating A Standard Model as A Reference Pattern:

The main purpose of recognizing typical performance patterns based on the parameter values that have been analysed statistically is to generate a standardized reference model for a particular implementation of a CPS. The generated model will act as a reference and control model of the optimal performance to distinguish anomalous patterns that deviate from it; this means we are exploiting the anomaly in performance and resource consumption as an indicator that reveals the existence of a cyber-attack, which requires an immediate response. Defining a standard pattern that serves as a reference model will contribute to developing the detection mechanism and improve the CPS performance by imposing the necessary restrictions on resource consumption to prevent the depletion of system resources resulting from unintended software errors or misuse. In our case study, the reference model (Chapter 4, Table 4-12) was defined based on the Rs cases' statistical analysis results. To create a flexible reference model, we determined the reference models' values as a set of values that fall between the highest and lowest values among Rs cases for each statistical criterion. In other words, the maximal values of the reference model for each statistical criterion are the highest values among the maximum values of Rs cases, and the minimum value is the lowest value among the minimum values of Rs cases. Additionally, consideration was given to the probability of having values very close to those of the reference model by calculating and adding the most significant differences between Rs cases (Table 5-2) to the reference model values.

5.7.5. Designing and Applying the Detection Mechanism:

The detection mechanism is the core of the architectural framework. The detection technique is based on recognizing anomalous patterns of the system's performance by observing specific values of selected statistical criteria for designated parameters that are compared to the generated reference model, as illustrated in Fig. 5-24. Thus, the outlier values are categorized as abnormal values, indicating an anomalous pattern that requires immediate action. The RCP pattern deviation from the standard predefined performance level enables the OS layer to predict a cyber-attack's existence. This mechanism was developed after proving that the ESs have an identifiable pattern under normal operating conditions. Also, it was proven that ESs, during exposure to various cyber-attacks, change their performance patterns and their resource consumption in a way that can be distinguished compared to their typical performance. By adopting this mechanism, it becomes possible to detect cyber-attacks based on deviation from the normal range and based on the abnormality of the pattern within the normal range.

5.7.6. Monitoring The System Performance Pattern:

After the detection mechanism is designed, it must be activated as an integral part of the operating system layer. Activating the mechanism involves permanent monitoring of the statistical classification criteria of the performance parameters by observing any deviation from the reference performance model. Embedding the detection mechanism instructions within the OS architecture will create an additional layer of protection. As long as there are no anomalies in the performance or resource consumption patterns, there will be no need to take any action; however, the moment the performance or resource consumption patterns deviate from the defined reference patterns, or its values diverge out of the normal range, then the system must immediately alert the user about the anomaly and attract attention by generating a sound alert or by displaying a warning message. The next step is then to automate the operating system layer by executing an appropriate procedure to prevent the attack.

However, if the functions that the ES was designed to perform have been modified, it is possible that the detected resource utilisation pattern might be categorized as an anomalous pattern, even if it is due to legitimate processes. Therefore, it is mandatory to

regenerate a new reference pattern according to the modified functions by following steps three and four. Also, as relying on one parameter might lead to false-positive detection, combining a set of parameters will increase the accuracy of prediction, thus preventing such case.

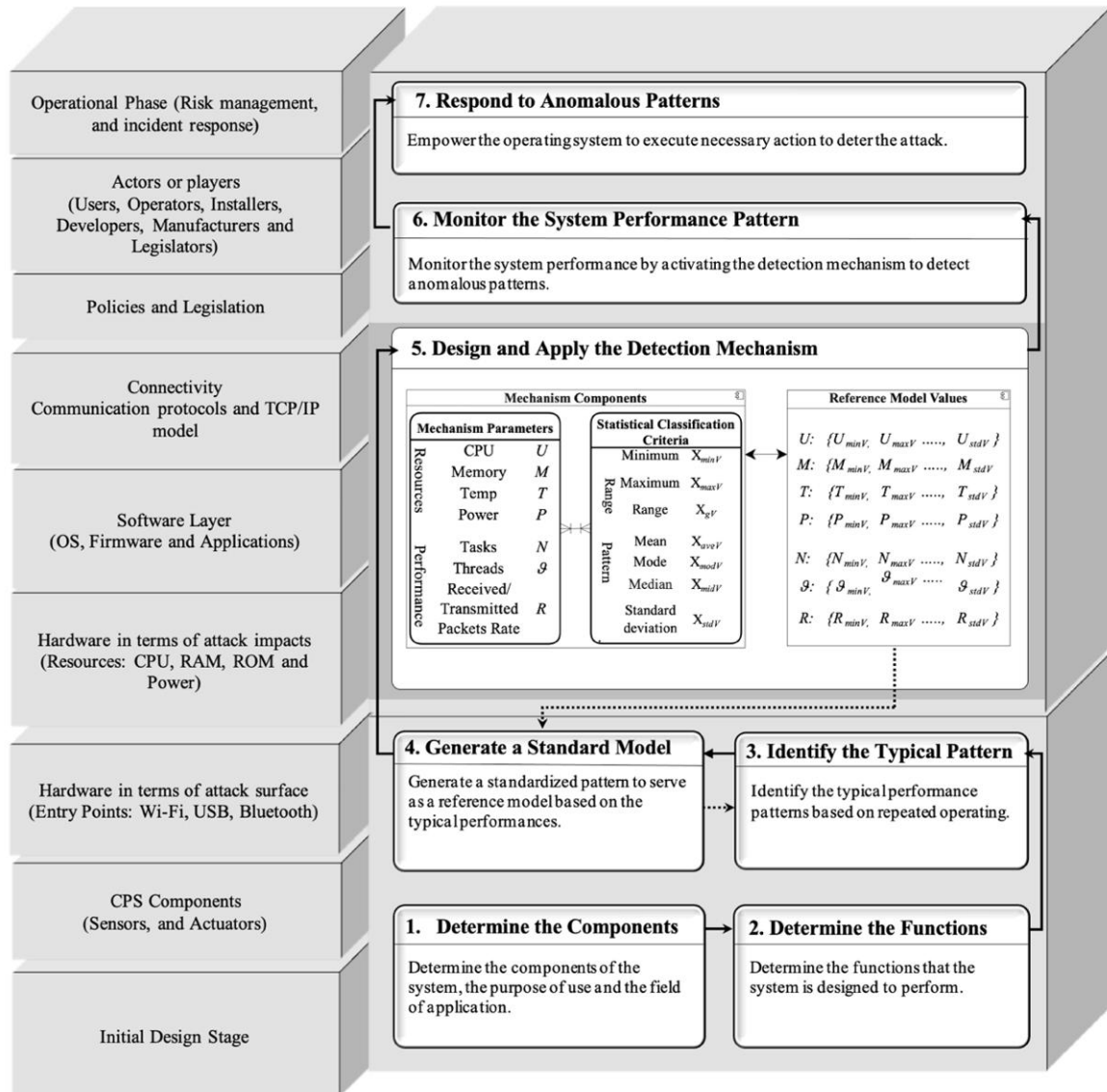


Figure 5-24. Architectural framework of ARCD approach.

In terms of the detection latency, which is the time between the initiation of the attack and it being detected, based on the proposed approach, it will be the time required to statistically evaluate the parameters' values as well as the time of anomaly formation in the performance pattern. The results of the DoS and password attack scenarios (Chapter

4, Sec 4.8) show that the DoS attack was executed at 00:26:25s with the abnormal pattern appearing at 00:26:26s, and the password attack was executed at 00:16:16s with the anomaly pattern starting to form at 00:16:18s (a 1s delay). Therefore, the time between attack execution and detection, considering the time taken to monitor the stat values in real-time, will be between 2000ms to 3000ms (Chapter 4 (Tables 4-17 and 4-18), and Chapter 6 (Fig. 6-11)). The following figure gives a visualization of the sequence of events and the timeline for detecting the attack according to the proposed approach.

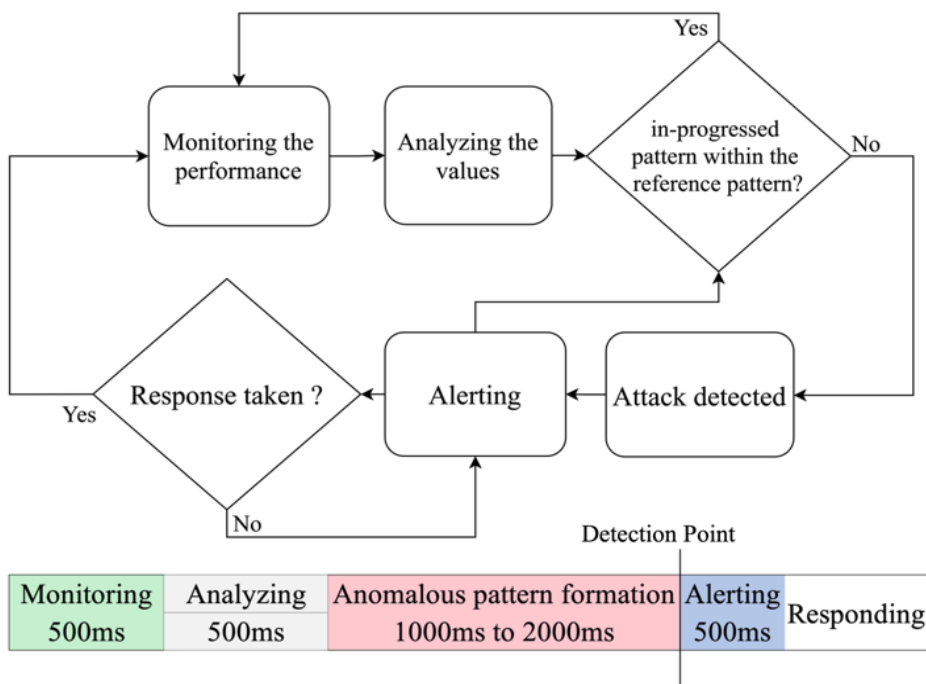


Figure 5-25. Chronology of the attack detection and events sequence.

5.7.7. Responding To Anomalous Patterns:

It would be best to build an autonomous response into the OS architecture, in order to benefit from the anomalous pattern auto-detection and provide an optional interaction from the user. The available response options for an operating system mainly depend on the OS layer's architecture and the hardware components used in the system construction. Automating the operating system's response to prevent attacks should not be an obstacle for software developers, as we have demonstrated the ability to detect a cyber-attack based on anomalous pattern recognition.

5.8. Conclusion

The proposed approach derived its rationale from three arguments. First, unlike conventional multitasked computer systems, ESs are dedicated to performing specific functions. Thus, (secondly) it was assumed that these systems perform their functions and consume their resources in a consistent pattern, therefore, extracting or generating a standard pattern based upon the typical patterns is possible. Third, based on the second argument, it was assumed that these systems might form observable anomalies in their performance and resource consumption patterns while being subjected to cyber-attacks. Thus, these anomalous patterns would deviate from the pre-defined standard pattern, and we have proven that it is possible to define this pattern in advance. All these assumptions were proven to be accurate.

By merging these findings, the approach's rationale was presented in a hypothesis, and the QSVM algorithm was used to test its validity. Thus, the approach's effectiveness has been tested and statistically and computationally validated by means of a testbed experiment. The high prediction accuracy percentages presented in the confusion matrices revealed promising results, proving this approach's effectiveness. Accordingly, the ARCD approach's architectural framework was developed to facilitate this approach's adoption by software engineers. The ARCD approach acts as an additional layer of protection for ESs, and it uses the system performance's irregular behaviour to reflect in the hardware and software layers as suggested improvements, without excessive computational requirements or additional hardware component costs. This is due to the statistical detection mechanism based on anomalous performance pattern recognition. The aim of delivering this approach is to detect cyberattacks without conflicting with the embedded system's characteristics. Thus, the ARCD approach has paved the way for software engineers to strengthen operating systems and enhance their rigidity and reliability.

5.9. References:

1. Papp D., Ma Z., Buttyan L. Embedded systems security: Threats, vulnerabilities, and attack taxonomy. 2015 13th Annual Conference on Privacy, Security and Trust, PST 2015. IEEE; 2015; : 145–152. Available at: DOI:10.1109/PST.2015.7232966
2. Vahid F., Givargis T. Embedded System Design: A Unified Hardware/Software Approach. 1999; : 103.
3. Pham Van P Van., Binh NN. Embedded System Architecture Design and Optimization at the Model Level. International Journal of Computer and Communication Engineering. 2012; 1(4): 345–349. Available at: DOI:10.7763/ijcce.2012.v1.87
4. Levy E. Crossover: online pests plaguing the off line world. IEEE Security & Privacy. November 2003; 1(6): 71–73. Available at: DOI:10.1109/MSECP.2003.1253573
5. He H., Maple C., Watson T., Tiwari A., Mehnen J., Jin Y., et al. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing other computational intelligence BT - 2016 IEEE Congress on Evolutionary Computation, CEC 2016, July 24, 2016 - July 29, 2016. IEEE Internet of Things Journal. 2016; : 1015–1021. Available at: DOI:10.1109/CEC.2016.7743900
6. Abomhara M., Køien GM. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility. 2015; 4(1): 65–88. Available at: DOI:10.13052/jcsm2245-1439.414 (Accessed: 27 July 2019)
7. Ravi S., Kocher P., Lee R., McGraw G., Raghunathan A. Security as a new dimension in embedded system design. Proceedings of the 41st annual conference on Design automation - DAC '04. New York, New York, USA: ACM Press; 2004. p. 753. Available at: DOI:10.1145/996566.996771
8. Hameed S., Khan FI., Hameed B. Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review. Journal of Computer Networks and Communications. 10 January 2019; 2019: 1–14. Available at:

- DOI:10.1155/2019/9629381
9. MESHRAM VH., SASANKAR AB. Security in Embedded Systems: Vulnerabilities , Pigeonholing of Attacks and Countermeasures. IOSR Journal of Computer Engineering. 2016; : 11–15.
 10. Bodei C., Chessa S., Galletta L. Measuring security in IoT communications. Theoretical Computer Science. Elsevier B.V.; 2019; 764: 100–124. Available at: DOI:10.1016/j.tcs.2018.12.002
 11. Parameswaran S., Wolf T. Embedded systems security—an overview. Design Automation for Embedded Systems. 17 September 2008; 12(3): 173–183. Available at: DOI:10.1007/s10617-008-9027-x (Accessed: 27 July 2019)
 12. Hwang DD., Schaumont P., Tiri K., Verbaauwhede I. Securing embedded systems. IEEE Security & Privacy Magazine. March 2006; 4(2): 40–49. Available at: DOI:10.1109/MSP.2006.51
 13. Marwedel P. Embedded System Design. Cham: Springer International Publishing; 2018. Available at: DOI:10.1007/978-3-319-56045-8 (Accessed: 15 August 2019)
 14. Wang W., Zhang X., Hao Q., Zhang Z., Xu B., Dong H., et al. Hardware-Enhanced Protection for the Runtime Data Security in Embedded Systems. Electronics. 2 January 2019; 8(1): 52. Available at: DOI:10.3390/electronics8010052 (Accessed: 8 September 2019)
 15. Radoglou Grammatikis PI., Sarigiannidis PG., Moscholios ID. Securing the Internet of Things: Challenges, threats and solutions. Internet of Things. Elsevier B.V.; 2018; 5: 41–70. Available at: DOI:10.1016/j.iot.2018.11.003
 16. Liu X., Zhao M., Li S., Zhang F., Trappe W. A Security Framework for the Internet of Things in the Future Internet Architecture. Future Internet. 28 June 2017; 9(3): 27. Available at: DOI:10.3390/fi9030027 (Accessed: 27 July 2019)
 17. Chai H., Zhang G., Zhou J., Sun J., Huang L., Wang T. A Short Review of Security-Aware Techniques in Real-Time Embedded Systems. Journal of Circuits, Systems and Computers. 12 February 2019; 28(02): 1930002. Available at: DOI:10.1142/S0218126619300022 (Accessed: 8 September 2019)
 18. Riahi Sfar A., Natalizio E., Challal Y., Chtourou Z. A roadmap for security challenges in the Internet of Things. Digital Communications and Networks. Elsevier Ltd; 2018; 4(2): 118–137. Available at: DOI:10.1016/j.dcan.2017.04.003

19. Habibzadeh H., Nussbaum BH., Anjomshoa F., Kantarci B., Soyata T. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*. Elsevier; October 2019; 50(June): 101660. Available at: DOI:10.1016/j.scs.2019.101660
20. Humayed A., Lin J., Li F., Luo B. Cyber-Physical Systems Security - A Survey. *IEEE Internet of Things Journal*. 2017; 4(6): 1802–1831. Available at: DOI:10.1109/JIOT.2017.2703172
21. Ali S., Al Balushi T., Nadir Z., Hussain OK. Risk Management for CPS Security. *springer*. Cham: Springer International Publishing; 2018. pp. 11–33. Available at: DOI:10.1007/978-3-319-75880-0_2 (Accessed: 15 August 2019)
22. Alooseel A., He H., Shaw C., Khan MA. Analytical Review of Cybersecurity for Embedded Systems. *IEEE Access*. 2021; 9: 961–982. Available at: DOI:10.1109/ACCESS.2020.3045972
23. Zhang X-D. Machine Learning. A Matrix Algebra Approach to Artificial Intelligence. Singapore: Springer Singapore; 2020. pp. 223–440. Available at: DOI:10.1007/978-981-15-2770-8_6
24. Hwang R-H., Peng M-C., Huang C-W., Lin P-C., Nguyen V-L. An Unsupervised Deep Learning Model for Early Network Traffic Anomaly Detection. *IEEE Access*. 2020; 8: 30387–30399. Available at: DOI:10.1109/ACCESS.2020.2973023
25. Shimeall TJ., Spring JM. Recognition Strategies. *Introduction to Information Security*. Elsevier; 2014. pp. 253–274. Available at: DOI:10.1016/B978-1-59749-969-9.00012-2
26. Meira J., Andrade R., Praça I., Carneiro J., Bolón-Canedo V., Alonso-Betanzos A., et al. Performance evaluation of unsupervised techniques in cyber-attack anomaly detection. *Journal of Ambient Intelligence and Humanized Computing*. 7 November 2020; 11(11): 4477–4489. Available at: DOI:10.1007/s12652-019-01417-9
27. Ahmed M., Mahmood AN. Novel Approach for Network Traffic Pattern Analysis using Clustering-based Collective Anomaly Detection. *Annals of Data Science*. 14 March 2015; 2(1): 111–130. Available at: DOI:10.1007/s40745-015-0035-y
28. FONTUGNE R., HIMURA Y., FUKUDA K. Evaluation of Anomaly Detection

- Method Based on Pattern Recognition. *IEICE Transactions on Communications*. 2010; E93-B(2): 328–335. Available at: DOI:10.1587/transcom.E93.B.328
29. Shabtai A., Kanonov U., Elovici Y., Glezer C., Weiss Y. “Andromaly”: a behavioral malware detection framework for android devices. *Journal of Intelligent Information Systems*. 6 February 2012; 38(1): 161–190. Available at: DOI:10.1007/s10844-010-0148-x
 30. Moustafa N., Hu J., Slay J. A holistic review of Network Anomaly Detection Systems: A comprehensive survey. *Journal of Network and Computer Applications*. Elsevier Ltd; February 2019; 128(October 2018): 33–55. Available at: DOI:10.1016/j.jnca.2018.12.006
 31. Latif S., Zou Z., Idrees Z., Ahmad J. A Novel Attack Detection Scheme for the Industrial Internet of Things Using a Lightweight Random Neural Network. *IEEE Access*. 2020; 8: 89337–89350. Available at: DOI:10.1109/ACCESS.2020.2994079
 32. Gulenko A., Wallschlagler M., Schmidt F., Kao O., Liu F. Evaluating machine learning algorithms for anomaly detection in clouds. 2016 IEEE International Conference on Big Data (Big Data). IEEE; 2016. pp. 2716–2721. Available at: DOI:10.1109/BigData.2016.7840917
 33. Tao X., Peng Y., Zhao F., Zhao P., Wang Y. A parallel algorithm for network traffic anomaly detection based on Isolation Forest. *International Journal of Distributed Sensor Networks*. 27 November 2018; 14(11): 155014771881447. Available at: DOI:10.1177/1550147718814471
 34. Chen C-L., Chen H-C. A resource utilization measurement detection against DDoS attacks. 2016 9th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI). IEEE; 2016. pp. 1938–1943. Available at: DOI:10.1109/CISP-BMEI.2016.7853035
 35. Schnorr LM., Legrand A., Vincent J-M. Detection and analysis of resource usage anomalies in large distributed systems through multi-scale visualization. *Concurrency and Computation: Practice and Experience*. October 2012; 24(15): 1792–1816. Available at: DOI:10.1002/cpe.1885
 36. Feinstein L., Schnackenberg D., Balupari R., Kindred D. Statistical approaches to DDoS attack detection and response. *Proceedings DARPA Information*

- Survivability Conference and Exposition. IEEE Comput. Soc; 2003. pp. 303–314. Available at: DOI:10.1109/DISCEX.2003.1194894
37. Seo J., Lee S. Abnormal Behavior Detection to Identify Infected Systems Using the APChain Algorithm and Behavioral Profiling. Security and Communication Networks. 2018; 2018. Available at: DOI:10.1155/2018/9706706
38. Agrawal B., Wiktorski T., Rong C. Adaptive real-time anomaly detection in cloud infrastructures. Concurrency Computation . New York, NY, USA: ACM; 25 December 2017; 29(24): e4193. Available at: DOI:10.1002/cpe.4193
39. Lazri K., Laniepce S., Zheng H., Ben-Othman J. AMAD: Resource Consumption Profile-Aware Attack Detection in IaaS Cloud. 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing. IEEE; 2014. pp. 379–386. Available at: DOI:10.1109/UCC.2014.48
40. Liu S., Chen Y., Trappe W., Greenstein LJ. ALDO: An Anomaly Detection Framework for Dynamic Spectrum Access Networks. IEEE INFOCOM 2009 - The 28th Conference on Computer Communications. IEEE; 2009. pp. 675–683. Available at: DOI:10.1109/INFCOM.2009.5061975
41. Ding M., Xiong Z., Yu J. Anomaly Detection Based on Job Monitoring Metrics in Distributed System. 2018 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC). IEEE; 2018. pp. 182–186. Available at: DOI:10.1109/SPAC46244.2018.8965641
42. Cook AA., Misirli G., Fan Z. Anomaly Detection for IoT Time-Series Data: A Survey. IEEE Internet of Things Journal. 2020; 7(7): 6481–6494. Available at: DOI:10.1109/JIOT.2019.2958185
43. Cherkasova L., Ozonat K., Mi N., Symons J., Smirni E. Automated anomaly detection and performance modeling of enterprise applications. ACM Transactions on Computer Systems. 14 November 2009; 27(3): 1–32. Available at: DOI:10.1145/1629087.1629089
44. Hayes MA., Capretz MA. Contextual anomaly detection framework for big sensor data. Journal of Big Data. 27 December 2015; 2(1): 2. Available at: DOI:10.1186/s40537-014-0011-y
45. Watanabe S. Pattern Recognition: Human and Mechanical. USA: John Wiley & Sons, Inc.; 1985.

46. The MathWorks I. <https://www.mathworks.com/products/matlab.html>.
47. Moler C., Little J. A history of MATLAB. Proceedings of the ACM on Programming Languages. 12 June 2020; 4(HOPL): 1–67. Available at: DOI:10.1145/3386331
48. Cortes C., Vapnik V. Support-vector networks. Machine Learning. September 1995; 20(3): 273–297. Available at: DOI:10.1007/BF00994018
49. Noble WS. What is a support vector machine? Nature Biotechnology. December 2006; 24(12): 1565–1567. Available at: DOI:10.1038/nbt1206-1565
50. Cheng WK., Dibble B., Assanis D. Guest editorial vapnik-chervonenkis (vc) learning theory and its applications. IEEE Transactions on Neural Networks. 1 September 1999; 10(5): 985–987. Available at: DOI:10.1109/TNN.1999.788639
51. Vapnik VN. An overview of statistical learning theory. IEEE Transactions on Neural Networks. 1999; 10(5): 988–999. Available at: DOI:10.1109/72.788640
52. Zhen H., Hong L., Mujiao F., Chunbi X. Application of statistical learning theory to predict corrosion rate of injecting water pipeline. 9th IEEE International Conference on Cognitive Informatics (ICCI'10). IEEE; 2010. pp. 132–136. Available at: DOI:10.1109/COGINF.2010.5599754

CHAPTER 6: DISCUSSION

CHAPTER 6: DISCUSSION

This chapter will focus on the real-world impact of the findings from this research. To understand the implications and potential implementation of the MuLFESC framework and the ARCD approach, the discussion in this chapter has been presented in the form of questions and answers from the supervisors, review panel members, IEEE reviewers and an expert from the industry. Additionally, the content of this chapter is based on the published discussion sections in [1], [2], [3].

6.1. How can the Security Risk Metrics Model be leveraged in parallel with the MuLFESC framework?

The security risk metrics model can be leveraged in parallel with the MuLFESC framework from the perspective of the assessment. For example, tackling attacks from the angle of asset value will lead to the enactment of the necessary policies in layer 7 to protect the assets according to the sensitivity of the data. Additionally, addressing attacks based on the attack surface will help in disabling unnecessary entry points in layer 3. Evaluating attacks from the targeted network layer will help in adopting the most secure and appropriate protocol. Therefore, the reflected feedback on layer 1 fed from other layers (Figure 3-3) as a continuous process will be enriched by considering these perspectives to achieve best practice and to implement a compatible countermeasure, thus avoiding any conflict with the requirements of the other layers. The multi-security risk metrics (Figure 3-1) might help in predicting the biggest possible number of cyber-attacks in terms of methods, types, surfaces, TCP/IP layer, and limitations of the ES's resources [1].

6.2. What is the main purpose of developing the MuLFESC framework?

MuLFESC provides a guidance for 'security by design', which is required by industry 4.0. The design stage is essential for the implementation of the CSES. The engineering cycle of the CSES, such as implementation, test and verification, is critical for the final security of a system, and the security of algorithms and protocols. Optimal security

solutions are the comprehensive solutions that cover all aspects at various levels. This was extracted from an analysis of previous studies and the influencing factors. Based on that, the security framework shown in Figure 3-3 has been suggested as a reference for a comprehensive security assessment and solutions.

Overall, considering the identified key factors, the proposed MuLFESC, the risk assessment metrics and all involved parties of the CSES will allow security practitioners to conduct a comprehensive assessment. Thus, more efficient application-specific security solutions can be designed, thereby improving CPS cybersecurity [1].

6.3. Based on what, the detection mechanism of the ARCD approach derived its rationale to be effective and applicable within an OS of an ES?

The detection mechanism of the ARCD approach derived its rationale from compelling mathematical results of the testbed parameters that have been analysed by seven statistical criteria. The following subsections discuss these results in more detail [2]

6.3.1. CPU utilisation parameter

Based on the results shown in the CPU utilisation parameter (Table 6-1), it is clear to us that the CPU utilisation rates under normal operational conditions (R1, R2, and R3) are very similar, whether in terms of ranges or patterns.

Table 6-1: Overall CPU Performance for all Cases

P	Pattern				Range (X_{gv})		
	Mean	Median	Mode	Std.D	Range	Min	Max
R1	12.39	11.80	7.90	4.40	20.20	6.20	26.40
R2	12.68	12.40	7.70	4.35	20.50	4.60	25.10
R3	12.74	12.50	7.50	4.53	22.80	5.70	28.50
DoS	31.90	31.40	30.90	6.26	47.30	6.80	54.10
BF	31.16	31.50	30.50	9.13	54.70	6.50	61.20
RCE	12.33	10.40	6.20	7.51	32.20	4.90	37.10
MITM	15.87	12.60	7.40	9.05	33.60	5.30	38.90

The typical range of CPU utilisation extends from 4.6% as the lowest value among Rs cases to 28.50% as the highest value, and the typical pattern of CPU utilisation (mode value) was

concentrated at 7.90%, 7.70%, and 7.50% for R1, R2, and R3, respectively. Based on the significant similarity of these results in terms of range and pattern, we defined the standard pattern (Std_p) and range (Std_r) of CPU utilisation. Thereby, the validity of the first part of the hypothesis in terms of this parameter has been proven.

In contrast, the CPU utilisation under all cyberattack conditions without exception had shown anomalous patterns. Consequently, based on the mathematical results of the collected and analysed data, it is possible to distinguish the regular consumption from anomalous consumption in terms of range and pattern. Therefore, as long as we were able to define a standard utilisation of the CPU based on the embedded system's functions, the cyberattacks had a distinguishable anomalous impact on the CPU performance. Thus, it has been proven to us that cyberattacks can be detected based on this technique. When looking closely at the values in Table 6-1, we notice that the mean values in all cyberattack cases are sufficiently different except for the RCE attack, which is somewhat close to the average of R1, R2, and R3. However, it differed in its range, pattern, lowest values, and highest values, which created a discernible anomalous pattern that enabled its distinction, especially if we consider the other parameters' anomalous patterns impacts.

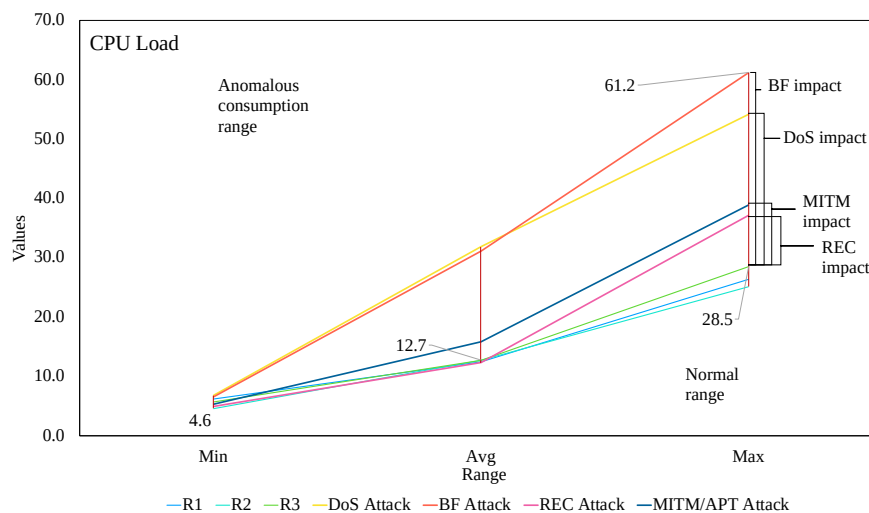


Figure 6-1. Overall CPU ranges for attacked cases vs standard cases.

In Figure 6-1, we see that the most deviated impacts of an attack from the normal range and pattern in terms of CPU utilisation compared to typical performance were the password attack (brute-force attack), followed by the denial-of-service attack, man-in-the-middle attack, and finally the remote code execution attack. Table 6-1 and Figure 6-1 show the effect that cyberattacks have had on the performance of the CPU. The abnormality of CPU

utilisation under the attack scenarios shows how these scenarios' CPU patterns deviated outside the normal range [2].

6.3.2. Memory usage parameter

Table 6-2 summarizes the final results that we obtained, and it clearly demonstrates that memory consumption in optimal operating conditions was not only similar but identical in terms of the most common value (9.50%), and the average is almost 9.5% in R1, R2, and R3. The lowest recorded value in R1, R2, and R3 was 9.30%. The highest values were 10.7%, 10.8%, and 10.7% for R1, R2, and R3, respectively. Thus, the possibility to define a standard pattern and range of the typical memory consumption due to its similarity pattern, which has reached a congruence level, has been proven.

Conversely, after analysing the pattern of memory consumption in the context of cyberattack cases, we notice that the general characteristic of the consumption pattern is anomalous compared to the standard patterns in R1, R2, and R3. Furthermore, defining the regular optimal pattern implicitly necessitates that any other patterns will be anomalous [2].

Table 6-2: Overall Memory Performance for all Cases

P	Pattern				Range		
	<i>Mean</i>	<i>Median</i>	<i>Mode</i>	<i>Std.D</i>	<i>Range</i>	<i>Min</i>	<i>Max</i>
R1	9.52	9.50	9.50	0.21	1.40	9.30	10.70
R2	9.51	9.50	9.50	0.23	1.50	9.30	10.80
R3	9.52	9.50	9.50	0.20	1.40	9.30	10.70
DoS	10.14	10.20	10.20	0.27	1.80	9.70	11.50
BF	9.78	9.60	9.60	0.33	1.90	9.40	11.30
RCE	9.90	9.90	9.90	0.00	0.00	9.90	9.90
MITM	10.50	10.50	10.50	0.01	0.10	10.50	10.60

Also, it is worth mentioning here that the impact of the cyberattacks does not necessitate the appearance of an abnormal increase, but rather, it may appear in the form of a decrease that calls attention and indicates the existence of function failure, such as that which occurred in the RCE attack scenario. In addition, the values distribution ranges in RCE and MITM attacks were 0 and 0.1, respectively, indicating the absence of alive activities and processes. Thus, it can be concluded that there was a malfunction in the system functions, and this is what exactly happened as the attacker in the RCE scenario disrupted

the recording camera. In the MITM attack, the camera was directed to an attacker's device to monitor streaming broadcasts instead of the recording function that was supposed to take place if it had not been hacked. Figure 6-2 demonstrates how the DoS and password attacks differ from the normal patterns of R1, R2, and R3. Also, how the RCE and MITM attacks shape an anomalous pattern in terms of memory usage compared to the normal performance can be seen.

In general, based on Table 6-2 and Figure 6-2, it becomes apparent that the memory parameter (M) fulfils the requirements to be a parameter that effectively detects cyberattacks in terms of anomalies and deviations from the normal range. Departing from the standard range requires an anomaly in the range of consumption. However, if consumption does not deviate from the defined standard range (Std_r), the anomalies in the patterns will be the vital factor in determining the feasibility of the parameter to be used to detect cyberattacks, and this is what happened in the RCE and MITM attacked cases.

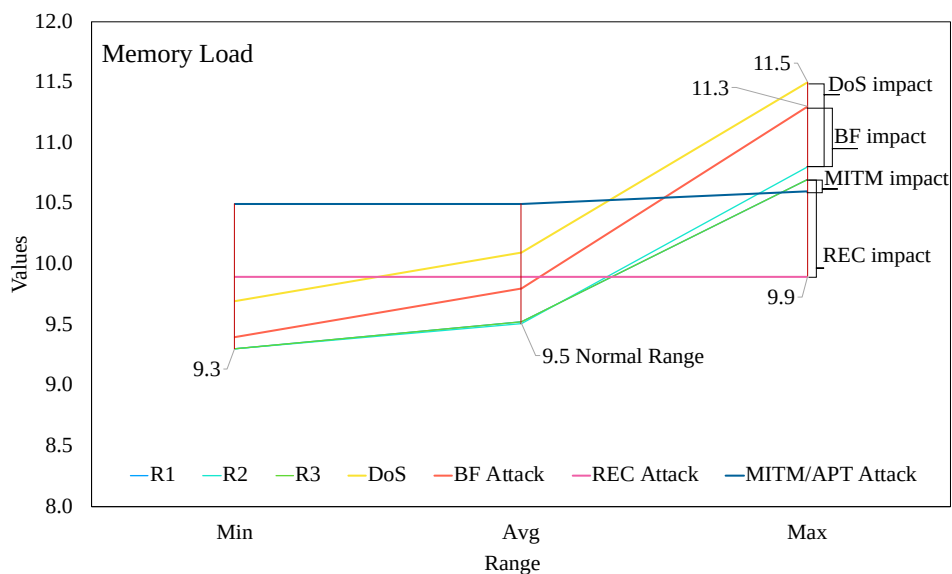


Figure 6-2. Overall memory ranges for attacked cases vs standard cases

Also, it is worth noting that the more coherent the typical consumption value is, the more precise a pattern is formed, from which the anomalous patterns are easily distinguished and vice versa. The more widespread the consumption values are, the more the pattern of attacks needs to be clearly anomalous to distinguish it. Therefore, when the mode values of Rs cases were identical precisely at 9.5%, any minor deviation would be enough to distinguish the anomalous pattern [2].

6.3.3. Tasks and Threads parameters

The numbers of alive tasks and threads are among the parameters of the testbed. Based on the analysis results in terms of executed tasks number, it has been precisely proven that the range and pattern of the regular performance of a Smart PiCar can be determined based on the collected values during repeated runs of the system's functions. As shown in Table 6-3, the normal ranges range between 173 tasks as the maximal value and 159 tasks as the minimal value. Also, the mean value (Std_{avgV}) is 168.2 tasks as the average of R1, R2, and R3. In addition, the median values (T_{midV}) were between congruence and similarity. Moreover, the standard deviation values were closely converging compared to the attacked cases. Table 6-3 summarizes these results.

In terms of pattern, the most frequent value or the density value was identical in R1, R2, and R3, which is 172 processes. This significant similarity in general and identity, in particular in terms of the most common values and maximum values, demonstrate to us the possibility of defining the normal range and pattern of tasks count that is supposed to be executed while the system performs its function under normal conditions. However, the tasks number values under the circumstances of cyberattacks with their anomalous patterns proves to us the effectiveness of this approach in detecting cyberattacks. Figure 6-3 illustrates the significant convergence in the pattern of tasks number in R1, R2, and R3 compared to attacked cases [2].

Table 6-3: Overall Tasks Number for all Cases

	Pattern				Range		
	<i>Mean</i>	<i>Median</i>	<i>Mode</i>	<i>Std.D</i>	<i>Range</i>	<i>Min</i>	<i>Max</i>
R1	167.90	172.00	172.00	4.52	14.00	159.00	173.00
R2	168.81	171.00	172.00	3.61	11.00	162.00	173.00
R3	168.15	172.00	172.00	4.17	13.00	160.00	173.00
DoS	181.64	184.00	171.00	9.39	33.00	166.00	199.00
BF	189.10	180.00	180.00	17.47	50.00	163.00	213.00
RCE	167.45	168.00	169.00	2.44	11.00	162.00	173.00
MITM	171.79	173.00	173.00	1.70	10.00	167.00	177.00

In the DoS attack scenario, the number of executed tasks reached 199 tasks. However, in the dictionary attack case, the number of executed tasks reached 213, which is an unprecedented value that caused an abnormality in the performance pattern compared to

Std_p and significantly deviated from the standard range (Std_r), as was also the case with the DoS attack [2].

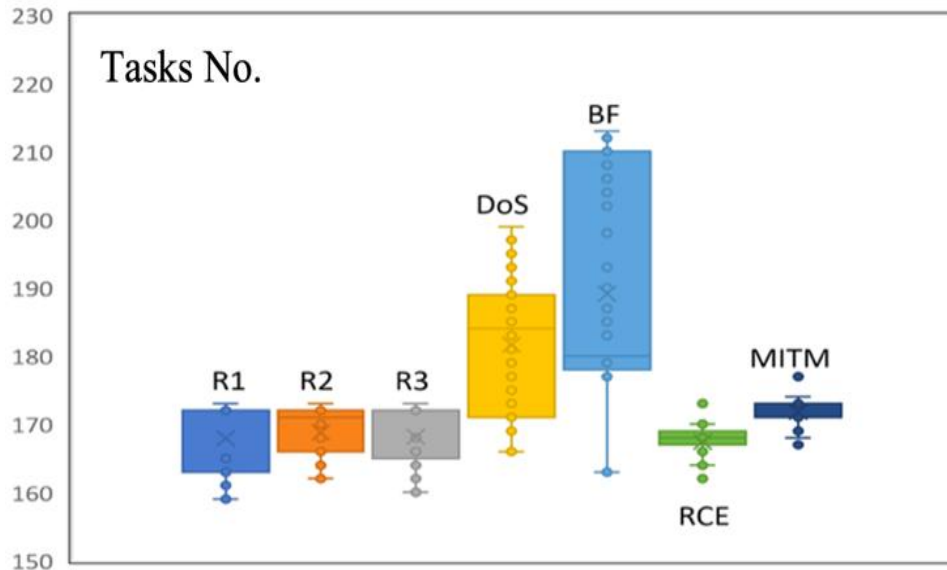


Figure 6-3. Overall tasks range for attacked cases vs standard cases.

In the RCE attack case, it has been noticed that the number of executed tasks did not significantly deviate out of the normal range, but the pattern was odd compared to the normal pattern in R1, R2, and R3. The most frequently occurring value was 169 tasks, the average was 167.4 tasks, and these two values differ from the normal pattern (Section 4.6, Table 6-4). Thus, the pattern has become anomalous in comparison to the normal pattern. Furthermore, taking into account the impacts of other parameters will clarify the distinguishability in this situation. The same applies to the MITM attack, where the highest value was slightly outside the normal range but the anomaly in terms of mean, minimum and maximum values supported the possibility of detecting the cyberattack.

In general, the results of the analysis criteria proved the accuracy of the defined standard model in terms of tasks number under normal operating conditions. Also, the obtained results under the circumstances of various cyberattack scenarios proved the ability to detect the attacks due to their abnormalities and deviations from the typical performance. Regarding the number of threads, the general trait is similar to the tasks number parameter because it is linked to it. As shown in Figure 6-4, the normal range is demonstrated within the blue area, starting from 219 threads to 234 threads as the maximum value (see Table 6-

4). Also, the normal pattern concentrated identically in 232 threads for R1, R2, and R3, shaping the Std_p in terms of $\mathcal{G}$.

Table 6-4: Overall Threads Number for all Cases

P	Pattern				Range		
	Mean	Median	Mode	Std.D	Range	Min	Max
R1	228.01	232	232	4.48	14	219	233
R2	228.93	231	232	3.61	12	222	234
R3	228.28	232	232	4.18	14	220	234
DoS	241.76	244	249	9.39	33	226	259
BF	249.23	240	240	17.52	50	223	273
RCE	220.56	221	221	2.49	11	215	226
MITM	239.89	241	241	1.78	10	235	245

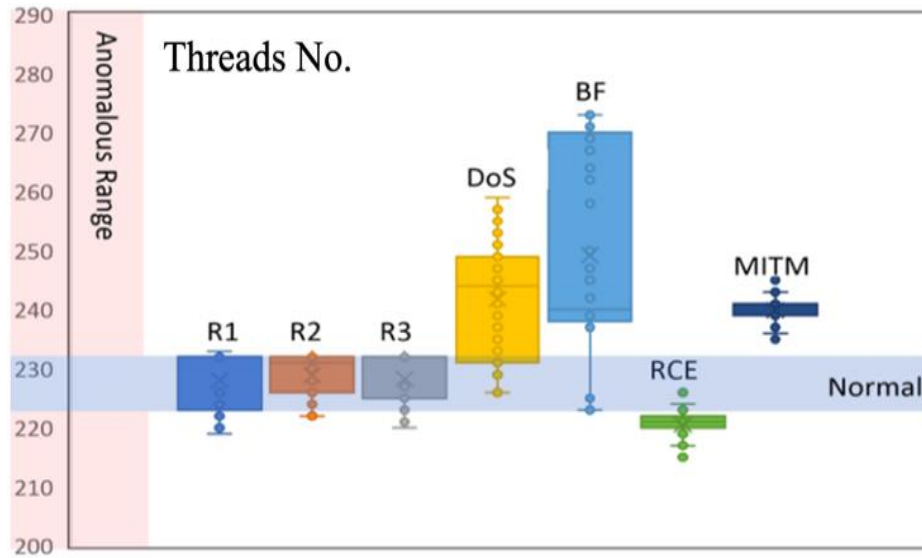


Figure 6-4. Overall threads range for attacked cases vs standard cases.

Thus, these results have proved the ability to determine the normal range, which has been used to generate the Std model and pattern for the threads number. In contrast, the attacked cases deviated from the normal range, and with its most common value (mode) at 249, 240, 221, and 241 for DoS, BF, RCE, and MITM, respectively. The anomalous behaviours have been monitored in comparison to the normal pattern, with the anomalous values appearing along the red zone, having more than 234 threads or less than 219 threads as shown in Figure 6-4. The following table summarizes the final results of the analysis criteria under all various conditions.

6.3.4. CPU Temperature

The reliance on CPU temperature to predict the existence of a cyberattack was effective in some cases and not sufficient in other cases. However, by looking at the maximal values shown in Table 6-5, the impact of cyberattacks that took the CPU temperatures to unprecedented levels compared to typical patterns can be observed.

Table 6-5: Overall CPU Temp Number for all Cases

P	Pattern				Range (XgV)		
	Mean	Median	Mode	Std.D	Range	Min	Max
R1	53.45	54.00	54.00	1.24	5.00	50.00	55.00
R2	46.60	47.00	50.00	3.32	14.00	38.00	52.00
R3	49.34	50.00	51.00	2.45	10.00	43.00	53.00
DoS	61.57	62.00	64.00	2.72	10.00	55.00	65.00
BF	58.11	59.00	60.00	3.29	13.00	50.00	63.00
RCE	54.63	54.00	54.00	1.95	8.00	52.00	60.00
MITM	56.15	56.00	55.00	1.34	6.00	54.00	60.00

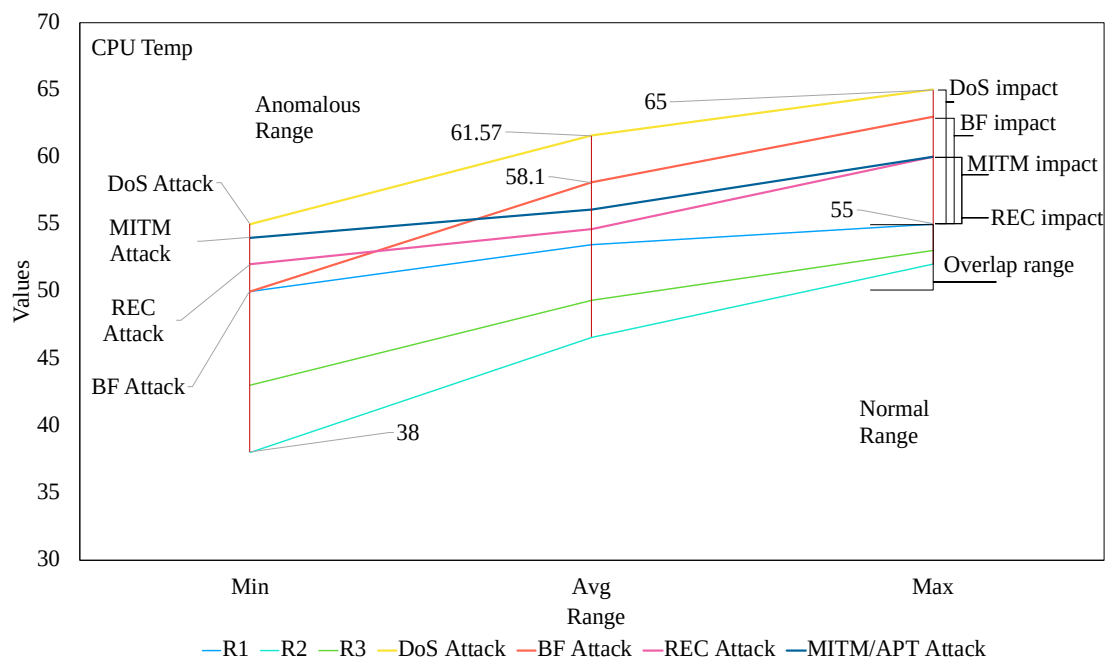


Figure 6-5. Overall temp ranges for attacked cases vs standard cases.

In general, attacks that consume more resources caused an increase in temperatures, while attacks that disrupted the system's functions interfered with the typical CPU temperature patterns. Therefore, the effectiveness of this parameter remains effective when combined with the effects of other parameters. Figure 6-5 depicts the temperature difference in the

attacked cases from those in the conventional cases. Also, the overlap of the lower limits of the attacked cases' CPU temperatures with the conventional cases' upper limits is presented in this figure [2].

6.3.5. The voltage and Current parameter

The values of voltage and current have been monitored during the testbed and while the system performs its functions. In terms of range and pattern, R1, R2, and R3 are very similar and several values are often identical in terms of range or pattern as shown in Tables 6-6 and 6-7. For example, the standard deviation values in terms of voltage were convergent in Rs cases. Therefore, defining the normal range and power consumption pattern is possible due to the identity and significant similarity of the consumption.

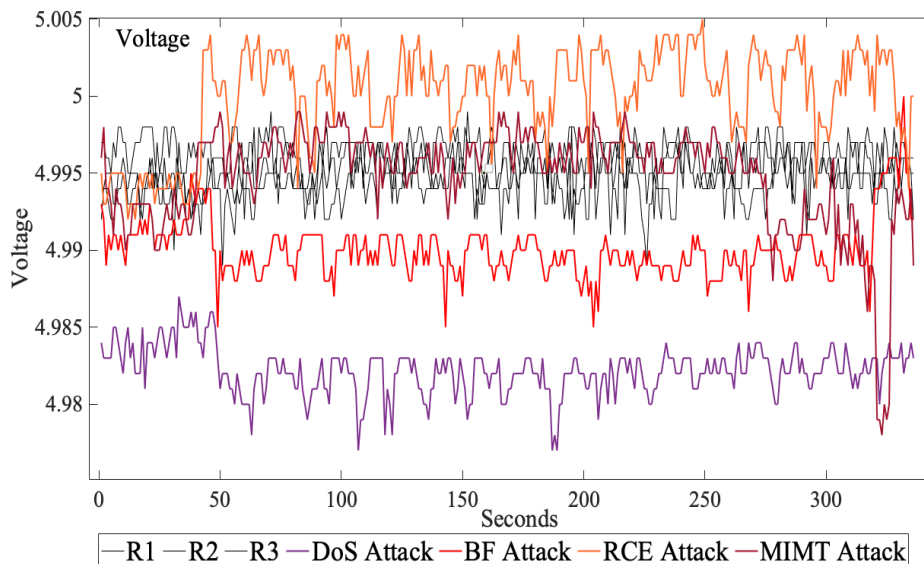


Figure 6-6. Overall voltage patterns for attacked cases vs standard cases.

For the attacked cases, in terms of the voltage parameter, the DoS attacks, BF, and RCE clearly deviate out of the normal range (X_{gV}), as shown in Figure 6-6. In the MITM attack case, the power consumption in terms of voltage differs slightly from the normal range but is clearer in terms of pattern. Thus, relying on this parameter separately to detect an attack is not enough. However, in this situation the impacts of other parameters will support the determination of a cyberattack's existence. The following table summarizes the results of power consumption in terms of voltage for all cases.

Table 6-6: Overall Voltage Consumption for all Cases

P	Pattern				Range		
	Mean	Median	Mode	Std.D	Range	Min	Max
R1	4.995	4.995	4.99	0.00146	0.01	4.99	5
R2	4.996	4.996	5	0.00142	0.01	4.99	5
R3	4.995	4.995	5	0.00149	0.01	4.99	5
DoS	4.982	4.982	4.98	0.00153	0.01	4.98	4.99
BF	4.99	4.99	4.99	0.00188	0.01	4.99	5
RCE	5	5.001	5	0.0031	0.01	4.99	5.01
MITM	4.995	4.996	5	0.00329	0.02	4.98	5

In terms of the current-voltage sub-parameter, the general trait is the overlap and similarities in the range or pattern except in the RCE attack case. In the RCE scenario, the rate of power consumption significantly differed from the normal range and shaped an anomalous pattern due to the failure of its function because of the RCE attack. Figure 6-7 demonstrates the P rate in terms of I_r and I_p in all cases as summarized in the following table [2].

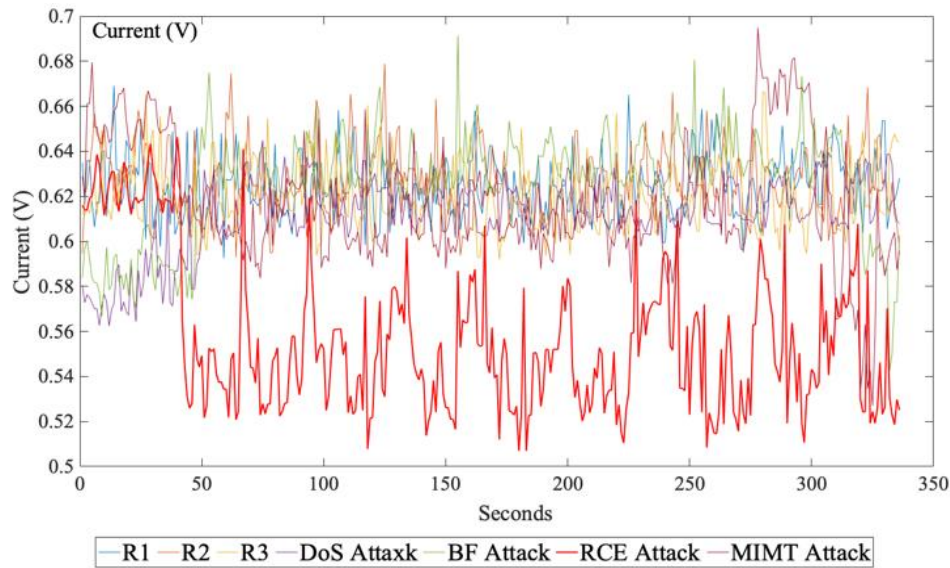


Figure 6-7. Overall current patterns for attacked cases vs standard cases.

Table 6-7: Overall Current Consumption for all Cases

P	Pattern				Range		
	Mean	Median	Mode	Std.D	Range	Min	Max
R1	0.624	0.623	0.61	0.01364	0.08	0.59	0.67
R2	0.625	0.625	0.62	0.01569	0.09	0.59	0.68
R3	0.62	0.618	0.61	0.01491	0.07	0.59	0.67
DoS	0.612	0.613	0.61	0.01638	0.08	0.56	0.64
BF	0.626	0.631	0.63	0.02249	0.15	0.54	0.69
RCE	0.557	0.551	0.55	0.03347	0.14	0.51	0.65
MITM	0.617	0.611	0.61	0.02729	0.17	0.53	0.69

6.3.6. Received and Transmitted packets parameters

The average of transmitted and received packets has been monitored during the RCE and MITM attacks as one of the testbed parameters. Based on the results in Table 6-8 and Figure 6-8, it is possible to define the normal range and patterns of the typical rate of received packets as we did in Section 4.6 because of the huge convergence in terms of packets count and due to its similarity in the performance pattern, which was sufficient to generate the *Std*. The range and pattern of R2 and R3 are almost identical in many aspects and very close to R1's range and pattern. Based on the that, the RX_r ranges from 0 to 27 packets, with 0 the most frequent value and 4.36 to 4.997 the average of received packets.

Table 6-8: Overall Received Packets for all Cases

Cases	Pattern				Range		
	Mean	Median	Mode	Std.D	Range	Mini	Max
R1	4.04	1.00	0.00	5.28	24.00	0.00	24.00
R2	4.29	1.00	0.00	5.72	27.00	0.00	27.00
R3	5.00	2.00	0.00	6.02	27.00	0.00	27.00
RCE	3.99	1.00	0.00	5.26	27.00	0.00	27.00
MITM	7.79	3.00	0.00	10.37	55.00	0.00	55.00

In the attacked cases, for the RCE attack case there is no significant difference in terms of received packets. However, in the MITM attack case, the rate of received packets per second has differed from the normal range. Thus, this sort of parameter might help in detecting specific kinds of attacks such as a network-based attack, where the attacks continuously receive data from the victim's device. The following figure shows the impact of RCE attacks and MITM on the volume of received packets/s.

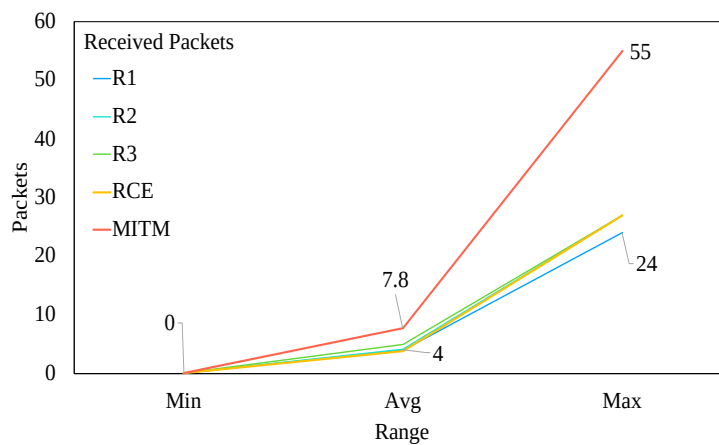


Figure 6-8. Overall RX patterns for MITM attack vs standard cases.

In terms of transmitted packets, the R1, R2, and R3 showed a sufficient convergence to determine the normal range and pattern. The normal range of the transmitted packets rate extended from 0 to 29 packets per second and the most common value was 0. Also, the average was between 4 to 5 packets per second. In the attacked cases, the general trait was similar to the received packets rate parameter. As shown in Figures 6-9 and 6-10, the RCE attack (yellow line) does not differ significantly from the normal range as the MITM attack shown in Figure 6-9, where even the pattern was somehow similar to R1, R2, and R3, [2]. Thus, the impacts of other parameters must be added in order to facilitate the separation ability in this case. In contrast, the TX parameter in the MITM case deviated significantly from the normal range, causing an anomalous pattern as shown in Figure 6-10. Therefore, having this parameter within the septenary tuple model will help detect specific kinds of attacks. The following table summarizes the final analytics results of the transmitted packets/s.

Table 6-9: Overall Transmitted Packets for all Cases

Cases	Pattern				Range		
	Mean	Median	Mode	Std.D	Range	Min	Max
R1	4.03	1.00	0.00	5.27	24.00	0.00	24.00
R2	4.29	1.00	0.00	5.72	29.00	0.00	29.00
R3	5.05	2.00	0.00	6.03	27.00	0.00	27.00
RCE	4.06	1.00	0.00	5.29	26.00	0.00	26.00
MITM	284.29	307.00	1.00	148.68	645.00	1.00	646.00

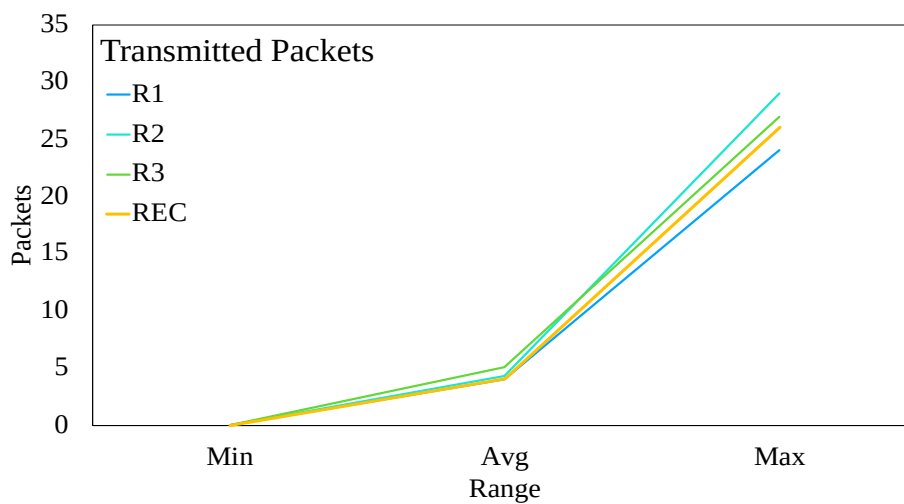


Figure 6-9. Overall TX patterns for RCE attack vs standard cases

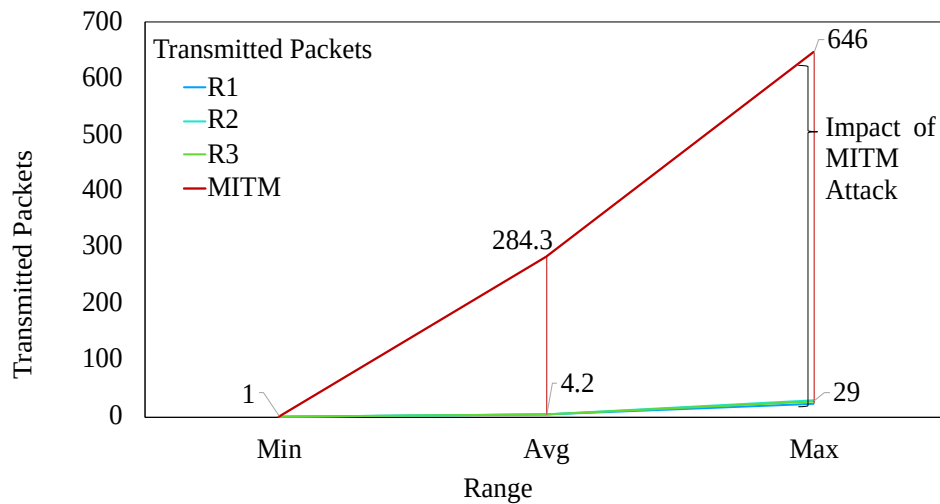


Figure 6-10. Overall TX patterns for MITM attack vs standard cases

Overall, the ability to define a standard model for the ES designed to perform specific functions paves the way for the software engineer to apply the necessary restrictions to maintain an optimal resource consumption level for the prevention of any heterogeneous consumption due to illegal activities, especially the anomalous patterns of the Smart PiCar performance under cyberattacks circumstances have clearly appeared and been observed.

6.4. How the ARCD approach can be implemented in line with an ES's resources and capabilities and what are its benefits and flexibility extent?

The ARCD approach detects cyber-attacks because of its ability to define a comparable reference performance pattern for the ES; this is due to its functions' determinability. After that, the anomalous pattern – if it exists and is observable during the attack – will be used as an indicator to detect the attack, activate an autonomous response and warn the system administrator.

Configuring the OS layer, controlling the hardware and applying restrictions to resource consumption are all solutions that are under the control of software engineers, and they can adapt these components to fit their needs. While cyber-attacks cannot be stopped entirely, they can be dealt with it and neutralised by adopting a security approach that detects such attacks. Since the ARCD approach creates an additional integrated layer of

protection in line with existing countermeasures, the autonomous response mechanism can be designed to (1) activate the built-in defences of the system's architecture, (2) apply restrictions on resource usage, (3) disable the attacked entry points, (4) auto-disable the compromised network port, and (5) end and re-establish the connection session. Another option is to (6) isolate the hacked system from the network by activating (auto-reboot) to interrupt the attack [3].

The architectural framework of the ARCD is a generalised approach that can be applied to any ES that normally operates within a constrained pattern of behaviour. If the IoT applications mainly range between monitoring, controlling, sensing, opening or closing, alerting, environment monitoring, safety, process monitoring, logistic management, signals transmitting, computing and switching, it is possible to define their functions. Thus, the ARCD approach, with its detection mechanism, is compatible with any processing unit embedded into a larger CPS to steer its specified functions. All that is needed is to determine the functions precisely and find the normal performance pattern default. This is defined as a reference pattern by following the proposed steps within the presented architectural framework. Any anomalous pattern will then be recognised as an indication of a cyber-attack or a system fault. Therefore, for the adoption of ARCD by software engineers, an additional layer of protection can be added to the embedded system's OS [3].

6.5. The mechanism of the detection method has been explained, but how effective is the proposed approach in terms of detection latency?

The early stages of this work mainly concentrated on the feasibility of detecting anomaly patterns using the proposed approach, which is illustrated in the results presented, but detection latency is also a critical factor in demonstrating its effectiveness. In the approach suggested by this research, the detection latency is closely related to the determination of the anomaly threshold, and the anomaly threshold depends on the formation of the abnormal pattern in performance. Therefore, according to the proposed approach, which is based on monitoring the values of specific parameters that represent the system performance and resource consumption in real time, the time taken to detect

the attack is the total time of monitoring, analysing and anomalous pattern formation. Thus, another vital factor related to the detection latency, and which plays an important role, is the time taken for the abnormal pattern to form and for its effect on system performance and resource consumption to appear. In other words, there is no problem in detecting the attack; as soon as there is an anomalous pattern, the attack will be detected, but how long does it take for the abnormal pattern to form? The following screenshots (Fig 6-11) depict the detection latency and the sequence of events for two different types of attack [3].

Moreover, if there is a delay in the formation of the abnormal pattern, it will reflect negatively on the accuracy of the prediction percentage (Section 5.6) because the dataset collected under attack scenarios would have been classified as being of a normal pattern, thereby reducing the prediction accuracy percentage. This did not happen in the test or training sessions. However, other factors, such as the type of attack, the architecture of the operating system and the computing capabilities of the ES need to be considered [3].



Figure 6-11: Snapshots of real time observation

6.6. References

1. Alooseel A., He H., Shaw C., Khan MA. Analytical Review of Cybersecurity for Embedded Systems. IEEE Access. 2021; 9: 961–982. Available at: DOI:10.1109/ACCESS.2020.3045972
2. Alooseel A., Al-Rubaye S., Zolotas A., He H., Shaw C. A Novel Approach for Detecting Cyberattacks in Embedded Systems Based on Anomalous Patterns of Resource Utilization-Part I. IEEE Access. 2021; 9: 103204–103229. Available at: DOI:10.1109/ACCESS.2021.3088395
3. Alooseel A., Al-Rubaye S., Zolotas A., Shaw C. Attack-Detection Architectural Framework Based on Anomalous Patterns of System Performance and Resource Utilization—Part II. IEEE Access. 2021; 9: 87611–87629. Available at: DOI:10.1109/ACCESS.2021.3088411

CHAPTER 7: CONCLUSIONS AND FUTURE WORK

CHAPTER 7: CONCLUSIONS AND FUTURE WORK

7.1. Conclusions

Finally, considering all aspects of this research, from the literature review of cybersecurity for embedded systems and the novel approach presented for detecting cyber-attacks in embedded systems to the attack-detection architectural framework, the following points are made:

- The multiple layers feedback framework of embedded system cybersecurity (MuLFESC) could contribute to the implementation of comprehensive and effective ‘security by design’ solutions by providing feedback to the design stage of cybersecurity for embedded systems (CSES).
- The anomalous resource consumption detection (ARCD) approach consists of a septenary tuple model as the detection mechanism, presenting a security solution that can work along with existing countermeasures to augment the security of the operating system layer.
- The architectural framework of the ARCD approach facilitates the adoption of this approach by software engineers.

The specific conclusions in relation to the research hypothesis and objectives can be described as follows:

- **Research Hypothesis:** based on the literature review, it was hypothesised that ‘*in ESs, which are designed to perform specific functions, performance and resource consumption are within a determinable pattern. Thus, an anomalous pattern, if it exists and is identifiable, can be exploited in comparison to a pre-identifiable reference pattern as an indicator to detect cyber-attacks*’.
- **Hypothesis Testing Result:** after testing the validity of the research hypothesis, the results of the realistic experiment proved the validity of what was assumed in the hypothesis in its first and second parts. Based on the final results of the septenary tuple model of the parameters’ values $\{U, M, N, \mathcal{G}, T, P, R\}$, and according to the statistical criteria results, it can be said that the range and pattern

of the ES's performance and its resource consumption under normal operating conditions (Rs cases) fall within a definable range and determinable pattern. Thus, it is possible to define a reference pattern for the ES that has been designed to perform specific functions.

In the second part of the hypothesis, the system showed abnormal performance patterns in all cases while it was exposed to different cyber-attacks. Therefore, these anomalous patterns enabled detection of the attacks.

The specific conclusions in relation to the research objectives can be described as follows:

Objective 1. To conduct a literature review in the field of CSES.

- **Related conclusion:** the common characteristics of embedded systems, such as small size, mobility, low cost, limited power consumption, specific functionality, remote accessibility and independence, when compared with conventional computer systems, have posed many challenges in CSES. Therefore, the embedded systems are exposed to countless security threats, like traditional computer systems, but with considerable limitations to manage complex advanced security solutions for efficient and effective defence. However, because the ESs are dedicated to performing specific functions, this unique feature enabled the development of the ARCD approach to improve the cybersecurity aspects of ESs.

Objective 2. To develop a security risks assessment framework supported by security risks metrics by identifying the influencing factors in cybersecurity of ESs based on the research directions.

- **Related conclusion:** the determination of the influencing factors enabled the shaping of the MuLFESC, supported by the security risk metrics model. The MuLFESC framework can be used by cybersecurity practitioners to assess their systems with regard to 12 identified cybersecurity aspects and could help to find more efficient solutions for CSES.

Objective 3. To set up a controlled testing environment by determining the requirement of the experiment and targeted parameters for performance measurement under different operating conditions – normal and attacked cases.

- **Related conclusion:** a Smart PiCar, which provides a realistic hardware-software environment to test the performance of the embedded system under different operational conditions, was assembled and programmed. An integrated ARM Cortex-A72 was embedded into a Smart PiCar, where a python code was developed to monitor the performance of the whole system.

Objective 4. To develop a statistical classification method, the detection mechanism, to evaluate a standard pattern's determinability and anomalous patterns' observability.

- **Related conclusion:** the final statistical results of the septenary tuple model proved the ability to define a standard pattern for the performance and resource consumption of the ES. The statistical analysis for the standard pattern's determinability test and anomalous patterns' observability test provided compelling numerical results. The distinctive feature of the ES, which is dedicated to performing specific functions, offered a baseline from which the pattern of ES normal states could be identified and used as a reference profile to distinguish anomalous patterns, thereby detecting the presence of the attack.

On the other hand, the anomalous patterns of the Smart PiCar resource consumption during exposure to different cyber-attacks have clearly appeared and have been observed. These anomalous patterns can be detected due to deviation from the predefined reference pattern.

Objective 5. To validate the proposed approach's efficiency computationally based on the prediction accuracy percentage results by applying the machine learning method for anomaly detection.

- **Related conclusion:** based on the confusion matrix results of the SVM algorithm, the final results showed very high prediction accuracies in terms of distinguishing anomalous RCP patterns from the typical patterns, where the prediction percentages of the true positive ratio (TPR) ranged between 100% and 98.8%, while the false negative ratio (FNR) percentages ranged between 0.1% and 1.2%. Therefore, detecting cyber-attacks based on the proposed approach (ARCD) is an effective method.

Objective 6. To develop an architectural framework which reflects the concept of the validated approach to facilitate its adoption.

- **Related conclusion:** the ARCD architectural framework was developed to facilitate the adoption of this approach, and it consists of seven steps that reflect the concept of the validated approach. Thus, the architectural framework paves the way for software engineers to strengthen the software layer of ESs by creating an additional layer of protection.

7.2. Future Work

For future research and application of this work, it would be beneficial to evaluate other cyber-attacks, such as a blackhole attack or an SQL injection, and expand the research to include other testbeds such as temperature monitoring systems or intelligent motion detection systems. Implementing the concepts of this approach within an open-source OS, and generating a practical software framework, would further test its feasibility and applicability as an off-the-shelf solution. Additionally, applying the concept of this approach to low-end devices, such as microcontrollers, with hardware machine learning support would be another possible extension.

Although all executed attack scenarios caused anomalous performance patterns, this approach is active in terms of detecting the existence of the attack but is not proactive in preventing the attack. Thus, it is better not to rely on the anomaly detection technique independently but to initially preserve the predefined standard performance by applying the necessary restrictions on resource consumption. Usually, cyber-attacks need an entry point, from where they pass on their harmful instructions, and this will be reflected negatively in the performance of the system. Therefore, cyber-attacks will be efficiently detected if a reference pattern has been defined. Accordingly, it is expected that other untested types of attacks will cause irregular performance patterns. It will be possible to detect them based on this approach, especially since the septenary tuple model, which represents the core of the detection mechanism, includes seven parameters that consider the architecture of the ES. Thus, this detection mechanism can comprehensively monitor the most important changes in the resources of the system. However, it would be beneficial to examine more attack types to discover an attack that does not have a noticeable impact on the performance of the system, as this would not be detected according to this technique.

7.3.References

1. Aloheel A., He H., Shaw C., Khan MA. Analytical Review of Cybersecurity for Embedded Systems. IEEE Access. 2021; 9: 961–982. Available at: DOI:10.1109/ACCESS.2020.3045972
2. Aloheel A., Al-Rubaye S., Zolotas A., He H., Shaw C. A Novel Approach for Detecting Cyberattacks in Embedded Systems Based on Anomalous Patterns of Resource Utilization-Part I. IEEE Access. 2021; 9: 103204–103229. Available at: DOI:10.1109/ACCESS.2021.3088395
3. Aloheel A., Al-Rubaye S., Zolotas A., Shaw C. Attack-Detection Architectural Framework Based on Anomalous Patterns of System Performance and Resource Utilization—Part II. IEEE Access. 2021; 9: 87611–87629. Available at: DOI:10.1109/ACCESS.2021.3088411

APPENDICES:

A: PYTHON FUNCTIONS

B: STATISTICS RESULTS

C: ROW DATA

Appendices: A, B, and C

A. Appendix A: Python Functions

```
# Cranfield University 2019 - 2022.
# Cybersecurity of Embedded Systems CSES2020 research.
# FOR REVIEW PURPOSE BY IEEE ACCESS NOT FOR PUBLICATION.
# Used Functions and Commands to extract the parameters' values
# Extracting Time_Stamp, CPU_Temp, CPU_Usage, Memory_Usage, Tasks, Threads,
# Recived Byets && Pakets, Transmitted Byets&&Pakets to logfile.csv # Dec.2019
# Extracting & Saving experiment parameters values to a log.csv file
```

```
#imported libraries
```

```
import psutil
import time
import sys
import datetime
import os
import subprocess
```

#-----Used Functions and Commands to extract the parameters' values-----

```
# TimeStamp function
```

```
def TimeStamp():
    return str(datetime.datetime.now().strftime("%Y-%m-%d %H:%M:%S"))
```

```
# OR def TimeMil():
```

```
    return str(datetime.datetime.now())
```

```
# CPU_Temp
```

```
def CpuTemp():
    temp = int(open('/sys/class/thermal/thermal_zone0/temp').read()) / 1000
    return str (temp)
```

```
# CPU_Usage
```

```
def cpu():
```

```
    cpu = psutil.cpu_percent(interval=0.0)
#    interval=0.0 can be added within brackets to start from 0
    return str(cpu)
# Mem_Usage
def memory():
    memory = psutil.virtual_memory()
    return str(memory.percent)

# Alive Tasks Count
getT = subprocess.Popen('sudo ps aux | wc -l', shell=True, stdout=subprocess.PIPE).stdout
vT = getT.read()

# Threads Count
getH = subprocess.Popen('sudo ps -eLf | wc -l', shell=True, stdout=subprocess.PIPE).stdout
#OR
getH = subprocess.Popen('sudo ps -eo nlwp | tail -n +2 | awk '{ num_threads += $1} END
    { print num_threads} ' ', shell=True, stdout=subprocess.PIPE).stdout
vH = getH.read()

# Received Rate of bytes and packets
rxByN = int(open('/sys/class/net/wlan0/statistics/rx_bytes').read())
rxPktN = int(open('/sys/class/net/wlan0/statistics/rx_packets').read())

# Transmitted Rate of bytes and packets
txByN = int(open('/sys/class/net/wlan0/statistics/tx_bytes').read())
txPktN = int(open('/sys/class/net/wlan0/statistics/tx_packets').read())
```

B. Appendix B: Statistical Results

Statistical Results as generated by IBM® SPSS® Statistics

R1- Statistical Results													
	Temp	CPU_Load	Mem_Load	ProNo,	ThreadsNo	RX_bit	RX_pkt	TX_bit	TX_pkt	Voltage(V)	Current(A)	D+(V)	D-(V)
Mean	53.4494	12.3875	9.5238	167.8958	228.0119	213.7202	4.0357	575.3274	4.0268	4.9945	0.6241	0.8513	0.6835
Median	54	11.8	9.5	172	232	52	1	150	1	4.995	0.6231	0.82	0.63
Mode	54	7.9	9.5	172	232	0	0	0	0	4.99	.61a	0.82	0.62
Std. Deviation	1.24246	4.40177	0.2094	4.51576	4.47946	276.43762	5.28178	744.66509	5.2708	0.00146	0.01364	0.04736	0.08447
Range	5	20.2	1.4	14	14	1248	24	3248	24	0.01	0.08	0.16	0.22
Minimum	50	6.2	9.3	159	219	0	0	0	0	4.99	0.59	0.77	0.59
Maximum	55	26.4	10.7	173	233	1248	24	3248	24	5	0.67	0.93	0.81

R2- Statistical Results													
	Temp	CPU_Load	Mem_Load	ProNo,	ThreadsNo	RX_bit	RX_pkt	TX_bit	TX_pkt	Voltage(V)	Current(A)	D+(V)	D-(V)
Mean	46.5982	12.6762	9.508	168.8065	228.9315	224.1071	4.2887	605.7202	4.2917	4.996	0.6254	0.8796	0.7042
Median	47	12.4	9.5	171	231	52	1	150	1	4.996	0.6246	0.87	0.66
Mode	50	7.7	9.5	172	232	0	0	0	0	5	.62a	0.86	0.66
Std. Deviation	3.32191	4.35081	0.22822	3.6111	3.61152	298.69661	5.72322	795.95707	5.71706	0.00142	0.01569	0.03746	0.07498
Range	14	20.5	1.5	11	12	1404	27	3894	29	0.01	0.09	0.17	0.24
Minimum	38	4.6	9.3	162	222	0	0	0	0	4.99	0.59	0.78	0.59
Maximum	52	25.1	10.8	173	234	1404	27	3894	29	5	0.68	0.95	0.83

R3- Statistical Results													
	Temp	CPU_Load	Mem_Load	ProNo,	ThreadsNo	RX_bit	RX_pkt	TX_bit	TX_pkt	Voltage(V)	Current(A)	D+(V)	D-(V)
Mean	49.3363	12.7369	9.5226	168.1458	228.2768	261.3214	4.997	718.0952	5.0536	4.9952	0.6204	0.8519	0.6819
Median	50	12.5	9.5	172	232	104	2	292	2	4.995	0.6179	0.83	0.62
Mode	51	7.50a	9.5	172	232	0	0	0	0	5	0.61	0.82	0.62
Std. Deviation	2.45375	4.53167	0.20125	4.16806	4.18072	314.5593	6.02358	847.54434	6.0335	0.00149	0.01491	0.04673	0.08423
Range	10	22.8	1.4	13	14	1404	27	3626	27	0.01	0.07	0.15	0.21
Minimum	43	5.7	9.3	160	220	0	0	0	0	4.99	0.59	0.77	0.59
Maximum	53	28.5	10.7	173	234	1404	27	3626	27	5	0.67	0.92	0.8

DoS attack- Statistical Results									
	Temp	CPU_Load	Mem_Load	ProNo,	ThreadsNo	Voltage(V)	Current(A)	D+(V)	D-(V)
Mean	61.5714	31.8988	10.1381	181.6369	241.7589	4.9822	0.6119	0.854	0.6996
Median	62	31.4	10.2	184	244	4.982	0.6128	0.82	0.635
Mode	64	30.9	10.2	171	249	4.98	.61a	0.81	0.61
Std. Deviation	2.7199	6.25629	0.26762	9.38524	9.39283	0.00153	0.01638	0.05116	0.09018
Range	10	47.3	1.8	33	33	0.01	0.08	0.16	0.23
Minimum	55	6.8	9.7	166	226	4.98	0.56	0.77	0.58
Maximum	65	54.1	11.5	199	259	4.99	0.64	0.93	0.81

Brute Force Attack- Statistics Results									
	Temp	CPU_Load	Mem_Load	ProNo,	ThreadsNo	Voltage(V)	Current(A)	D+(V)	D-(V)
Mean	58.1071	31.1613	9.7842	189.1012	249.2262	4.99	0.6264	0.8413	0.6792
Median	59	31.5	9.6	180	240	4.99	0.6306	0.82	0.63
Mode	60.00a	30.5	9.6	180	240	4.99	.63a	0.91	0.8
Std. Deviation	3.29094	9.12873	0.32748	17.46797	17.52089	0.00188	0.02249	0.05257	0.08747
Range	13	54.7	1.9	50	50	0.01	0.15	0.17	0.24
Minimum	50	6.5	9.4	163	223	4.99	0.54	0.75	0.57
Maximum	63	61.2	11.3	213	273	5	0.69	0.92	0.81

Remote Code Execution Attack- Statistical Results											
	Temp	CPU_Load	Mem_Load	ProNo,	ThreadsNo	RX_bit	RX_pkt	TX_bit	TX_pkt	Voltage(V)	Current(A)
Mean	54.631	12.3324	9.9	167.4524	220.5565	209.1964	3.9881	574.9226	4.0565	5.0001	0.557
Median	54	10.4	9.9	168	221	52	1	150	1	5.001	0.5505
Mode	54	6.20a	9.9	169	221	0	0	0	0	5	0.55
Std. Deviation	1.95031	7.50913	0	2.43925	2.48634	276.21832	5.26264	744.24488	5.28527	0.0031	0.03347
Range	8	32.2	0	11	11	1416	27	3508	26	0.01	0.14
Minimum	52	4.9	9.9	162	215	0	0	0	0	4.99	0.51
Maximum	60	37.1	9.9	173	226	1416	27	3508	26	5.01	0.65

Man in the Middle Attack- Statistical Results											
	Temp	CPU_Load	Mem_Load	ProNo,	ThreadsNo	RX_bit	RX_pkt	TX_bit	TX_pkt	Voltage(V)	Current(A)
Mean	56.1488	15.8685	10.5003	171.7887	239.8929	415.0625	7.7887	388523.7738	284.2887	4.9948	0.6174
Median	56	12.6	10.5	173	241	156	3	419263.5	307	4.996	0.6113
Mode	55	7.40a	10.5	173	241	0	0	142.00a	1.00a	5	0.61
Std. Deviation	1.34337	9.05374	0.00546	1.70337	1.78396	543.79037	10.37074	216204.4785	148.68238	0.00329	0.02729
Range	6	33.6	0.1	10	10	2864	55	908814	645	0.02	0.17
Minimum	54	5.3	10.5	167	235	0	0	142	1	4.98	0.53
Maximum	60	38.9	10.6	177	245	2864	55	908956	646	5	0.69

a: Multiple modes exist. The smallest value is shown

C. Appendix C: Row Data

Row Data

Run-1-Log															
	Date	T.Stamp	Temp	CPU_Load	Mem_Load	ProNo,	ThreadsNo	RX_bit	RX_pkt	TX_bit	TX_pkt	Voltage(V)	Current(A)	D+(V)	D-(V)
1	2020-03-13	12:23:37	50	12.7	9.3	173	233	728	14	1972	14	4.992	0.6349	0.82	0.62
2	2020-03-13	12:23:38	51	11.6	9.3	173	233	728	14	1988	14	4.994	0.6163	0.82	0.62
3	2020-03-13	12:23:39	50	8.4	9.4	173	233	728	14	1988	14	4.995	0.6359	0.82	0.62
4	2020-03-13	12:23:40	50	7.7	9.3	172	232	780	15	2228	16	4.995	0.6359	0.92	0.8
5	2020-03-13	12:23:41	50	7.2	9.4	172	232	804	15	2256	16	4.995	0.6168	0.81	0.61
6	2020-03-13	12:23:42	50	14.2	9.4	172	232	676	13	1696	12	4.993	0.6064	0.77	0.59
7	2020-03-13	12:23:43	51	8.5	9.4	172	232	0	0	150	1	4.993	0.6174	0.82	0.63
8	2020-03-13	12:23:44	50	8.6	9.4	172	232	52	1	150	1	4.995	0.6171	0.82	0.63
9	2020-03-13	12:23:45	51	8.3	9.4	172	232	132	3	350	3	4.995	0.6402	0.82	0.63
10	2020-03-13	12:23:46	50	7.3	9.4	172	232	676	13	1846	13	4.996	0.6402	0.91	0.79
11	2020-03-13	12:23:47	51	11.0	9.4	172	232	740	14	1846	13	4.995	0.6111	0.81	0.62
12	2020-03-13	12:23:48	51	19.1	9.4	172	233	728	14	1988	14	4.993	0.6314	0.82	0.63
13	2020-03-13	12:23:49	51	14.0	9.4	172	232	728	15	2114	15	4.993	0.6453	0.82	0.63
14	2020-03-13	12:23:50	50	8.5	9.4	172	232	364	7	1002	7	4.994	0.6691	0.82	0.63
15	2020-03-13	12:23:51	51	8.1	9.4	172	232	52	1	150	1	4.994	0.6318	0.78	0.6
16	2020-03-13	12:23:52	52	12.9	9.4	172	232	0	0	0	0	4.995	0.6318	0.9	0.78
17	2020-03-13	12:23:53	50	17.8	9.4	172	232	52	1	150	1	4.992	0.6163	0.82	0.63
18	2020-03-13	12:23:54	51	18.3	9.4	172	232	156	3	434	3	4.994	0.6208	0.81	0.62
19	2020-03-13	12:23:55	51	17.7	9.4	172	232	0	0	0	0	4.994	0.6449	0.82	0.63
20	2020-03-13	12:23:56	51	7.9	9.4	172	232	0	0	0	0	4.994	0.6416	0.77	0.59
21	2020-03-13	12:23:57	51	7.5	9.4	172	232	208	4	576	4	4.996	0.6145	0.82	0.62

22	2020-03-13	12:23:58	52	18.2	9.8	172	232	0	0	0	0	4.994	0.6145	0.86	0.68
23	2020-03-13	12:24:00	52	16.8	9.4	172	232	104	2	276	2	4.995	0.6329	0.8	0.61
24	2020-03-13	12:24:01	52	23.4	9.4	172	232	208	4	568	4	4.995	0.6292	0.92	0.8
25	2020-03-13	12:24:02	53	20.9	9.4	172	232	676	13	1846	13	4.993	0.6508	0.82	0.61
26	2020-03-13	12:24:03	53	16.4	10.2	172	232	780	15	2130	15	4.993	0.6312	0.82	0.61
27	2020-03-13	12:24:06	52	9.1	9.4	172	232	728	14	1988	14	4.996	0.6009	0.82	0.63
28	2020-03-13	12:24:07	51	7.7	9.4	172	232	1248	24	3248	24	4.994	0.6355	0.81	0.62
29	2020-03-13	12:24:08	51	13.7	9.4	172	232	1196	23	3082	23	4.994	0.6343	0.82	0.63
30	2020-03-13	12:24:09	52	6.4	9.4	172	232	52	1	150	1	4.995	0.6055	0.81	0.62
31	2020-03-13	12:24:10	52	15.1	9.4	172	232	0	0	0	0	4.995	0.6129	0.82	0.63
32	2020-03-13	12:24:11	52	11.1	9.4	172	232	0	0	394	3	4.993	0.6194	0.82	0.62
33	2020-03-13	12:24:12	52	8.8	9.4	172	232	428	8	292	2	4.997	0.5976	0.9	0.79
34	2020-03-13	12:24:13	52	9.9	9.4	172	232	0	0	0	0	4.995	0.6231	0.91	0.8
35	2020-03-13	12:24:14	53	22.1	9.4	172	232	52	1	150	1	4.995	0.6204	0.9	0.79
36	2020-03-13	12:24:15	53	12.8	9.4	172	232	0	0	0	0	4.992	0.6257	0.82	0.62
37	2020-03-13	12:24:16	52	7.3	9.4	172	232	520	10	1420	10	4.992	0.6074	0.81	0.62
38	2020-03-13	12:24:17	51	16.2	9.4	172	232	780	15	1988	14	4.994	0.6489	0.8	0.61
39	2020-03-13	12:24:18	52	8.4	9.4	172	232	156	3	434	3	4.992	0.6031	0.9	0.79
40	2020-03-13	12:24:19	53	8.0	9.4	172	232	52	1	150	1	4.993	0.6066	0.92	0.8
41	2020-03-13	12:24:20	52	12.8	9.4	172	232	522	6	0	0	4.993	0.6135	0.92	0.8
42	2020-03-13	12:24:21	51	11.1	9.4	172	232	260	5	702	5	4.991	0.607	0.82	0.63
43	2020-03-13	12:24:22	51	7.5	9.4	172	232	0	0	0	0	4.994	0.6127	0.82	0.63
44	2020-03-13	12:24:23	52	17.3	9.4	172	232	0	0	150	1	4.993	0.6489	0.82	0.63
45	2020-03-13	12:24:24	52	8.1	9.4	172	232	52	1	0	0	4.996	0.6023	0.81	0.62
46	2020-03-13	12:24:25	52	8.0	9.4	172	232	728	14	1988	14	4.995	0.6023	0.91	0.8

47	2020-03-13	12:24:26	51	11.3	9.4	172	232	52	1	150	1	4.996	0.6326	0.9	0.79
48	2020-03-13	12:24:27	53	20.4	9.4	173	233	676	13	1830	13	4.994	0.6506	0.82	0.62
49	2020-03-13	12:24:28	52	12.8	9.4	173	233	728	14	1988	14	4.994	0.6223	0.81	0.61
50	2020-03-13	12:24:29	53	14.3	9.4	173	233	780	15	2130	15	4.994	0.607	0.82	0.62
51	2020-03-13	12:24:30	53	10.1	9.4	173	232	728	14	1996	14	4.989	0.6053	0.82	0.62
52	2020-03-13	12:24:31	51	7.3	9.4	172	232	0	0	0	0	4.993	0.611	0.91	0.8
53	2020-03-13	12:24:32	53	9.3	9.4	172	232	260	5	702	5	4.994	0.6176	0.91	0.8
54	2020-03-13	12:24:33	52	12.4	9.6	172	232	0	0	0	0	4.993	0.6248	0.915	0.8
55	2020-03-13	12:24:34	51	9.6	9.4	172	232	52	1	150	1	4.992	0.632	0.92	0.8
56	2020-03-13	12:24:35	52	6.6	9.4	172	232	272	5	662	5	4.991	0.6056	0.91	0.8
57	2020-03-13	12:24:36	52	19.5	9.4	172	232	104	2	312	2	4.994	0.6202	0.83	0.62
58	2020-03-13	12:24:37	52	7.6	9.4	172	233	0	0	0	0	4.993	0.6481	0.82	0.62
59	2020-03-13	12:24:38	52	11.9	10.2	172	232	208	4	576	4	4.994	0.5925	0.82	0.62
60	2020-03-13	12:24:39	53	12.4	9.7	172	232	0	0	0	0	4.994	0.6276	0.91	0.8
61	2020-03-13	12:24:40	53	24.1	9.4	172	233	52	1	150	1	4.994	0.6272	0.92	0.8
62	2020-03-13	12:24:40	53	25.1	9.4	172	232	0	0	0	0	4.994	0.6272	0.92	0.8
63	2020-03-13	12:24:41	55	16.0	9.4	172	232	208	4	560	4	4.992	0.6306	0.92	0.8
64	2020-03-13	12:24:42	53	14.4	9.4	172	232	0	0	0	0	4.992	0.6479	0.81	0.61
65	2020-03-13	12:24:43	52	11.7	9.4	172	233	116	2	426	3	4.994	0.6229	0.82	0.62
66	2020-03-13	12:24:44	53	11.8	9.4	172	232	156	3	150	1	4.994	0.623	0.82	0.62
67	2020-03-13	12:24:45	53	8.2	9.4	172	232	0	0	0	0	4.995	0.6308	0.81	0.61
68	2020-03-13	12:24:46	53	13.8	9.4	172	232	116	2	450	3	4.996	0.6353	0.78	0.59
69	2020-03-13	12:24:47	54	14.9	9.4	172	232	180	3	576	4	4.996	0.6353	0.9	0.79
70	2020-03-13	12:24:48	54	11.9	9.4	172	232	0	0	0	0	4.995	0.6164	0.92	0.8
71	2020-03-13	12:24:49	53	11.8	9.4	172	232	0	0	0	0	4.995	0.619	0.82	0.63

72	2020-03-13	12:24:50	53	11.0	9.4	172	232	208	4	576	4	4.995	0.6174	0.81	0.62
73	2020-03-13	12:24:51	52	18.1	9.4	172	232	0	0	0	0	4.994	0.6157	0.82	0.63
74	2020-03-13	12:24:52	54	19.2	9.4	172	232	312	6	852	6	4.995	0.6188	0.9	0.79
75	2020-03-13	12:24:53	54	18.2	9.4	172	232	728	14	1988	14	4.994	0.619	0.91	0.79
76	2020-03-13	12:24:54	53	8.4	9.4	172	232	676	13	1854	13	4.994	0.6349	0.91	0.8
77	2020-03-13	12:24:55	53	8.5	9.4	172	232	104	2	284	2	4.994	0.632	0.82	0.63
78	2020-03-13	12:24:56	54	17.7	9.4	172	233	676	13	1846	13	4.995	0.6178	0.82	0.62
79	2020-03-13	12:24:57	53	9.1	9.4	172	232	728	14	1988	14	4.995	0.6106	0.82	0.63
80	2020-03-13	12:24:58	53	11.0	9.4	172	232	832	16	2130	15	4.994	0.6432	0.91	0.79
81	2020-03-13	12:24:59	52	11.0	9.4	172	233	156	3	434	3	4.994	0.6102	0.9	0.79
82	2020-03-13	12:25:00	53	6.9	9.4	172	232	468	9	1420	10	4.994	0.606	0.91	0.79
83	2020-03-13	12:25:01	52	12.9	9.4	172	232	780	15	1988	14	4.994	0.6147	0.91	0.79
84	2020-03-13	12:25:02	53	7.4	9.4	172	232	572	11	1428	10	4.995	0.6113	0.79	0.61
85	2020-03-13	12:25:03	53	9.0	9.4	172	232	52	1	150	1	4.992	0.6141	0.82	0.63
86	2020-03-13	12:25:04	54	13.5	9.4	172	232	0	0	0	0	4.993	0.6096	0.82	0.63
87	2020-03-13	12:25:05	54	20.3	9.5	172	232	52	1	150	1	4.993	0.6031	0.91	0.79
88	2020-03-13	12:25:06	53	13.2	9.4	172	232	0	0	0	0	4.995	0.6184	0.91	0.79
89	2020-03-13	12:25:07	52	7.5	9.4	172	232	0	0	0	0	4.992	0.6388	0.9	0.79
90	2020-03-13	12:25:08	52	7.2	9.4	172	232	208	4	560	4	4.994	0.6414	0.82	0.63
91	2020-03-13	12:25:09	54	17.5	9.4	172	232	0	0	0	0	4.997	0.6414	0.82	0.63
92	2020-03-13	12:25:10	53	13.4	10.7	172	232	520	10	1420	10	4.996	0.6202	0.81	0.61
93	2020-03-13	12:25:11	52	9.2	10.2	172	232	416	8	1112	8	4.992	0.6155	0.82	0.62
94	2020-03-13	12:25:12	52	9.0	9.7	172	232	0	0	0	0	4.992	0.6047	0.88	0.72
95	2020-03-13	12:25:13	53	8.5	9.5	172	233	364	7	994	7	4.992	0.6292	0.91	0.79
96	2020-03-13	12:25:14	53	10.7	9.5	172	232	520	10	1428	10	4.993	0.6316	0.91	0.8

97	2020-03-13	12:25:15	55	8.1	9.4	172	232	52	1	150	1	4.993	0.6351	0.82	0.63
98	2020-03-13	12:25:16	53	14.9	9.4	172	232	0	0	0	0	4.994	0.6208	0.81	0.62
99	2020-03-13	12:25:17	53	12.6	9.4	172	232	208	4	568	4	4.994	0.6147	0.82	0.63
100	2020-03-13	12:25:18	54	13.7	9.5	172	232	728	14	1988	14	4.992	0.6231	0.91	0.78
101	2020-03-13	12:25:19	53	12.8	9.5	172	232	624	12	1712	12	4.993	0.6196	0.9	0.78
102	2020-03-13	12:25:20	53	12.7	9.5	172	233	52	1	150	1	4.994	0.6208	0.9	0.79
103	2020-03-13	12:25:21	52	7.7	9.5	172	232	0	0	0	0	4.995	0.6261	0.82	0.64
104	2020-03-13	12:25:22	53	17.8	9.5	172	232	208	4	576	4	4.995	0.6074	0.8	0.61
105	2020-03-13	12:25:23	53	9.2	9.5	172	232	0	0	0	0	4.994	0.6163	0.82	0.63
106	2020-03-13	12:25:24	52	8.1	9.4	172	232	156	3	702	5	4.996	0.6583	0.81	0.62
107	2020-03-13	12:25:25	53	13.7	9.5	172	232	52	1	0	0	4.996	0.6292	0.91	0.79
108	2020-03-13	12:25:26	52	15.6	9.4	172	232	0	0	0	0	4.996	0.6212	0.81	0.62
109	2020-03-13	12:25:27	54	17.3	9.4	172	232	988	19	2586	19	4.995	0.6214	0.82	0.63
110	2020-03-13	12:25:28	54	19.1	9.4	172	232	728	14	1932	14	4.993	0.6214	0.82	0.63
111	2020-03-13	12:25:29	54	14.3	9.5	172	232	0	0	0	0	4.994	0.6251	0.82	0.63
112	2020-03-13	12:25:30	55	19.6	9.5	172	232	52	1	142	1	4.995	0.6508	0.81	0.62
113	2020-03-13	12:25:31	53	18.5	9.5	172	232	0	0	0	0	4.995	0.6312	0.91	0.79
114	2020-03-13	12:25:32	54	15.8	9.5	172	232	52	1	142	1	4.994	0.6294	0.82	0.63
115	2020-03-13	12:25:33	53	9.4	9.5	172	232	0	0	0	0	4.992	0.6274	0.82	0.63
116	2020-03-13	12:25:34	53	6.9	9.5	172	232	52	1	142	1	4.997	0.6274	0.82	0.63
117	2020-03-13	12:25:35	54	7.6	9.5	172	232	0	0	0	0	4.996	0.5984	0.81	0.62
118	2020-03-13	12:25:36	54	14.2	9.5	172	232	104	2	268	2	4.996	0.6522	0.82	0.63
119	2020-03-13	12:25:37	53	11.4	9.5	172	232	0	0	0	0	4.996	0.6322	0.91	0.79
120	2020-03-13	12:25:38	53	9.9	9.7	172	232	52	1	142	1	4.996	0.6229	0.82	0.62
121	2020-03-13	12:25:39	53	6.2	9.5	172	232	0	0	0	0	4.994	0.6017	0.82	0.62

122	2020-03-13	12:25:40	53	13.7	9.5	172	232	0	0	0	0	4.994	0.6017	0.92	0.81
123	2020-03-13	12:25:41	53	16.9	9.5	172	232	52	1	142	1	4.997	0.6039	0.82	0.62
124	2020-03-13	12:25:42	53	15.3	9.5	172	232	0	0	0	0	4.995	0.6416	0.82	0.62
125	2020-03-13	12:25:43	54	21.3	9.5	172	233	52	1	142	1	4.995	0.6231	0.82	0.62
126	2020-03-13	12:25:44	54	26.4	10.5	173	233	0	0	0	0	4.994	0.6329	0.92	0.8
127	2020-03-13	12:25:47	53	7.1	9.5	172	232	52	1	284	2	4.996	0.6037	0.82	0.62
128	2020-03-13	12:25:48	53	11.2	9.5	172	232	0	0	0	0	4.998	0.6208	0.82	0.61
129	2020-03-13	12:25:49	53	11.1	9.5	172	232	0	0	268	2	4.997	0.6104	0.82	0.62
130	2020-03-13	12:25:50	53	7.1	9.5	172	232	52	1	178	1	4.995	0.621	0.82	0.62
131	2020-03-13	12:25:51	53	7.5	9.5	172	232	52	1	142	1	4.996	0.6263	0.91	0.8
132	2020-03-13	12:25:52	53	7.9	9.5	172	232	0	0	0	0	4.996	0.6239	0.92	0.8
133	2020-03-13	12:25:53	54	7.5	9.5	172	232	76	1	114	1	4.997	0.6182	0.92	0.8
134	2020-03-13	12:25:54	55	6.9	9.5	172	232	52	1	142	1	4.995	0.6225	0.82	0.62
135	2020-03-13	12:25:55	52	9.4	9.5	172	232	0	0	0	0	4.997	0.61	0.82	0.62
136	2020-03-13	12:25:56	54	19.5	9.5	172	232	52	1	142	1	4.996	0.6157	0.82	0.63
137	2020-03-13	12:25:57	52	12.4	9.5	172	232	0	0	0	0	4.995	0.6257	0.9	0.79
138	2020-03-13	12:25:58	52	13.0	9.5	172	232	80	2	208	2	4.994	0.6255	0.9	0.79
139	2020-03-13	12:25:59	54	11.1	9.5	172	233	0	0	0	0	4.994	0.618	0.91	0.79
140	2020-03-13	12:26:00	53	6.8	9.5	172	232	52	1	142	1	4.994	0.6239	0.8	0.61
141	2020-03-13	12:26:01	53	7.6	9.5	172	233	104	2	292	2	4.995	0.6145	0.82	0.63
142	2020-03-13	12:26:02	53	7.9	9.5	172	232	0	0	0	0	4.994	0.619	0.82	0.62
143	2020-03-13	12:26:03	54	8.9	9.5	172	233	260	5	710	5	4.996	0.619	0.83	0.62
144	2020-03-13	12:26:04	53	7.5	9.5	172	232	688	13	1988	14	4.996	0.6043	0.81	0.61
145	2020-03-13	12:26:05	54	10.2	9.5	172	232	728	14	1988	14	4.996	0.6337	0.82	0.62
146	2020-03-13	12:26:06	53	12.9	9.5	172	232	468	9	1144	8	4.996	0.6163	0.92	0.8

147	2020-03-13	12:26:07	53	11.6	9.5	172	232	52	1	150	1	4.995	0.6245	0.83	0.63
148	2020-03-13	12:26:08	53	13.2	9.5	172	232	52	1	150	1	4.995	0.6219	0.82	0.62
149	2020-03-13	12:26:09	53	14.4	9.5	172	233	0	0	0	0	4.996	0.6188	0.81	0.61
150	2020-03-13	12:26:10	53	16.4	9.5	172	232	156	3	568	4	4.996	0.6375	0.91	0.8
151	2020-03-13	12:26:11	53	7.6	9.5	172	233	676	13	1846	13	4.995	0.6341	0.91	0.8
152	2020-03-13	12:26:12	53	6.8	9.5	172	232	676	13	1988	14	4.995	0.6117	0.92	0.8
153	2020-03-13	12:26:13	54	9.0	9.7	172	232	624	12	1570	11	4.995	0.6145	0.83	0.63
154	2020-03-13	12:26:14	53	8.0	9.5	172	232	52	1	150	1	4.995	0.6096	0.82	0.62
155	2020-03-13	12:26:15	53	7.3	9.5	172	232	0	0	0	0	4.992	0.6316	0.82	0.62
156	2020-03-13	12:26:16	53	10.3	9.5	172	232	52	1	150	1	4.994	0.6051	0.82	0.62
157	2020-03-13	12:26:17	52	12.8	9.5	172	232	0	0	0	0	4.993	0.6137	0.92	0.8
158	2020-03-13	12:26:18	54	14.3	9.6	172	232	0	0	0	0	4.993	0.6168	0.92	0.8
159	2020-03-13	12:26:19	54	19.3	10.4	172	232	208	4	560	4	4.993	0.6153	0.91	0.8
160	2020-03-13	12:26:22	54	17.1	9.5	172	232	0	0	0	0	4.995	0.6357	0.82	0.62
161	2020-03-13	12:26:23	54	25.3	9.5	172	232	416	8	1136	8	4.994	0.6357	0.91	0.79
162	2020-03-13	12:26:24	54	15.7	9.5	172	232	364	7	1002	7	4.994	0.6581	0.8	0.62
163	2020-03-13	12:26:25	55	12.8	9.5	172	232	104	2	150	1	4.994	0.6208	0.82	0.63
164	2020-03-13	12:26:26	54	10.4	9.5	172	232	0	0	0	0	4.994	0.6166	0.82	0.63
165	2020-03-13	12:26:27	53	7.8	9.5	172	233	156	3	434	3	4.994	0.6123	0.82	0.63
166	2020-03-13	12:26:28	54	8.1	9.5	172	232	0	0	0	0	4.995	0.6296	0.81	0.62
167	2020-03-13	12:26:29	53	8.0	9.5	172	232	52	1	150	1	4.996	0.6296	0.81	0.62
168	2020-03-13	12:26:30	52	16.2	9.5	172	232	0	0	0	0	4.996	0.6426	0.91	0.8
169	2020-03-13	12:26:31	54	16.5	9.5	172	232	52	1	150	1	4.994	0.6426	0.92	0.8
170	2020-03-13	12:26:32	54	15.1	9.5	172	232	52	1	150	1	4.994	0.6353	0.92	0.8
171	2020-03-13	12:26:33	54	14.0	9.5	172	232	0	0	0	0	4.995	0.6322	0.81	0.62

172	2020-03-13	12:26:34	55	17.0	9.5	172	232	0	0	0	0	4.995	0.6302	0.83	0.63
173	2020-03-13	12:26:35	54	17.2	9.5	172	232	208	4	576	4	4.994	0.6263	0.82	0.62
174	2020-03-13	12:26:36	54	14.4	9.5	172	232	0	0	0	0	4.995	0.6326	0.92	0.8
175	2020-03-13	12:26:37	54	10.0	9.5	172	232	52	1	150	1	4.995	0.6306	0.92	0.81
176	2020-03-13	12:26:38	54	7.5	9.5	172	232	520	10	1278	9	4.995	0.6168	0.92	0.8
177	2020-03-13	12:26:39	53	9.9	9.5	172	232	520	10	1428	10	4.997	0.6072	0.92	0.8
178	2020-03-13	12:26:40	53	7.9	9.5	172	232	52	1	150	1	4.996	0.6314	0.82	0.62
179	2020-03-13	12:26:41	54	17.3	9.5	172	232	52	1	142	1	4.997	0.6206	0.81	0.61
180	2020-03-13	12:26:42	54	7.8	9.5	166	227	104	2	292	2	4.992	0.6108	0.83	0.62
181	2020-03-13	12:26:43	54	7.1	9.5	164	224	0	0	0	0	4.996	0.6119	0.91	0.8
182	2020-03-13	12:26:44	53	12.8	9.5	163	223	520	10	1420	10	4.996	0.5992	0.92	0.8
183	2020-03-13	12:26:45	54	10.4	9.5	163	223	624	12	1704	12	4.995	0.6216	0.8	0.6
184	2020-03-13	12:26:46	54	8.6	9.5	162	222	780	15	2114	15	4.993	0.6139	0.82	0.62
185	2020-03-13	12:26:47	55	15.8	9.5	161	221	832	16	2122	15	4.993	0.6072	0.83	0.62
186	2020-03-13	12:26:48	54	18.3	10.0	161	222	0	0	0	0	4.996	0.6265	0.83	0.62
187	2020-03-13	12:26:49	54	12.6	9.6	162	222	52	1	150	1	4.994	0.6247	0.92	0.8
188	2020-03-13	12:26:50	54	10.1	9.5	160	220	0	0	0	0	4.993	0.6383	0.91	0.8
189	2020-03-13	12:26:51	55	7.7	9.5	160	221	324	6	860	6	4.995	0.6066	0.92	0.8
190	2020-03-13	12:26:52	54	7.7	9.5	159	219	0	0	0	0	4.994	0.6051	0.92	0.8
191	2020-03-13	12:26:53	53	16.9	10.5	159	221	156	3	410	3	4.994	0.6178	0.81	0.61
192	2020-03-13	12:26:54	53	7.6	10.1	161	221	688	13	1846	13	4.992	0.609	0.82	0.61
193	2020-03-13	12:26:56	54	13.3	9.5	162	222	792	15	1988	14	4.993	0.6357	0.92	0.8
194	2020-03-13	12:26:57	54	16.6	9.5	162	222	728	14	2130	15	4.996	0.6245	0.93	0.81
195	2020-03-13	12:26:58	54	14.9	9.5	162	222	208	4	434	3	4.992	0.6248	0.92	0.8
196	2020-03-13	12:26:59	54	13.8	9.5	162	222	156	3	434	3	4.994	0.6223	0.83	0.62

197	2020-03-13	12:27:00	54	16.9	9.5	162	222	0	0	0	0	4.993	0.6186	0.82	0.62
198	2020-03-13	12:27:01	55	15.1	9.5	162	223	52	1	150	1	4.993	0.6278	0.8	0.61
199	2020-03-13	12:27:02	54	10.9	9.5	162	222	0	0	0	0	4.994	0.6263	0.82	0.62
200	2020-03-13	12:27:03	53	7.3	9.5	162	222	52	1	150	1	4.994	0.6133	0.82	0.63
201	2020-03-13	12:27:04	54	7.9	9.5	162	222	0	0	0	0	4.996	0.6133	0.91	0.79
202	2020-03-13	12:27:05	54	11.6	9.5	162	222	0	0	142	1	4.996	0.6469	0.8	0.62
203	2020-03-13	12:27:06	54	12.7	9.5	162	222	676	13	1846	13	4.996	0.6058	0.82	0.62
204	2020-03-13	12:27:07	54	7.6	9.5	162	222	208	4	576	4	4.996	0.6151	0.83	0.62
205	2020-03-13	12:27:08	53	8.1	9.5	162	222	467	5	560	4	4.994	0.6192	0.82	0.62
206	2020-03-13	12:27:09	54	8.0	9.5	162	222	259	1	0	0	4.997	0.6125	0.81	0.61
207	2020-03-13	12:27:10	53	8.2	9.5	162	222	0	0	142	1	4.997	0.6125	0.93	0.81
208	2020-03-13	12:27:11	55	7.1	9.5	162	222	467	5	434	3	4.997	0.6357	0.83	0.62
209	2020-03-13	12:27:12	53	9.1	9.5	162	222	0	0	0	0	4.995	0.6129	0.82	0.62
210	2020-03-13	12:27:13	54	14.8	9.5	162	222	52	1	150	1	4.995	0.6051	0.83	0.62
211	2020-03-13	12:27:14	54	19.4	9.5	162	222	52	1	142	1	4.991	0.6218	0.8	0.6
212	2020-03-13	12:27:15	54	13.4	9.5	162	222	415	4	434	3	4.994	0.6324	0.82	0.62
213	2020-03-13	12:27:16	54	7.7	9.5	162	223	0	0	0	0	4.995	0.6324	0.92	0.8
214	2020-03-13	12:27:17	54	7.4	9.5	162	222	208	4	576	4	4.997	0.6457	0.83	0.62
215	2020-03-13	12:27:18	53	7.9	9.5	162	222	0	0	0	0	4.995	0.6102	0.81	0.62
216	2020-03-13	12:27:19	54	7.6	9.5	162	222	104	2	284	2	4.995	0.608	0.81	0.62
217	2020-03-13	12:27:20	53	7.3	9.5	162	222	728	14	1988	14	4.994	0.6045	0.82	0.63
218	2020-03-13	12:27:21	54	11.1	9.5	161	221	728	14	1988	14	4.996	0.6096	0.82	0.63
219	2020-03-13	12:27:22	53	9.3	9.5	162	222	312	6	860	6	4.995	0.6096	0.91	0.79
220	2020-03-13	12:27:23	54	10.4	9.5	162	222	156	3	434	3	4.995	0.6394	0.8	0.61
221	2020-03-13	12:27:24	54	13.0	9.5	162	222	0	0	0	0	4.995	0.6072	0.82	0.63

222	2020-03-13	12:27:25	54	9.8	9.5	163	223	0	0	0	0	4.995	0.6186	0.82	0.62
223	2020-03-13	12:27:26	54	13.3	9.5	163	223	208	4	576	4	4.994	0.6106	0.82	0.63
224	2020-03-13	12:27:27	54	20.3	10.7	164	224	0	0	0	0	4.992	0.629	0.83	0.62
225	2020-03-13	12:27:28	53	11.7	10.2	163	223	52	1	150	1	4.991	0.6652	0.92	0.8
226	2020-03-13	12:27:29	53	7.3	9.8	163	223	364	7	994	7	4.989	0.6351	0.92	0.8
227	2020-03-13	12:27:30	54	9.9	9.5	163	223	728	14	1988	14	4.993	0.6304	0.92	0.8
228	2020-03-13	12:27:31	54	18.2	9.5	163	224	728	14	1988	14	4.993	0.6121	0.92	0.8
229	2020-03-13	12:27:32	54	19.3	9.5	163	223	312	6	860	6	4.995	0.6257	0.83	0.62
230	2020-03-13	12:27:33	54	18.6	9.5	163	223	416	8	1278	9	4.994	0.6337	0.82	0.62
231	2020-03-13	12:27:34	55	17.4	9.5	163	223	468	9	1144	8	4.994	0.6269	0.83	0.62
232	2020-03-13	12:27:35	55	17.2	9.5	163	224	52	1	142	1	4.994	0.6247	0.92	0.8
233	2020-03-13	12:27:36	54	15.3	9.5	163	223	104	2	292	2	4.994	0.6243	0.91	0.8
234	2020-03-13	12:27:37	55	13.8	9.5	163	223	0	0	0	0	4.994	0.6242	0.92	0.8
235	2020-03-13	12:27:38	54	20.6	9.5	163	223	52	1	150	1	4.994	0.62	0.82	0.62
236	2020-03-13	12:27:39	54	17.2	9.5	163	223	0	0	0	0	4.992	0.6312	0.82	0.62
237	2020-03-13	12:27:40	53	11.7	9.5	163	224	208	4	576	4	4.992	0.6294	0.83	0.62
238	2020-03-13	12:27:41	54	10.5	9.5	163	223	0	0	0	0	4.992	0.6267	0.82	0.62
239	2020-03-13	12:27:42	54	12.6	9.5	163	223	52	1	142	1	4.997	0.5994	0.81	0.62
240	2020-03-13	12:27:43	54	10.3	9.5	163	223	728	14	1988	14	4.995	0.5994	0.92	0.8
241	2020-03-13	12:27:44	54	7.1	9.5	163	223	208	4	576	4	4.995	0.6202	0.82	0.63
242	2020-03-13	12:27:45	54	6.6	9.5	163	223	52	1	150	1	4.997	0.6178	0.81	0.62
243	2020-03-13	12:27:46	54	9.3	9.5	163	223	52	1	150	1	4.997	0.6117	0.82	0.62
244	2020-03-13	12:27:47	53	13.4	9.5	163	223	0	0	0	0	4.995	0.609	0.81	0.62
245	2020-03-13	12:27:48	54	11.4	9.5	163	223	52	1	150	1	4.995	0.6145	0.79	0.6
246	2020-03-13	12:27:49	54	8.1	9.5	163	224	0	0	0	0	4.996	0.6145	0.91	0.8

247	2020-03-13	12:27:50	54	7.7	9.5	163	223	304	5	860	6	4.997	0.6176	0.91	0.79
248	2020-03-13	12:27:51	54	14.2	9.5	163	223	0	0	0	0	4.995	0.6104	0.83	0.63
249	2020-03-13	12:27:52	54	17.8	9.5	163	223	0	0	0	0	4.994	0.6192	0.81	0.61
250	2020-03-13	12:27:53	55	15.4	9.5	163	223	116	2	814	5	4.994	0.6361	0.83	0.62
251	2020-03-13	12:27:54	55	13.4	9.5	163	223	272	5	1342	5	4.994	0.6496	0.82	0.62
252	2020-03-13	12:27:55	54	9.0	9.5	163	223	104	2	276	2	4.995	0.6469	0.92	0.8
253	2020-03-13	12:27:56	54	18.5	9.5	163	223	0	0	0	0	4.994	0.6237	0.92	0.81
254	2020-03-13	12:27:57	55	9.1	9.5	163	223	260	5	702	5	4.994	0.6432	0.92	0.8
255	2020-03-13	12:27:58	54	6.6	9.5	163	223	0	0	0	0	4.995	0.6589	0.82	0.62
256	2020-03-13	12:27:59	54	8.2	9.5	163	223	52	1	150	1	4.995	0.6276	0.82	0.62
257	2020-03-13	12:28:00	55	11.9	10.6	163	223	0	0	0	0	4.996	0.6404	0.82	0.62
258	2020-03-13	12:28:01	54	8.3	10.1	163	223	52	1	142	1	4.992	0.6312	0.92	0.8
259	2020-03-13	12:28:02	54	8.0	9.6	163	223	728	14	1988	14	4.994	0.6542	0.92	0.8
260	2020-03-13	12:28:03	54	15.0	9.5	163	224	728	14	1980	14	4.994	0.64	0.92	0.8
261	2020-03-13	12:28:04	55	19.9	9.5	163	223	52	1	150	1	4.995	0.6569	0.82	0.62
262	2020-03-13	12:28:05	55	19.7	9.5	163	224	0	0	0	0	4.994	0.6498	0.82	0.62
263	2020-03-13	12:28:06	55	15.9	9.5	164	224	0	0	0	0	4.994	0.6367	0.82	0.62
264	2020-03-13	12:28:07	54	16.4	9.5	164	224	52	1	150	1	4.994	0.6241	0.81	0.62
265	2020-03-13	12:28:08	55	18.0	9.5	164	224	0	0	0	0	4.993	0.6214	0.91	0.8
266	2020-03-13	12:28:09	55	17.7	9.5	163	223	676	13	1846	13	4.993	0.6357	0.91	0.79
267	2020-03-13	12:28:10	55	15.2	9.5	163	223	728	14	1988	14	4.992	0.6273	0.91	0.79
268	2020-03-13	12:28:11	55	12.6	9.5	163	223	260	5	718	5	4.992	0.61	0.81	0.62
269	2020-03-13	12:28:12	54	10.7	9.5	163	223	52	1	150	1	4.993	0.6133	0.8	0.61
270	2020-03-13	12:28:13	54	8.1	9.5	163	223	0	0	0	0	4.994	0.6113	0.82	0.62
271	2020-03-13	12:28:14	55	7.9	9.5	163	223	208	4	576	4	4.994	0.6114	0.91	0.79

272	2020-03-13	12:28:15	55	10.0	9.5	163	223	0	0	0	0	4.994	0.595	0.91	0.79
273	2020-03-13	12:28:16	55	17.3	9.5	163	223	52	1	150	1	4.994	0.6125	0.92	0.8
274	2020-03-13	12:28:17	54	21.1	9.5	163	223	0	0	0	0	4.994	0.6202	0.83	0.63
275	2020-03-13	12:28:18	55	20.5	9.5	163	224	208	4	568	4	4.992	0.6271	0.82	0.63
276	2020-03-13	12:28:19	55	15.4	9.5	163	223	728	14	1988	14	4.994	0.6282	0.82	0.62
277	2020-03-13	12:28:20	55	10.4	9.5	163	224	416	8	1002	7	4.994	0.6204	0.8	0.61
278	2020-03-13	12:28:21	54	7.9	9.5	163	224	52	1	150	1	4.995	0.6094	0.9	0.79
279	2020-03-13	12:28:22	55	7.3	9.5	163	224	0	0	0	0	4.995	0.6035	0.91	0.79
280	2020-03-13	12:28:23	53	7.5	9.5	163	224	156	3	434	3	4.995	0.6078	0.81	0.63
281	2020-03-13	12:28:24	54	11.1	9.5	163	224	0	0	0	0	4.996	0.6176	0.82	0.63
282	2020-03-13	12:28:25	54	7.9	9.5	163	224	104	2	276	2	4.996	0.6176	0.82	0.63
283	2020-03-13	12:28:26	54	7.3	9.5	163	224	0	0	0	0	4.996	0.632	0.82	0.63
284	2020-03-13	12:28:27	55	8.4	9.5	163	223	52	1	150	1	4.997	0.6259	0.91	0.8
285	2020-03-13	12:28:28	55	10.6	9.5	163	223	0	0	0	0	4.997	0.6351	0.93	0.81
286	2020-03-13	12:28:29	55	22.1	9.5	163	223	260	5	702	5	4.994	0.6304	0.92	0.8
287	2020-03-13	12:28:30	55	14.1	9.5	163	223	0	0	0	0	4.993	0.6351	0.92	0.8
288	2020-03-13	12:28:31	55	13.1	9.5	163	223	364	7	1002	7	4.996	0.6514	0.83	0.62
289	2020-03-13	12:28:32	54	7.6	9.5	163	223	52	1	150	1	4.995	0.6335	0.8	0.6
290	2020-03-13	12:28:33	54	12.2	10.6	164	225	0	0	0	0	4.997	0.6212	0.83	0.62
291	2020-03-13	12:28:34	55	19.3	10.1	164	224	52	1	150	1	4.994	0.6092	0.92	0.8
292	2020-03-13	12:28:35	55	8.6	9.7	164	224	0	0	0	0	4.991	0.6414	0.92	0.8
293	2020-03-13	12:28:36	55	6.2	9.5	164	224	156	3	434	3	4.995	0.6229	0.92	0.8
294	2020-03-13	12:28:37	54	8.5	9.5	164	224	0	0	0	0	4.997	0.6249	0.83	0.62
295	2020-03-13	12:28:38	54	17.2	9.5	164	225	52	1	142	1	4.997	0.628	0.82	0.62
296	2020-03-13	12:28:39	55	18.8	9.5	164	224	156	3	434	3	4.995	0.6443	0.82	0.62

297	2020-03-13	12:28:40	55	15.9	9.5	164	224	0	0	0	0	4.995	0.6426	0.82	0.62
298	2020-03-13	12:28:41	55	14.7	9.5	164	224	52	1	150	1	4.996	0.6267	0.82	0.62
299	2020-03-13	12:28:42	54	18.7	9.5	164	224	0	0	0	0	4.996	0.6235	0.92	0.8
300	2020-03-13	12:28:43	54	17.4	9.5	164	224	260	5	576	4	4.995	0.63	0.83	0.63
301	2020-03-13	12:28:44	55	18.9	9.5	164	224	0	0	0	0	4.995	0.63	0.8	0.6
302	2020-03-13	12:28:45	55	9.7	9.5	164	224	156	3	568	4	4.994	0.6357	0.82	0.62
303	2020-03-13	12:28:46	55	13.8	9.5	164	224	728	13	1846	13	4.996	0.6163	0.82	0.62
304	2020-03-13	12:28:47	55	7.0	9.5	164	225	624	12	1570	11	4.996	0.6163	0.92	0.8
305	2020-03-13	12:28:48	54	10.4	9.5	164	225	208	4	568	4	4.997	0.6373	0.92	0.8
306	2020-03-13	12:28:49	54	7.9	9.5	164	224	792	15	2224	16	4.996	0.631	0.91	0.79
307	2020-03-13	12:28:50	54	12.1	9.5	164	224	572	11	1846	13	4.996	0.6394	0.82	0.63
308	2020-03-13	12:28:51	54	17.2	9.6	164	224	388	7	1874	11	4.996	0.6371	0.82	0.63
309	2020-03-13	12:28:52	55	17.4	9.6	164	224	104	2	708	2	4.994	0.652	0.81	0.61
310	2020-03-13	12:28:53	54	17.2	9.5	164	224	208	4	576	4	4.994	0.6471	0.9	0.79
311	2020-03-13	12:28:54	55	16.9	9.5	164	224	0	0	0	0	4.995	0.6434	0.91	0.79
312	2020-03-13	12:28:55	55	14.1	9.5	164	224	52	1	142	1	4.995	0.631	0.91	0.79
313	2020-03-13	12:28:56	55	12.8	9.5	164	224	156	3	434	3	4.995	0.6335	0.81	0.62
314	2020-03-13	12:28:57	55	17.7	9.5	164	224	0	0	0	0	4.995	0.6251	0.81	0.62
315	2020-03-13	12:28:58	55	16.6	9.5	164	224	180	3	434	3	4.995	0.6212	0.81	0.62
316	2020-03-13	12:28:59	55	16.3	9.5	164	224	0	0	0	0	4.995	0.6269	0.81	0.62
317	2020-03-13	12:29:00	55	14.8	9.5	164	224	312	6	852	6	4.995	0.6235	0.91	0.79
318	2020-03-13	12:29:01	54	15.0	9.5	165	225	676	13	1846	13	4.995	0.6113	0.91	0.79
319	2020-03-13	12:29:02	55	10.9	9.5	165	225	468	9	1286	9	4.993	0.6367	0.82	0.62
320	2020-03-13	12:29:03	54	7.7	9.5	165	225	156	3	434	3	4.995	0.6166	0.8	0.61
321	2020-03-13	12:29:04	55	7.0	9.5	165	225	52	1	150	1	4.995	0.6039	0.81	0.62

322	2020-03-13	12:29:05	54	7.6	9.5	165	225	0	0	0	0	4.995	0.6292	0.82	0.63
323	2020-03-13	12:29:06	55	18.9	10.7	165	225	0	0	0	0	4.997	0.6347	0.82	0.62
324	2020-03-13	12:29:07	55	8.2	10.2	165	225	0	0	142	1	4.994	0.6347	0.91	0.79
325	2020-03-13	12:29:08	55	18.1	9.7	165	226	52	1	0	0	4.994	0.6235	0.81	0.62
326	2020-03-13	12:29:09	54	13.1	9.5	166	226	104	2	268	2	4.992	0.6416	0.81	0.62
327	2020-03-13	12:29:10	55	11.8	9.5	166	226	0	0	0	0	4.992	0.631	0.82	0.63
328	2020-03-13	12:29:11	55	7.3	9.5	166	226	0	0	142	1	4.995	0.6324	0.81	0.62
329	2020-03-13	12:29:12	55	16.6	9.5	166	225	52	1	0	0	4.997	0.6536	0.8	0.61
330	2020-03-13	12:29:13	55	7.2	9.5	165	225	0	0	0	0	4.996	0.6536	0.92	0.8
331	2020-03-13	12:29:14	55	7.8	9.6	165	225	52	1	142	1	4.994	0.6055	0.82	0.63
332	2020-03-13	12:29:15	54	7.9	9.6	165	225	0	0	0	0	4.996	0.6131	0.82	0.63
333	2020-03-13	12:29:16	55	10.3	9.6	165	225	52	1	142	1	4.996	0.6182	0.82	0.62
334	2020-03-13	12:29:16	55	14.5	9.6	165	225	0	0	0	0	4.996	0.6182	0.82	0.62
335	2020-03-13	12:29:17	55	14.8	9.6	165	225	104	2	268	2	4.995	0.6221	0.82	0.62
336	2020-03-13	12:29:18	55	16.3	9.6	165	225	0	0	0	0	4.995	0.628	0.83	0.64

Run-2-Log															
	Date	T.Stamp	Temp	CPU_Load	Mem_Load	ProNo,	ThreadsNo	RX_bit	RX_pkt	TX_bit	TX_pkt	Voltage(V)	Current(A)	D+(V)	D-(V)
1	2020-03-13	13:31:53	38	18.2	9.3	170	230	792	15	2130	15	4.997	0.5945	0.94	0.81
2	2020-03-13	13:31:54	39	17.3	9.3	170	230	104	2	292	2	4.997	0.6204	0.92	0.77
3	2020-03-13	13:31:55	39	17.4	9.3	170	230	52	1	150	1	4.996	0.6245	0.89	0.7
4	2020-03-13	13:31:56	39	17.4	9.3	170	231	0	0	0	0	4.996	0.6337	0.95	0.83
5	2020-03-13	13:31:57	40	16.2	9.3	170	231	156	3	434	3	4.995	0.6424	0.95	0.83
6	2020-03-13	13:31:58	39	6.8	9.3	170	230	0	0	0	0	4.997	0.6567	0.95	0.83
7	2020-03-13	13:31:59	39	8.9	9.3	170	230	0	0	0	0	4.996	0.6473	0.88	0.7
8	2020-03-13	13:32:00	39	16.6	9.3	170	230	208	4	576	4	4.998	0.6461	0.93	0.79
9	2020-03-13	13:32:01	41	24.1	9.3	170	230	0	0	0	0	4.998	0.6361	0.93	0.79
10	2020-03-13	13:32:02	41	22.1	9.3	171	231	364	7	994	7	4.997	0.651	0.88	0.68
11	2020-03-13	13:32:03	40	19.3	9.4	171	231	884	17	2394	17	4.997	0.6371	0.93	0.8
12	2020-03-13	13:32:04	40	16.2	9.3	171	232	272	5	654	5	4.995	0.6371	0.95	0.83
13	2020-03-13	13:32:05	40	13.3	9.3	172	232	0	0	0	0	4.995	0.6341	0.95	0.83
14	2020-03-13	13:32:06	40	12.0	9.3	171	231	260	5	702	5	4.996	0.6186	0.88	0.67
15	2020-03-13	13:32:07	40	12.3	9.3	171	231	0	0	0	0	4.997	0.6159	0.84	0.63
16	2020-03-13	13:32:08	40	8.0	9.3	171	231	52	1	142	1	4.997	0.6316	0.87	0.67
17	2020-03-13	13:32:09	40	9.7	9.4	171	231	156	3	434	3	4.997	0.6312	0.93	0.81
18	2020-03-13	13:32:10	40	8.5	9.4	171	231	0	0	0	0	4.998	0.6263	0.93	0.8
19	2020-03-13	13:32:11	41	9.5	9.4	171	231	52	1	150	1	4.998	0.6298	0.93	0.81
20	2020-03-13	13:32:12	41	7.7	9.4	171	231	0	0	0	0	4.998	0.6335	0.86	0.66
21	2020-03-13	13:32:13	40	14.4	9.4	171	231	52	1	150	1	4.998	0.6337	0.87	0.66
22	2020-03-13	13:32:14	41	21.0	9.4	171	231	0	0	0	0	4.998	0.6294	0.87	0.68
23	2020-03-13	13:32:15	42	19.2	9.4	171	231	376	7	1278	9	4.996	0.6477	0.86	0.66

24	2020-03-13	13:32:16	40	13.3	9.3	171	232	988	19	2492	18	4.994	0.6583	0.93	0.81
25	2020-03-13	13:32:17	41	8.7	9.3	171	231	416	8	1144	8	4.995	0.6512	0.92	0.8
26	2020-03-13	13:32:18	41	7.3	9.3	171	231	52	1	150	1	4.996	0.6335	0.93	0.81
27	2020-03-13	13:32:19	40	9.4	9.5	171	231	0	0	0	0	4.998	0.6437	0.86	0.66
28	2020-03-13	13:32:20	42	16.0	10.4	171	231	260	5	710	5	4.998	0.6426	0.88	0.67
29	2020-03-13	13:32:23	41	7.5	9.4	171	231	156	3	434	3	4.996	0.6037	0.85	0.65
30	2020-03-13	13:32:24	42	14.3	9.4	171	231	0	0	0	0	4.998	0.6013	0.86	0.66
31	2020-03-13	13:32:25	41	10.9	9.4	171	231	636	12	1656	13	4.998	0.6013	0.93	0.81
32	2020-03-13	13:32:26	42	10.1	9.4	171	231	728	14	1846	13	4.997	0.6263	0.86	0.66
33	2020-03-13	13:32:27	42	14.3	9.4	171	231	728	14	1988	14	4.994	0.6131	0.86	0.65
34	2020-03-13	13:32:28	41	22.6	9.3	171	231	260	5	718	5	4.994	0.6166	0.86	0.66
35	2020-03-13	13:32:29	42	17.9	9.4	171	231	52	1	150	1	4.995	0.6286	0.88	0.67
36	2020-03-13	13:32:30	42	17.8	9.4	171	231	0	0	0	0	4.995	0.6473	0.88	0.67
37	2020-03-13	13:32:31	42	17.7	9.3	171	232	324	6	1420	10	4.997	0.6473	0.93	0.81
38	2020-03-13	13:32:32	42	15.2	9.4	171	232	544	9	1876	12	4.996	0.6251	0.87	0.66
39	2020-03-13	13:32:33	42	15.7	9.4	171	231	52	1	0	0	4.997	0.62	0.92	0.8
40	2020-03-13	13:32:34	42	15.1	9.4	171	231	364	7	994	7	4.996	0.6119	0.88	0.67
41	2020-03-13	13:32:35	42	13.6	9.4	171	231	572	11	1570	11	4.997	0.6216	0.88	0.67
42	2020-03-13	13:32:36	42	14.0	9.4	171	231	52	1	150	1	4.997	0.6184	0.94	0.82
43	2020-03-13	13:32:37	42	10.2	9.4	171	231	0	0	0	0	4.996	0.6174	0.93	0.81
44	2020-03-13	13:32:38	43	10.1	9.4	171	231	180	3	398	3	4.997	0.6176	0.93	0.81
45	2020-03-13	13:32:39	43	18.9	9.4	171	231	728	14	1988	14	4.997	0.6023	0.87	0.66
46	2020-03-13	13:32:40	43	13.2	9.4	171	231	728	14	1988	14	4.997	0.6119	0.85	0.64
47	2020-03-13	13:32:41	42	16.1	9.4	171	231	312	6	860	6	4.994	0.6494	0.87	0.66
48	2020-03-13	13:32:42	43	7.5	9.4	171	231	156	3	434	3	4.994	0.6131	0.93	0.81

49	2020-03-13	13:32:43	43	7.7	9.4	171	231	28	1	66	1	4.994	0.6163	0.94	0.81
50	2020-03-13	13:32:44	42	15.4	9.4	171	231	0	0	0	0	4.995	0.6027	0.93	0.81
51	2020-03-13	13:32:45	43	13.3	9.4	171	231	208	4	576	4	4.995	0.6009	0.88	0.67
52	2020-03-13	13:32:46	42	12.5	9.4	171	231	0	0	0	0	4.995	0.6153	0.88	0.67
53	2020-03-13	13:32:47	44	11.5	9.4	171	231	52	1	150	1	4.995	0.6139	0.87	0.66
54	2020-03-13	13:32:48	43	10.0	9.4	171	231	52	1	142	1	4.995	0.61	0.87	0.66
55	2020-03-13	13:32:49	43	10.3	9.6	171	231	208	4	560	4	4.998	0.6005	0.86	0.66
56	2020-03-13	13:32:50	42	7.8	9.4	171	231	0	0	0	0	4.998	0.6253	0.93	0.8
57	2020-03-13	13:32:51	42	13.9	9.4	171	232	156	3	426	3	4.998	0.6351	0.93	0.81
58	2020-03-13	13:32:52	42	11.2	9.4	171	231	104	2	276	2	4.995	0.6318	0.82	0.63
59	2020-03-13	13:32:53	43	15.8	9.4	172	232	0	0	0	0	4.994	0.6253	0.86	0.66
60	2020-03-13	13:32:54	43	24.0	10.2	172	233	104	2	292	2	4.996	0.6575	0.86	0.66
61	2020-03-13	13:32:55	44	15.4	10.3	173	233	208	4	576	4	4.996	0.654	0.92	0.8
62	2020-03-13	13:32:56	43	11.8	9.8	173	233	0	0	0	0	4.995	0.6746	0.92	0.8
63	2020-03-13	13:32:58	43	7.0	9.4	172	232	104	2	276	2	4.995	0.6449	0.92	0.8
64	2020-03-13	13:32:59	44	8.2	9.4	172	233	0	0	0	0	4.998	0.5929	0.86	0.66
65	2020-03-13	13:33:00	42	8.4	9.4	172	232	156	3	434	3	4.994	0.6235	0.86	0.66
66	2020-03-13	13:33:01	43	7.8	9.4	172	232	0	0	0	0	4.998	0.6182	0.86	0.66
67	2020-03-13	13:33:02	43	12.3	9.4	172	232	52	1	142	1	4.997	0.6263	0.92	0.8
68	2020-03-13	13:33:03	43	13.2	9.4	172	232	208	4	576	4	4.997	0.6298	0.92	0.8
69	2020-03-13	13:33:04	43	7.3	9.4	172	232	0	0	0	0	4.998	0.6559	0.92	0.8
70	2020-03-13	13:33:05	44	15.5	9.4	172	232	156	3	402	3	4.997	0.6312	0.86	0.66
71	2020-03-13	13:33:06	44	15.1	9.4	172	232	0	0	0	0	4.999	0.6184	0.87	0.66
72	2020-03-13	13:33:07	44	10.7	9.4	172	232	52	1	150	1	4.995	0.6184	0.87	0.66
73	2020-03-13	13:33:08	44	10.4	9.4	172	233	0	0	0	0	4.995	0.6259	0.83	0.63

74	2020-03-13	13:33:09	44	13.3	9.4	172	232	364	7	1136	8	4.998	0.6117	0.86	0.66
75	2020-03-13	13:33:10	44	11.3	9.4	172	233	1300	25	3232	24	4.998	0.6436	0.92	0.8
76	2020-03-13	13:33:11	43	8.0	9.4	172	232	780	15	2114	15	4.998	0.6221	0.92	0.81
77	2020-03-13	13:33:12	43	11.8	9.4	172	232	1404	27	3894	29	4.997	0.6196	0.84	0.64
78	2020-03-13	13:33:13	44	11.1	9.4	172	232	1364	26	3500	26	4.997	0.595	0.86	0.66
79	2020-03-13	13:33:14	43	7.2	9.4	172	232	884	17	2508	18	4.996	0.595	0.86	0.66
80	2020-03-13	13:33:15	45	9.1	9.4	172	232	208	4	434	3	4.997	0.6058	0.92	0.8
81	2020-03-13	13:33:16	43	8.3	9.4	172	232	52	1	150	1	4.996	0.619	0.93	0.81
82	2020-03-13	13:33:17	43	15.1	9.4	172	232	0	0	0	0	4.996	0.6151	0.93	0.81
83	2020-03-13	13:33:18	45	20.5	9.4	172	232	208	4	576	4	4.996	0.6119	0.87	0.66
84	2020-03-13	13:33:19	44	19.4	9.4	172	232	0	0	0	0	4.994	0.6218	0.87	0.66
85	2020-03-13	13:33:20	45	16.2	9.4	172	232	52	1	150	1	4.994	0.6333	0.86	0.65
86	2020-03-13	13:33:21	44	16.0	9.4	172	232	0	0	0	0	4.993	0.6259	0.85	0.65
87	2020-03-13	13:33:22	46	18.6	9.4	172	232	156	3	426	3	4.994	0.6212	0.92	0.8
88	2020-03-13	13:33:23	45	19.7	9.7	172	232	1352	26	3516	26	4.994	0.6194	0.92	0.8
89	2020-03-13	13:33:24	45	19.8	9.4	172	232	780	15	2062	15	4.994	0.6221	0.93	0.8
90	2020-03-13	13:33:25	44	18.7	9.4	172	232	0	0	300	2	4.993	0.6219	0.86	0.65
91	2020-03-13	13:33:26	44	12.7	9.4	172	232	116	2	0	0	4.994	0.6339	0.86	0.66
92	2020-03-13	13:33:27	44	10.2	9.4	172	233	572	10	1072	8	4.995	0.6335	0.86	0.66
93	2020-03-13	13:33:28	45	8.4	9.4	172	232	468	9	1254	9	4.997	0.6017	0.93	0.81
94	2020-03-13	13:33:29	45	12.1	10.5	172	233	52	1	150	1	4.998	0.6119	0.92	0.8
95	2020-03-13	13:33:30	45	9.0	10.0	172	232	0	0	0	0	4.995	0.5964	0.86	0.66
96	2020-03-13	13:33:31	45	21.6	9.6	172	232	104	2	268	2	4.996	0.6475	0.87	0.66
97	2020-03-13	13:33:32	45	20.5	9.4	172	232	208	4	560	4	4.996	0.6628	0.86	0.65
98	2020-03-13	13:33:33	45	13.9	9.4	172	232	0	0	0	0	4.994	0.6571	0.87	0.66

99	2020-03-13	13:33:34	45	13.9	9.4	172	232	52	1	150	1	4.995	0.6257	0.88	0.67
100	2020-03-13	13:33:35	45	13.8	9.4	172	232	0	0	0	0	4.996	0.6166	0.93	0.81
101	2020-03-13	13:33:36	44	8.5	9.4	172	232	156	3	438	3	4.996	0.6129	0.94	0.81
102	2020-03-13	13:33:37	45	9.5	9.4	172	232	0	0	0	0	4.997	0.6127	0.93	0.81
103	2020-03-13	13:33:38	45	7.3	9.4	172	232	156	3	438	3	4.997	0.6031	0.87	0.67
104	2020-03-13	13:33:39	45	9.2	9.4	172	232	52	1	150	1	4.997	0.6078	0.87	0.66
105	2020-03-13	13:33:40	44	12.5	9.4	172	232	0	0	0	0	4.997	0.608	0.86	0.65
106	2020-03-13	13:33:41	45	6.8	9.4	172	232	208	4	552	4	4.997	0.6214	0.93	0.81
107	2020-03-13	13:33:42	44	8.1	9.4	172	232	52	1	150	1	4.995	0.6174	0.93	0.81
108	2020-03-13	13:33:43	46	13.1	9.4	172	232	0	0	0	0	4.997	0.6263	0.93	0.81
109	2020-03-13	13:33:44	45	15.8	9.4	172	232	128	2	264	2	4.997	0.6182	0.84	0.64
110	2020-03-13	13:33:45	46	13.1	9.4	172	232	208	4	576	4	4.995	0.6394	0.87	0.66
111	2020-03-13	13:33:46	45	9.7	9.4	172	232	0	0	0	0	4.995	0.6654	0.87	0.66
112	2020-03-13	13:33:47	46	14.9	9.4	172	232	156	3	426	3	4.996	0.6496	0.87	0.66
113	2020-03-13	13:33:48	45	8.1	9.4	172	233	52	1	150	1	4.997	0.6512	0.93	0.81
114	2020-03-13	13:33:49	46	11.3	9.4	172	232	652	13	1770	13	4.995	0.6298	0.87	0.66
115	2020-03-13	13:33:50	46	15.6	9.4	172	233	780	15	2114	15	4.997	0.6198	0.86	0.66
116	2020-03-13	13:33:51	45	16.5	9.4	172	232	364	7	986	7	4.996	0.6198	0.86	0.66
117	2020-03-13	13:33:52	45	18.4	9.4	172	232	0	0	0	0	4.994	0.6251	0.83	0.64
118	2020-03-13	13:33:53	46	16.6	9.4	172	232	416	8	1136	8	4.995	0.62	0.87	0.66
119	2020-03-13	13:33:54	45	16.0	9.4	172	232	676	13	1854	13	4.995	0.632	0.87	0.66
120	2020-03-13	13:33:55	46	11.9	9.4	172	232	52	1	150	1	4.995	0.6392	0.93	0.81
121	2020-03-13	13:33:56	47	17.2	9.4	172	233	0	0	0	0	4.996	0.6369	0.93	0.81
122	2020-03-13	13:33:57	46	19.1	10.2	172	232	0	0	0	0	4.997	0.6459	0.93	0.81
123	2020-03-13	13:33:58	46	17.5	9.7	172	232	832	16	2224	16	4.995	0.6481	0.87	0.66

124	2020-03-13	13:33:59	46	11.8	9.4	172	232	584	11	1680	12	4.995	0.6549	0.87	0.66
125	2020-03-13	13:34:00	46	7.4	9.4	172	232	52	1	150	1	4.995	0.6789	0.86	0.65
126	2020-03-13	13:34:01	45	7.6	9.4	172	232	0	0	0	0	4.995	0.6257	0.93	0.81
127	2020-03-13	13:34:02	46	19.6	10.1	172	232	208	4	568	4	4.997	0.6255	0.93	0.81
128	2020-03-13	13:34:03	46	7.3	9.7	172	232	520	10	1428	10	4.996	0.6335	0.93	0.81
129	2020-03-13	13:34:04	46	10.5	9.5	172	232	208	4	568	4	4.994	0.6353	0.86	0.65
130	2020-03-13	13:34:05	45	14.1	9.5	172	232	780	15	2114	15	4.997	0.6491	0.87	0.66
131	2020-03-13	13:34:06	46	7.4	9.5	172	232	104	2	292	2	4.997	0.6514	0.87	0.66
132	2020-03-13	13:34:07	46	12.0	9.5	172	232	52	1	150	1	4.998	0.6125	0.93	0.81
133	2020-03-13	13:34:08	46	15.4	9.5	172	232	0	0	0	0	4.998	0.631	0.94	0.82
134	2020-03-13	13:34:09	46	22.5	9.5	172	232	156	3	434	3	4.997	0.6265	0.93	0.81
135	2020-03-13	13:34:10	47	23.2	9.5	173	234	52	1	150	1	4.996	0.6326	0.87	0.66
136	2020-03-13	13:34:11	46	18.7	9.5	173	233	0	0	0	0	4.995	0.6322	0.84	0.64
137	2020-03-13	13:34:12	47	12.8	9.5	173	233	208	4	576	4	4.994	0.6322	0.85	0.66
138	2020-03-13	13:34:13	46	12.0	9.5	172	232	0	0	0	0	4.997	0.6284	0.86	0.66
139	2020-03-13	13:34:14	46	7.1	9.5	172	232	52	1	150	1	4.997	0.6204	0.86	0.65
140	2020-03-13	13:34:15	46	7.5	9.5	172	232	0	0	0	0	4.998	0.6328	0.84	0.63
141	2020-03-13	13:34:16	47	8.1	9.4	172	232	156	3	426	3	4.998	0.6206	0.92	0.8
142	2020-03-13	13:34:17	47	11.5	9.5	172	233	208	4	576	4	4.997	0.6306	0.86	0.66
143	2020-03-13	13:34:18	46	8.8	9.4	172	232	0	0	0	0	4.997	0.6255	0.87	0.66
144	2020-03-13	13:34:19	46	12.4	9.5	172	232	0	0	0	0	4.996	0.6394	0.87	0.66
145	2020-03-13	13:34:20	46	12.0	9.5	172	232	0	0	142	1	4.997	0.617	0.87	0.66
146	2020-03-13	13:34:21	47	8.4	9.4	172	232	104	2	142	1	4.998	0.6632	0.93	0.81
147	2020-03-13	13:34:22	48	17.5	9.4	172	232	0	0	0	0	4.997	0.6274	0.93	0.81
148	2020-03-13	13:34:23	47	14.7	9.4	172	232	116	2	142	1	4.998	0.6333	0.93	0.81

149	2020-03-13	13:34:24	47	10.8	9.4	172	232	0	0	0	0	4.995	0.6418	0.86	0.65
150	2020-03-13	13:34:25	47	11.8	9.4	172	232	52	1	142	1	4.995	0.6292	0.87	0.66
151	2020-03-13	13:34:26	47	12.6	9.5	172	232	0	0	0	0	4.998	0.6117	0.87	0.66
152	2020-03-13	13:34:27	47	13.2	9.4	172	232	0	0	0	0	4.997	0.6237	0.93	0.81
153	2020-03-13	13:34:28	48	10.8	9.4	172	232	52	1	142	1	4.997	0.6159	0.94	0.82
154	2020-03-13	13:34:29	47	8.0	9.4	172	232	0	0	0	0	4.997	0.6121	0.93	0.81
155	2020-03-13	13:34:30	47	7.1	9.4	172	232	52	1	142	1	4.997	0.6176	0.87	0.66
156	2020-03-13	13:34:31	47	9.5	9.5	172	232	52	1	142	1	4.997	0.5937	0.87	0.66
157	2020-03-13	13:34:32	47	10.2	9.4	172	232	0	0	0	0	4.998	0.6025	0.84	0.63
158	2020-03-13	13:34:33	46	13.7	9.4	172	233	0	0	142	1	4.995	0.6013	0.87	0.66
159	2020-03-13	13:34:34	47	10.4	9.4	172	232	116	2	142	1	4.994	0.6013	0.93	0.81
160	2020-03-13	13:34:35	47	14.8	9.4	172	232	0	0	0	0	4.995	0.6062	0.93	0.81
161	2020-03-13	13:34:36	48	20.2	10.7	172	232	52	1	142	1	4.996	0.6047	0.86	0.65
162	2020-03-13	13:34:37	46	12.8	10.2	172	232	0	0	0	0	4.997	0.6324	0.87	0.66
163	2020-03-13	13:34:38	46	9.0	9.8	172	232	52	1	142	1	4.997	0.6561	0.87	0.66
164	2020-03-13	13:34:39	46	7.3	9.4	172	232	0	0	0	0	4.994	0.6479	0.87	0.66
165	2020-03-13	13:34:40	46	7.6	9.4	172	232	52	1	142	1	4.995	0.6498	0.93	0.81
166	2020-03-13	13:34:41	47	7.3	9.4	172	232	0	0	0	0	4.995	0.64	0.93	0.81
167	2020-03-13	13:34:42	47	9.7	9.4	172	233	52	1	142	1	4.997	0.6284	0.93	0.81
168	2020-03-13	13:34:43	46	17.6	9.4	172	232	0	0	0	0	4.997	0.6243	0.87	0.66
169	2020-03-13	13:34:44	47	18.3	9.4	172	232	52	1	142	1	4.997	0.6424	0.87	0.66
170	2020-03-13	13:34:45	47	18.7	9.4	172	232	0	0	0	0	4.995	0.6302	0.87	0.66
171	2020-03-13	13:34:46	48	16.9	9.4	172	232	0	0	142	1	4.997	0.6253	0.87	0.66
172	2020-03-13	13:34:47	48	20.2	9.4	172	232	416	8	994	7	4.997	0.6257	0.93	0.81
173	2020-03-13	13:34:48	48	17.6	9.4	172	232	624	12	1704	12	4.996	0.6253	0.93	0.81

174	2020-03-13	13:34:49	47	14.6	9.4	172	232	728	14	1988	14	4.995	0.6402	0.93	0.81
175	2020-03-13	13:34:50	48	13.0	9.4	172	232	676	13	1846	13	4.995	0.6239	0.87	0.66
176	2020-03-13	13:34:51	48	15.9	9.4	172	232	728	14	1980	14	4.996	0.6078	0.87	0.66
177	2020-03-13	13:34:52	47	15.3	9.5	172	232	0	0	142	1	4.996	0.6225	0.86	0.65
178	2020-03-13	13:34:53	47	14.5	9.4	172	232	208	4	434	3	4.995	0.6186	0.87	0.66
179	2020-03-13	13:34:54	49	13.5	9.4	172	232	0	0	0	0	4.995	0.6164	0.86	0.65
180	2020-03-13	13:34:55	47	13.0	9.4	172	232	52	1	150	1	4.997	0.6164	0.93	0.81
181	2020-03-13	13:34:56	47	11.1	9.4	172	232	0	0	0	0	4.997	0.6121	0.86	0.65
182	2020-03-13	13:34:57	48	6.9	9.4	172	232	364	7	994	7	4.997	0.6304	0.87	0.66
183	2020-03-13	13:34:58	48	7.7	9.5	172	232	728	14	1988	14	4.997	0.6163	0.87	0.66
184	2020-03-13	13:34:59	48	10.7	9.5	172	232	468	9	1286	9	4.998	0.6027	0.86	0.65
185	2020-03-13	13:35:00	47	9.6	9.5	172	232	208	4	576	4	4.994	0.6024	0.86	0.65
186	2020-03-13	13:35:01	48	23.2	9.5	172	232	0	0	0	0	4.997	0.6024	0.93	0.81
187	2020-03-13	13:35:02	48	13.5	9.5	172	232	0	0	142	1	4.993	0.6161	0.86	0.66
188	2020-03-13	13:35:03	47	8.2	9.5	172	232	676	13	1846	13	4.995	0.6257	0.86	0.66
189	2020-03-13	13:35:04	48	13.9	9.7	172	232	364	7	860	6	4.995	0.6035	0.86	0.66
190	2020-03-13	13:35:05	47	12.9	9.5	172	232	0	0	0	0	4.996	0.6131	0.84	0.64
191	2020-03-13	13:35:06	48	8.0	9.5	172	232	416	8	1136	8	4.995	0.6074	0.86	0.65
192	2020-03-13	13:35:07	48	9.1	9.5	166	226	312	6	860	6	4.997	0.6074	0.93	0.81
193	2020-03-13	13:35:08	48	7.3	9.5	164	224	52	1	150	1	4.996	0.6251	0.86	0.65
194	2020-03-13	13:35:09	48	21.9	10.8	165	225	0	0	0	0	4.998	0.6017	0.85	0.65
195	2020-03-13	13:35:10	48	7.9	10.3	165	225	52	1	150	1	4.998	0.6066	0.85	0.64
196	2020-03-13	13:35:11	48	7.1	9.8	165	225	0	0	0	0	4.991	0.619	0.86	0.66
197	2020-03-13	13:35:13	49	7.1	9.5	163	223	52	1	150	1	4.995	0.6233	0.86	0.66
198	2020-03-13	13:35:14	48	15.1	9.5	164	224	0	0	0	0	4.995	0.6233	0.92	0.8

199	2020-03-13	13:35:15	48	16.0	9.5	164	224	312	6	852	6	4.996	0.6009	0.85	0.65
200	2020-03-13	13:35:16	48	8.1	9.5	164	225	1144	22	3232	24	4.995	0.6174	0.84	0.63
201	2020-03-13	13:35:17	49	16.2	9.5	164	223	884	17	2114	15	4.995	0.6219	0.87	0.66
202	2020-03-13	13:35:18	47	6.9	9.5	162	222	896	17	2098	15	4.995	0.6161	0.86	0.66
203	2020-03-13	13:35:19	47	8.4	9.5	162	222	780	15	2114	15	4.995	0.6492	0.85	0.65
204	2020-03-13	13:35:20	47	8.7	9.4	162	223	572	11	1570	11	4.998	0.6492	0.92	0.8
205	2020-03-13	13:35:21	47	8.5	9.5	162	223	52	1	150	1	4.997	0.62	0.85	0.65
206	2020-03-13	13:35:22	49	13.2	9.5	162	222	0	0	0	0	4.995	0.6056	0.86	0.65
207	2020-03-13	13:35:23	49	11.6	9.5	162	223	0	0	0	0	4.995	0.6068	0.87	0.66
208	2020-03-13	13:35:24	48	9.2	9.5	162	223	208	4	576	4	4.996	0.6143	0.86	0.65
209	2020-03-13	13:35:25	48	8.4	9.5	162	222	0	0	0	0	4.997	0.6375	0.82	0.63
210	2020-03-13	13:35:26	48	10.3	9.5	162	222	52	1	150	1	4.997	0.6375	0.86	0.66
211	2020-03-13	13:35:27	48	19.5	9.5	162	222	0	0	0	0	4.997	0.6298	0.85	0.65
212	2020-03-13	13:35:28	49	18.3	9.5	162	222	208	4	568	4	4.994	0.6086	0.86	0.65
213	2020-03-13	13:35:29	49	8.1	9.5	162	222	676	13	1846	13	4.994	0.6271	0.93	0.81
214	2020-03-13	13:35:30	48	7.0	9.5	162	222	728	14	1988	14	4.992	0.6337	0.83	0.62
215	2020-03-13	13:35:30	49	15.2	9.5	162	222	520	10	1428	10	4.998	0.6312	0.87	0.66
216	2020-03-13	13:35:31	48	8.6	9.5	162	222	104	2	284	2	4.997	0.6312	0.87	0.66
217	2020-03-13	13:35:32	49	7.3	9.5	162	222	52	1	150	1	4.991	0.6025	0.86	0.65
218	2020-03-13	13:35:33	48	14.2	9.5	162	222	0	0	0	0	4.996	0.6005	0.82	0.62
219	2020-03-13	13:35:35	48	7.2	9.5	162	222	260	5	576	4	4.996	0.6062	0.92	0.8
220	2020-03-13	13:35:36	48	9.0	9.5	162	222	0	0	0	0	4.996	0.6375	0.86	0.66
221	2020-03-13	13:35:37	49	8.4	9.5	162	222	0	0	300	2	4.998	0.6206	0.85	0.65
222	2020-03-13	13:35:37	48	8.2	9.5	163	223	116	2	0	0	4.997	0.6206	0.85	0.66
223	2020-03-13	13:35:38	48	10.9	9.5	163	223	260	5	576	4	4.995	0.6135	0.82	0.63

224	2020-03-13	13:35:39	48	16.6	9.5	163	223	0	0	0	0	4.995	0.6284	0.87	0.66
225	2020-03-13	13:35:40	48	14.4	9.5	163	223	52	1	142	1	4.995	0.618	0.93	0.81
226	2020-03-13	13:35:41	48	7.8	9.5	163	223	104	2	292	2	4.997	0.6447	0.86	0.66
227	2020-03-13	13:35:42	48	15.2	10.8	163	223	0	0	0	0	4.997	0.6088	0.84	0.64
228	2020-03-13	13:35:43	48	8.8	10.4	163	223	104	2	292	2	4.997	0.6088	0.83	0.64
229	2020-03-13	13:35:44	48	7.6	9.9	163	223	156	3	434	3	4.992	0.6092	0.85	0.65
230	2020-03-13	13:35:45	48	7.8	9.5	163	223	0	0	0	0	4.995	0.6363	0.86	0.65
231	2020-03-13	13:35:46	49	8.0	9.5	162	222	52	1	142	1	4.995	0.6366	0.93	0.81
232	2020-03-13	13:35:47	49	11.9	9.5	162	222	156	3	434	3	4.995	0.6534	0.85	0.64
233	2020-03-13	13:35:48	50	10.8	9.5	162	223	0	0	0	0	4.998	0.6206	0.86	0.65
234	2020-03-13	13:35:49	49	7.5	9.5	162	222	480	9	1278	9	4.997	0.6206	0.86	0.65
235	2020-03-13	13:35:50	48	17.1	9.5	162	222	1352	26	3374	25	4.996	0.6166	0.86	0.65
236	2020-03-13	13:35:51	49	12.1	9.5	163	223	780	15	2114	15	4.996	0.6092	0.84	0.64
237	2020-03-13	13:35:52	50	12.8	9.5	163	223	780	15	2130	15	4.996	0.6363	0.93	0.81
238	2020-03-13	13:35:53	49	12.4	9.5	163	223	624	12	1960	14	4.997	0.6318	0.92	0.79
239	2020-03-13	13:35:54	49	15.9	9.5	163	223	856	16	1988	14	4.996	0.6492	0.93	0.81
240	2020-03-13	13:35:55	49	9.7	9.5	162	222	260	5	718	5	4.996	0.6398	0.87	0.66
241	2020-03-13	13:35:56	50	11.5	9.5	162	222	52	1	150	1	4.994	0.6369	0.83	0.63
242	2020-03-13	13:35:57	49	13.1	9.5	162	222	0	0	0	0	4.998	0.6261	0.86	0.65
243	2020-03-13	13:35:58	49	6.9	9.5	162	222	236	5	642	5	4.998	0.6661	0.86	0.65
244	2020-03-13	13:35:59	48	11.2	9.5	163	223	0	0	0	0	4.997	0.6286	0.93	0.81
245	2020-03-13	13:36:00	48	9.5	9.5	163	224	52	1	150	1	4.997	0.6218	0.92	0.8
246	2020-03-13	13:36:01	49	7.7	9.5	163	224	0	0	0	0	4.997	0.6263	0.92	0.8
247	2020-03-13	13:36:02	48	7.9	9.5	163	223	156	3	426	3	4.997	0.6174	0.85	0.65
248	2020-03-13	13:36:03	50	10.7	9.5	164	224	792	15	1988	14	4.997	0.6206	0.84	0.64

249	2020-03-13	13:36:04	49	22.0	9.5	164	224	520	10	1428	10	4.996	0.6174	0.84	0.63
250	2020-03-13	13:36:05	50	23.3	9.5	164	224	52	1	150	1	4.995	0.6271	0.92	0.8
251	2020-03-13	13:36:06	50	22.0	9.5	164	224	0	0	0	0	4.995	0.6308	0.92	0.79
252	2020-03-13	13:36:07	50	16.8	9.5	164	224	0	0	142	1	4.995	0.6383	0.92	0.8
253	2020-03-13	13:36:08	51	18.1	9.5	164	224	208	4	434	3	4.995	0.6247	0.85	0.64
254	2020-03-13	13:36:09	50	17.5	9.5	164	224	0	0	0	0	4.994	0.625	0.86	0.65
255	2020-03-13	13:36:10	51	18.8	10.1	164	225	52	1	150	1	4.995	0.625	0.86	0.65
256	2020-03-13	13:36:11	50	15.6	9.7	165	225	428	8	1136	8	4.996	0.6184	0.85	0.65
257	2020-03-13	13:36:12	50	13.9	9.5	165	225	572	11	1570	11	4.995	0.6581	0.86	0.65
258	2020-03-13	13:36:13	50	14.5	9.5	165	225	52	1	142	1	4.995	0.6379	0.93	0.81
259	2020-03-13	13:36:14	50	13.2	9.5	165	225	156	3	434	3	4.997	0.6341	0.86	0.65
260	2020-03-13	13:36:15	50	12.5	9.7	165	225	0	0	0	0	4.997	0.62	0.86	0.65
261	2020-03-13	13:36:16	49	14.0	10.1	165	225	52	1	150	1	4.996	0.62	0.86	0.65
262	2020-03-13	13:36:17	49	15.8	9.6	165	226	0	0	0	0	4.994	0.6174	0.86	0.65
263	2020-03-13	13:36:18	50	13.5	9.5	166	226	156	3	426	3	4.994	0.629	0.85	0.66
264	2020-03-13	13:36:19	50	10.6	9.5	166	226	52	1	150	1	4.994	0.651	0.92	0.8
265	2020-03-13	13:36:20	50	11.5	9.5	166	226	0	0	0	0	4.994	0.64	0.85	0.66
266	2020-03-13	13:36:21	49	17.3	9.5	166	226	676	13	1846	13	4.997	0.6115	0.8	0.61
267	2020-03-13	13:36:22	51	17.3	9.5	166	226	104	2	292	2	4.995	0.6115	0.85	0.66
268	2020-03-13	13:36:23	49	15.2	9.5	166	226	52	1	150	1	4.995	0.6231	0.86	0.66
269	2020-03-13	13:36:24	50	14.2	9.5	166	226	0	0	0	0	4.997	0.6206	0.84	0.63
270	2020-03-13	13:36:25	51	13.2	9.5	166	226	520	10	1428	10	4.997	0.6379	0.92	0.8
271	2020-03-13	13:36:26	50	12.3	9.5	166	226	52	1	150	1	4.997	0.6284	0.85	0.65
272	2020-03-13	13:36:27	49	8.1	9.5	166	226	0	0	0	0	4.998	0.6121	0.85	0.65
273	2020-03-13	13:36:28	50	7.6	9.5	166	226	0	0	0	0	4.995	0.6121	0.86	0.66

274	2020-03-13	13:36:29	50	8.7	9.5	166	226	208	4	576	4	4.995	0.6068	0.84	0.64
275	2020-03-13	13:36:30	50	12.8	9.5	166	226	0	0	0	0	4.998	0.6033	0.82	0.63
276	2020-03-13	13:36:31	50	25.1	9.5	166	226	52	1	150	1	4.998	0.6502	0.92	0.8
277	2020-03-13	13:36:32	50	10.2	9.5	167	227	52	1	150	1	4.997	0.6432	0.86	0.66
278	2020-03-13	13:36:33	50	8.8	9.5	167	227	0	0	0	0	4.994	0.6127	0.85	0.65
279	2020-03-13	13:36:34	50	7.4	9.5	167	227	0	0	0	0	4.996	0.6127	0.85	0.65
280	2020-03-13	13:36:35	50	7.7	9.5	166	226	208	4	576	4	4.998	0.6023	0.81	0.62
281	2020-03-13	13:36:36	50	17.4	9.5	166	226	0	0	0	0	4.998	0.6331	0.85	0.65
282	2020-03-13	13:36:37	50	18.0	9.5	166	226	52	1	150	1	4.998	0.6333	0.91	0.79
283	2020-03-13	13:36:38	51	17.1	9.5	166	226	104	2	284	2	4.995	0.6273	0.84	0.64
284	2020-03-13	13:36:39	51	16.0	9.5	166	226	104	2	292	2	4.994	0.6237	0.83	0.63
285	2020-03-13	13:36:40	50	14.2	9.5	166	226	0	0	0	0	4.995	0.6237	0.91	0.8
286	2020-03-13	13:36:41	50	15.0	9.5	166	226	52	1	150	1	4.996	0.6178	0.84	0.63
287	2020-03-13	13:36:42	51	15.1	9.5	166	226	520	10	1420	10	4.996	0.6149	0.84	0.64
288	2020-03-13	13:36:43	51	21.2	9.5	166	227	728	14	1988	14	4.996	0.6192	0.83	0.64
289	2020-03-13	13:36:44	51	19.4	9.8	166	226	260	5	718	5	4.995	0.6261	0.91	0.79
290	2020-03-13	13:36:45	50	13.2	9.5	166	226	0	0	0	0	4.995	0.6337	0.91	0.79
291	2020-03-13	13:36:46	51	7.1	9.5	167	227	364	7	1136	8	4.995	0.6255	0.91	0.79
292	2020-03-13	13:36:47	50	7.1	9.5	167	227	468	9	1144	8	4.996	0.6164	0.83	0.63
293	2020-03-13	13:36:48	50	8.4	9.5	167	227	52	1	150	1	4.997	0.6265	0.84	0.63
294	2020-03-13	13:36:49	50	7.7	9.5	167	227	0	0	0	0	4.997	0.6312	0.85	0.66
295	2020-03-13	13:36:50	50	12.2	10.5	167	227	260	5	852	6	4.997	0.6328	0.82	0.62
296	2020-03-13	13:36:51	51	9.2	10.0	167	227	728	14	1988	14	4.995	0.6278	0.91	0.79
297	2020-03-13	13:36:53	49	4.6	9.5	167	227	468	9	1144	8	4.995	0.6416	0.91	0.79
298	2020-03-13	13:36:54	50	9.0	9.5	167	228	52	1	150	1	4.995	0.6415	0.82	0.62

299	2020-03-13	13:36:55	50	11.4	9.5	167	227	0	0	0	0	4.997	0.6241	0.8	0.61
300	2020-03-13	13:36:56	51	13.8	9.5	167	227	208	4	710	5	4.997	0.6244	0.84	0.66
301	2020-03-13	13:36:57	51	18.7	9.5	167	227	780	15	1972	14	4.997	0.6229	0.91	0.79
302	2020-03-13	13:36:58	51	15.1	9.5	167	227	52	1	150	1	4.995	0.6172	0.83	0.63
303	2020-03-13	13:36:59	50	13.1	9.5	167	228	0	0	0	0	4.994	0.6151	0.82	0.62
304	2020-03-13	13:37:00	50	9.6	9.5	167	228	624	12	1846	13	4.995	0.6151	0.8	0.61
305	2020-03-13	13:37:01	50	8.9	9.5	167	228	780	15	1996	14	4.996	0.6084	0.83	0.63
306	2020-03-13	13:37:02	50	7.7	9.5	167	227	0	0	0	0	4.994	0.6302	0.83	0.63
307	2020-03-13	13:37:03	51	12.7	9.5	167	227	52	1	150	1	4.994	0.6003	0.91	0.79
308	2020-03-13	13:37:04	51	13.7	9.5	167	227	0	0	0	0	4.996	0.609	0.81	0.61
309	2020-03-13	13:37:05	50	6.4	9.5	167	228	780	15	1988	14	4.992	0.6035	0.88	0.68
310	2020-03-13	13:37:06	50	7.7	9.5	167	227	532	10	1570	11	4.997	0.6035	0.94	0.82
311	2020-03-13	13:37:07	49	14.0	9.5	167	228	208	4	576	4	4.997	0.6125	0.86	0.65
312	2020-03-13	13:37:08	51	13.6	9.5	167	227	0	0	0	0	4.997	0.6198	0.84	0.63
313	2020-03-13	13:37:09	50	13.5	9.5	167	227	0	0	0	0	4.997	0.6094	0.84	0.64
314	2020-03-13	13:37:10	51	23.9	9.5	167	227	676	13	1846	13	4.994	0.6261	0.93	0.81
315	2020-03-13	13:37:11	52	7.7	9.5	167	227	520	10	1396	10	4.994	0.6561	0.87	0.66
316	2020-03-13	13:37:12	51	7.1	9.5	167	227	0	0	0	0	4.997	0.6125	0.84	0.64
317	2020-03-13	13:37:13	51	10.4	9.5	167	227	260	5	710	5	4.998	0.6125	0.85	0.64
318	2020-03-13	13:37:14	51	9.2	9.5	167	228	792	15	2256	16	4.997	0.6349	0.86	0.67
319	2020-03-13	13:37:15	51	15.8	9.5	167	227	416	8	970	7	4.997	0.6345	0.83	0.62
320	2020-03-13	13:37:16	51	7.9	9.5	167	227	168	3	402	3	4.994	0.6377	0.82	0.62
321	2020-03-13	13:37:17	51	11.2	9.8	167	228	0	0	0	0	4.997	0.64	0.92	0.8
322	2020-03-13	13:37:18	51	13.7	9.5	168	228	364	7	1136	8	4.996	0.6459	0.91	0.79
323	2020-03-13	13:37:19	51	8.4	9.5	168	229	688	13	1988	14	4.994	0.6685	0.92	0.8

324	2020-03-13	13:37:20	50	7.7	9.5	168	228	532	10	1248	8	4.998	0.621	0.83	0.63
325	2020-03-13	13:37:21	50	17.7	9.5	168	228	0	0	142	1	4.997	0.6253	0.82	0.61
326	2020-03-13	13:37:22	51	15.7	9.5	168	229	156	3	292	2	4.995	0.6225	0.84	0.63
327	2020-03-13	13:37:23	51	18.8	10.6	168	228	0	0	0	0	4.996	0.6461	0.92	0.8
328	2020-03-13	13:37:24	52	16.6	10.2	168	228	312	6	860	6	4.995	0.6477	0.92	0.8
329	2020-03-13	13:37:25	51	9.2	9.7	168	228	0	0	0	0	4.993	0.6255	0.93	0.81
330	2020-03-13	13:37:26	51	9.7	9.5	168	228	208	4	710	5	4.995	0.628	0.85	0.64
331	2020-03-13	13:37:27	51	8.4	9.5	168	229	728	14	1846	13	4.997	0.6174	0.84	0.63
332	2020-03-13	13:37:28	50	11.1	9.5	168	228	728	14	1988	14	4.997	0.6125	0.82	0.62
333	2020-03-13	13:37:29	50	7.3	9.5	168	228	728	14	1964	14	4.996	0.6263	0.78	0.59
334	2020-03-13	13:37:30	51	12.9	9.5	168	228	52	1	150	1	4.996	0.6121	0.92	0.81
335	2020-03-13	13:37:31	51	12.6	9.5	168	229	52	1	150	1	4.995	0.6072	0.92	0.8
336	2020-03-13	13:37:32	51	8.3	9.5	168	228	0	0	0	0	4.992	0.597	0.91	0.79

Run-3-Log															
	Date	T.Stamp	Temp	CPU_Load	Mem_Load	ProNo,	ThreadsNo	RX_bit	RX_pkt	TX_bit	TX_pkt	Voltage(V)	Current(A)	D+(V)	D-(V)
1	2020-03-13	13:54:53	43	13.0	9.3	172	232	728	14	1988	14	4.992	0.6129	0.92	0.8
2	2020-03-13	13:54:54	44	13.8	9.4	172	233	676	13	1846	13	4.994	0.6117	0.83	0.62
3	2020-03-13	13:54:55	44	18.1	9.4	172	232	780	15	1988	14	4.994	0.6147	0.81	0.61
4	2020-03-13	13:54:56	44	17.6	9.4	172	232	844	16	2130	15	4.993	0.6125	0.83	0.62
5	2020-03-13	13:54:57	44	11.3	9.4	172	232	676	13	1854	13	4.992	0.6192	0.92	0.8
6	2020-03-13	13:54:58	44	16.1	9.3	172	232	0	0	150	1	4.992	0.6267	0.92	0.8
7	2020-03-13	13:54:59	44	18.6	9.3	172	232	52	1	0	0	4.993	0.6119	0.8	0.6
8	2020-03-13	13:55:00	44	17.8	9.4	172	232	0	0	0	0	4.994	0.6225	0.82	0.62
9	2020-03-13	13:55:01	44	14.5	9.4	172	232	260	5	702	5	4.994	0.6492	0.82	0.62
10	2020-03-13	13:55:02	44	14.2	9.4	172	232	0	0	0	0	4.995	0.6155	0.82	0.62
11	2020-03-13	13:55:03	45	12.8	9.4	172	232	232	4	402	3	4.994	0.6135	0.81	0.61
12	2020-03-13	13:55:04	43	10.2	9.4	172	232	0	0	0	0	4.994	0.6135	0.85	0.67
13	2020-03-13	13:55:05	44	8.7	9.4	172	232	416	8	1136	8	4.995	0.6094	0.82	0.62
14	2020-03-13	13:55:06	45	12.6	9.4	172	232	728	14	1988	14	4.995	0.6235	0.82	0.63
15	2020-03-13	13:55:07	44	16.7	9.4	172	232	624	12	1696	12	4.995	0.63	0.82	0.62
16	2020-03-13	13:55:08	44	20.4	9.4	172	232	52	1	150	1	4.995	0.6163	0.79	0.6
17	2020-03-13	13:55:09	45	20.8	9.4	172	232	0	0	0	0	4.993	0.6331	0.81	0.61
18	2020-03-13	13:55:10	45	16.2	9.4	172	232	104	2	284	2	4.992	0.6331	0.9	0.78
19	2020-03-13	13:55:11	45	14.9	9.4	172	232	676	13	1838	13	4.994	0.6233	0.82	0.62
20	2020-03-13	13:55:12	44	12.5	9.4	172	232	0	0	0	0	4.995	0.6312	0.81	0.62
21	2020-03-13	13:55:13	44	13.6	10.0	172	232	104	2	292	2	4.995	0.6255	0.79	0.61
22	2020-03-13	13:55:15	45	5.8	9.4	172	232	0	0	0	0	4.996	0.6473	0.83	0.62
23	2020-03-13	13:55:16	45	9.0	9.4	172	232	260	5	702	5	4.994	0.6176	0.91	0.8

24	2020-03-13	13:55:17	46	8.3	9.4	172	232	0	0	0	0	4.997	0.61	0.92	0.8
25	2020-03-13	13:55:18	45	23.4	10.3	172	232	0	0	0	0	4.995	0.6099	0.92	0.8
26	2020-03-13	13:55:19	45	7.8	9.9	172	232	52	1	150	1	4.995	0.6084	0.92	0.8
27	2020-03-13	13:55:20	46	11.7	9.4	172	232	0	0	0	0	4.993	0.6655	0.82	0.62
28	2020-03-13	13:55:21	45	13.6	9.4	172	232	52	1	150	1	4.993	0.6365	0.82	0.62
29	2020-03-13	13:55:22	46	23.4	9.4	172	232	156	3	434	3	4.993	0.6432	0.83	0.63
30	2020-03-13	13:55:23	45	8.4	9.4	172	232	0	0	0	0	4.994	0.6498	0.91	0.8
31	2020-03-13	13:55:24	46	12.9	9.4	172	232	52	1	150	1	4.99	0.6249	0.92	0.8
32	2020-03-13	13:55:25	46	12.6	9.4	172	232	0	0	0	0	4.996	0.6273	0.92	0.8
33	2020-03-13	13:55:26	45	7.9	9.4	172	232	208	4	576	4	4.995	0.6555	0.83	0.62
34	2020-03-13	13:55:27	45	13.9	9.4	172	232	0	0	0	0	4.995	0.618	0.83	0.62
35	2020-03-13	13:55:28	45	18.2	9.4	172	232	156	3	426	3	4.995	0.6292	0.82	0.61
36	2020-03-13	13:55:29	46	18.2	9.4	172	232	832	16	2098	15	4.993	0.6282	0.82	0.62
37	2020-03-13	13:55:30	45	15.9	9.4	172	232	740	14	2130	15	4.994	0.619	0.83	0.63
38	2020-03-13	13:55:31	46	13.1	9.4	172	232	728	14	1988	14	4.992	0.619	0.92	0.8
39	2020-03-13	13:55:32	46	12.1	9.4	172	232	156	3	434	3	4.993	0.6168	0.92	0.8
40	2020-03-13	13:55:33	46	14.8	9.4	172	233	52	1	150	1	4.994	0.611	0.83	0.62
41	2020-03-13	13:55:34	46	15.2	9.4	173	234	0	0	0	0	4.994	0.6074	0.83	0.62
42	2020-03-13	13:55:35	46	12.8	9.4	173	233	52	1	150	1	4.993	0.6186	0.83	0.62
43	2020-03-13	13:55:36	46	8.9	9.4	173	234	104	2	268	2	4.993	0.6202	0.92	0.8
44	2020-03-13	13:55:37	46	6.9	9.4	172	233	728	14	1972	14	4.994	0.6121	0.92	0.8
45	2020-03-13	13:55:38	46	17.6	9.4	172	232	740	14	1988	14	4.994	0.6021	0.92	0.8
46	2020-03-13	13:55:39	45	8.8	9.4	172	232	580	10	2532	16	4.995	0.602	0.83	0.62
47	2020-03-13	13:55:40	46	7.7	9.4	172	232	168	3	344	2	4.996	0.6367	0.81	0.61
48	2020-03-13	13:55:41	46	12.5	9.4	172	232	208	4	576	4	4.996	0.5939	0.83	0.62

49	2020-03-13	13:55:42	46	7.9	9.4	172	232	0	0	0	0	4.996	0.5943	0.9	0.78
50	2020-03-13	13:55:43	47	7.1	9.4	172	232	52	1	284	2	4.996	0.6117	0.9	0.78
51	2020-03-13	13:55:44	45	15.4	9.4	172	232	156	3	292	2	4.996	0.6005	0.92	0.8
52	2020-03-13	13:55:45	47	17.0	9.4	172	232	0	0	0	0	4.994	0.5958	0.92	0.8
53	2020-03-13	13:55:46	47	23.6	9.4	172	233	52	1	150	1	4.995	0.6131	0.83	0.62
54	2020-03-13	13:55:47	46	23.1	9.4	172	232	0	0	0	0	4.994	0.6437	0.82	0.62
55	2020-03-13	13:55:48	46	22.1	9.4	172	232	520	10	1420	10	4.994	0.6441	0.82	0.62
56	2020-03-13	13:55:49	46	13.3	9.4	172	232	780	15	1996	14	4.993	0.6314	0.83	0.62
57	2020-03-13	13:55:50	46	15.6	9.4	172	232	0	0	0	0	4.994	0.617	0.82	0.62
58	2020-03-13	13:55:51	47	8.6	9.4	172	233	676	13	1846	13	4.996	0.617	0.91	0.79
59	2020-03-13	13:55:52	48	12.8	10.5	172	232	1352	26	3516	26	4.997	0.607	0.82	0.62
60	2020-03-13	13:55:53	47	10.4	10.1	172	232	636	12	1554	11	4.992	0.6267	0.79	0.59
61	2020-03-13	13:55:55	46	5.7	9.4	172	232	0	0	142	1	4.995	0.61	0.82	0.62
62	2020-03-13	13:55:56	46	8.4	9.4	172	232	156	3	292	2	4.997	0.6135	0.82	0.62
63	2020-03-13	13:55:57	46	7.7	9.4	172	232	0	0	0	0	4.997	0.6135	0.91	0.79
64	2020-03-13	13:55:58	47	10.6	9.4	172	232	52	1	150	1	4.994	0.5996	0.82	0.62
65	2020-03-13	13:55:59	47	18.2	9.4	172	232	0	0	0	0	4.994	0.6125	0.82	0.62
66	2020-03-13	13:56:00	47	22.4	9.4	172	232	208	4	576	4	4.994	0.6178	0.82	0.62
67	2020-03-13	13:56:01	48	18.9	9.4	172	232	0	0	0	0	4.994	0.6341	0.8	0.6
68	2020-03-13	13:56:02	47	17.3	9.4	172	232	0	0	0	0	4.994	0.6441	0.91	0.79
69	2020-03-13	13:56:03	47	18.3	9.4	172	232	832	16	2192	16	4.995	0.6239	0.91	0.79
70	2020-03-13	13:56:04	47	14.5	9.4	172	232	520	10	1428	10	4.995	0.63	0.91	0.79
71	2020-03-13	13:56:05	47	13.8	9.4	172	232	52	1	150	1	4.995	0.6398	0.91	0.79
72	2020-03-13	13:56:06	47	21.8	9.4	172	232	0	0	0	0	4.995	0.6379	0.79	0.61
73	2020-03-13	13:56:07	47	11.6	9.4	172	233	0	0	0	0	4.996	0.6351	0.81	0.61

74	2020-03-13	13:56:08	47	10.8	9.4	172	232	208	4	576	4	4.993	0.6284	0.82	0.62
75	2020-03-13	13:56:09	48	12.4	9.4	172	232	0	0	0	0	4.996	0.6221	0.91	0.78
76	2020-03-13	13:56:10	47	11.6	9.4	172	232	52	1	150	1	4.996	0.6202	0.89	0.74
77	2020-03-13	13:56:11	48	8.8	9.4	172	232	0	0	0	0	4.997	0.6546	0.91	0.78
78	2020-03-13	13:56:12	48	17.4	9.4	172	232	312	6	844	6	4.996	0.6166	0.82	0.62
79	2020-03-13	13:56:13	47	14.3	9.4	172	232	52	1	150	1	4.996	0.6227	0.82	0.63
80	2020-03-13	13:56:14	48	10.2	9.4	172	232	0	0	0	0	4.994	0.6251	0.82	0.62
81	2020-03-13	13:56:15	47	17.6	9.4	172	232	0	0	142	1	4.995	0.6145	0.9	0.78
82	2020-03-13	13:56:16	47	16.8	9.4	172	232	1196	23	3000	22	4.996	0.6208	0.83	0.63
83	2020-03-13	13:56:17	48	16.8	9.4	172	232	1404	27	3484	26	4.994	0.6196	0.81	0.62
84	2020-03-13	13:56:18	48	14.7	9.4	172	232	676	13	1972	14	4.994	0.6196	0.91	0.79
85	2020-03-13	13:56:19	48	14.9	9.4	172	232	1040	20	2602	19	4.994	0.6237	0.83	0.63
86	2020-03-13	13:56:20	48	14.5	9.5	172	232	1364	26	3626	27	4.994	0.6139	0.83	0.62
87	2020-03-13	13:56:21	49	16.0	9.8	172	232	416	8	860	6	4.995	0.6135	0.83	0.62
88	2020-03-13	13:56:22	49	15.3	9.5	172	232	52	1	150	1	4.995	0.6135	0.91	0.79
89	2020-03-13	13:56:23	47	13.1	9.4	172	232	0	0	0	0	4.994	0.6392	0.9	0.78
90	2020-03-13	13:56:24	48	9.0	9.5	172	232	208	4	576	4	4.995	0.6359	0.83	0.63
91	2020-03-13	13:56:25	48	14.1	9.5	172	233	0	0	0	0	4.997	0.6159	0.83	0.62
92	2020-03-13	13:56:26	49	24.4	10.3	172	232	52	1	150	1	4.997	0.6231	0.83	0.62
93	2020-03-13	13:56:27	48	15.8	10.0	172	232	0	0	0	0	4.995	0.6265	0.83	0.63
94	2020-03-13	13:56:28	48	12.5	9.6	172	232	156	3	426	3	4.994	0.6496	0.83	0.62
95	2020-03-13	13:56:29	49	5.8	9.5	172	233	676	13	1846	13	4.995	0.6375	0.92	0.8
96	2020-03-13	13:56:30	48	6.5	9.5	172	232	728	14	1988	14	4.997	0.6451	0.92	0.8
97	2020-03-13	13:56:31	47	8.7	9.4	172	232	728	14	1988	14	4.997	0.5937	0.92	0.8
98	2020-03-13	13:56:32	48	11.4	9.5	172	232	104	2	292	2	4.997	0.5988	0.83	0.62

99	2020-03-13	13:56:33	47	11.5	9.5	172	232	0	0	0	0	4.996	0.5985	0.8	0.6
100	2020-03-13	13:56:34	49	8.6	9.5	172	233	52	1	150	1	4.997	0.6176	0.82	0.62
101	2020-03-13	13:56:35	48	9.2	9.5	172	233	260	5	702	5	4.997	0.6457	0.91	0.79
102	2020-03-13	13:56:36	47	7.1	9.4	172	233	76	1	114	1	4.997	0.6229	0.81	0.61
103	2020-03-13	13:56:37	49	23.6	9.4	172	232	52	1	150	1	4.997	0.6051	0.81	0.62
104	2020-03-13	13:56:38	49	12.9	9.4	172	232	0	0	0	0	4.994	0.6051	0.81	0.61
105	2020-03-13	13:56:39	49	12.5	9.4	172	232	52	1	142	1	4.996	0.6496	0.82	0.62
106	2020-03-13	13:56:40	48	8.0	9.4	172	233	52	1	150	1	4.995	0.6066	0.82	0.63
107	2020-03-13	13:56:41	49	17.5	9.4	172	232	28	1	66	1	4.997	0.6353	0.81	0.62
108	2020-03-13	13:56:42	48	7.7	9.4	172	232	596	11	1704	12	4.997	0.6249	0.91	0.79
109	2020-03-13	13:56:43	49	11.4	9.5	172	232	596	11	2040	14	4.994	0.6135	0.9	0.79
110	2020-03-13	13:56:44	48	12.1	9.4	172	233	832	16	2130	15	4.997	0.6104	0.92	0.8
111	2020-03-13	13:56:45	49	7.5	9.5	172	232	260	5	718	5	4.997	0.6467	0.83	0.62
112	2020-03-13	13:56:46	49	9.0	9.4	172	232	468	9	1278	9	4.997	0.6202	0.81	0.61
113	2020-03-13	13:56:47	49	8.1	9.4	172	232	896	17	2398	17	4.997	0.6096	0.83	0.62
114	2020-03-13	13:56:48	49	7.9	9.5	172	233	468	9	1270	9	4.996	0.6045	0.92	0.8
115	2020-03-13	13:56:49	48	7.8	9.5	172	233	260	5	710	5	4.997	0.611	0.92	0.8
116	2020-03-13	13:56:50	48	12.7	9.5	172	232	728	14	1988	14	4.997	0.6096	0.92	0.8
117	2020-03-13	13:56:51	49	19.9	9.5	173	233	780	15	2130	15	4.997	0.6163	0.82	0.61
118	2020-03-13	13:56:52	48	12.9	9.5	173	233	728	14	2130	15	4.995	0.6604	0.8	0.6
119	2020-03-13	13:56:53	50	17.2	9.5	173	233	208	4	576	4	4.996	0.6125	0.82	0.62
120	2020-03-13	13:56:54	49	7.2	9.5	173	233	416	8	1278	9	4.995	0.5996	0.8	0.61
121	2020-03-13	13:56:55	49	10.4	9.6	172	232	728	14	1846	13	4.993	0.6033	0.9	0.79
122	2020-03-13	13:56:56	48	8.0	9.5	172	232	104	2	426	3	4.996	0.6316	0.91	0.79
123	2020-03-13	13:56:57	48	7.5	9.5	172	232	416	8	1002	7	4.993	0.6506	0.91	0.79

124	2020-03-13	13:56:58	48	7.1	9.5	172	232	0	0	0	0	4.994	0.6139	0.77	0.59
125	2020-03-13	13:56:59	49	8.4	9.4	172	232	168	3	292	2	4.994	0.6123	0.82	0.62
126	2020-03-13	13:57:00	48	16.2	10.2	172	232	0	0	0	0	4.996	0.6123	0.82	0.62
127	2020-03-13	13:57:01	49	15.6	9.8	172	232	208	4	576	4	4.994	0.6098	0.81	0.62
128	2020-03-13	13:57:02	49	12.2	9.4	172	232	0	0	0	0	4.995	0.6467	0.8	0.61
129	2020-03-13	13:57:03	48	17.6	9.5	172	232	312	6	844	6	4.995	0.6302	0.91	0.79
130	2020-03-13	13:57:04	50	22.4	9.5	172	232	0	0	284	2	4.996	0.6253	0.82	0.63
131	2020-03-13	13:57:05	50	22.3	9.5	172	232	104	2	292	2	4.996	0.6257	0.83	0.62
132	2020-03-13	13:57:06	49	17.9	9.5	172	232	0	0	0	0	4.994	0.6298	0.82	0.62
133	2020-03-13	13:57:07	49	18.4	9.4	172	232	52	1	150	1	4.994	0.6231	0.83	0.62
134	2020-03-13	13:57:08	49	14.2	9.4	172	232	0	0	0	0	4.993	0.6235	0.92	0.8
135	2020-03-13	13:57:09	50	12.3	9.4	172	232	520	10	1420	10	4.994	0.6186	0.92	0.8
136	2020-03-13	13:57:10	49	11.9	9.5	172	232	728	14	1988	14	4.994	0.6145	0.92	0.8
137	2020-03-13	13:57:11	49	7.5	9.5	172	232	728	14	1988	14	4.994	0.618	0.83	0.62
138	2020-03-13	13:57:12	48	8.1	9.5	172	232	260	5	702	5	4.994	0.607	0.83	0.62
139	2020-03-13	13:57:13	50	16.0	9.5	172	232	156	3	434	3	4.995	0.6003	0.83	0.62
140	2020-03-13	13:57:14	49	14.7	9.5	172	232	0	0	0	0	4.994	0.6163	0.92	0.8
141	2020-03-13	13:57:15	49	13.7	9.5	172	232	52	1	150	1	4.995	0.6131	0.92	0.8
142	2020-03-13	13:57:16	49	19.9	9.5	172	233	156	3	560	4	4.994	0.6145	0.92	0.8
143	2020-03-13	13:57:17	50	18.9	9.5	172	232	156	3	426	3	4.994	0.6278	0.83	0.63
144	2020-03-13	13:57:18	50	16.5	9.5	172	233	52	1	150	1	4.994	0.6278	0.8	0.6
145	2020-03-13	13:57:19	49	8.6	9.5	172	232	0	0	0	0	4.996	0.6218	0.82	0.62
146	2020-03-13	13:57:20	50	16.4	9.5	172	232	52	1	150	1	4.997	0.6218	0.82	0.62
147	2020-03-13	13:57:21	50	8.6	9.4	172	232	624	12	1704	12	4.995	0.6304	0.81	0.61
148	2020-03-13	13:57:22	50	8.5	9.4	172	232	780	15	2130	15	4.997	0.6053	0.81	0.61

149	2020-03-13	13:57:23	50	7.4	9.4	172	232	156	3	434	3	4.997	0.6041	0.92	0.8
150	2020-03-13	13:57:24	50	15.5	9.5	172	233	208	4	576	4	4.995	0.606	0.82	0.63
151	2020-03-13	13:57:25	50	7.1	9.5	172	233	0	0	0	0	4.994	0.6172	0.82	0.62
152	2020-03-13	13:57:26	50	10.9	9.5	172	232	52	1	150	1	4.999	0.6172	0.82	0.62
153	2020-03-13	13:57:27	49	9.1	9.4	172	232	0	0	0	0	4.997	0.6386	0.8	0.61
154	2020-03-13	13:57:28	50	10.8	9.7	172	232	52	1	150	1	4.997	0.6053	0.82	0.62
155	2020-03-13	13:57:29	50	20.5	9.5	172	232	0	0	0	0	4.997	0.6386	0.91	0.79
156	2020-03-13	13:57:30	51	24.9	9.5	172	232	156	3	426	3	4.992	0.6416	0.82	0.62
157	2020-03-13	13:57:31	50	18.5	9.5	172	232	208	4	576	4	4.995	0.6353	0.81	0.62
158	2020-03-13	13:57:32	50	17.0	9.9	172	232	468	9	1278	9	4.993	0.6353	0.81	0.62
159	2020-03-13	13:57:33	50	15.4	9.9	172	232	728	14	1988	14	4.995	0.6235	0.81	0.61
160	2020-03-13	13:57:35	50	7.2	9.5	172	232	780	15	1988	14	4.995	0.6479	0.89	0.75
161	2020-03-13	13:57:36	50	10.4	9.5	172	232	780	15	2130	15	4.997	0.6345	0.91	0.79
162	2020-03-13	13:57:37	50	9.4	9.5	172	232	156	3	434	3	4.998	0.6131	0.83	0.62
163	2020-03-13	13:57:38	50	7.5	9.5	172	232	0	0	0	0	4.997	0.5929	0.82	0.62
164	2020-03-13	13:57:39	50	11.6	9.5	172	232	116	2	450	3	4.994	0.5929	0.82	0.62
165	2020-03-13	13:57:40	50	13.7	9.5	172	232	0	0	0	0	4.994	0.6047	0.91	0.79
166	2020-03-13	13:57:41	50	12.9	9.5	172	232	480	9	1420	10	4.991	0.5994	0.9	0.79
167	2020-03-13	13:57:42	50	16.8	9.5	172	232	324	6	1912	12	4.994	0.6159	0.9	0.78
168	2020-03-13	13:57:43	50	16.3	9.5	172	232	556	10	1896	10	4.994	0.6243	0.82	0.62
169	2020-03-13	13:57:44	50	9.5	9.5	172	232	0	0	0	0	4.993	0.6231	0.81	0.62
170	2020-03-13	13:57:45	50	8.7	9.5	172	232	52	1	150	1	4.995	0.6149	0.82	0.63
171	2020-03-13	13:57:46	50	11.3	9.5	172	232	0	0	0	0	4.997	0.6049	0.82	0.63
172	2020-03-13	13:57:47	50	12.0	9.5	172	232	324	6	978	7	4.995	0.5919	0.91	0.79
173	2020-03-13	13:57:48	50	6.4	9.5	168	228	0	0	0	0	4.992	0.6027	0.91	0.79

174	2020-03-13	13:57:49	49	10.3	9.5	167	227	104	2	292	2	4.997	0.5998	0.9	0.78
175	2020-03-13	13:57:50	49	10.5	9.5	161	221	104	2	284	2	4.996	0.6064	0.82	0.62
176	2020-03-13	13:57:51	50	11.9	9.5	161	221	156	3	434	3	4.995	0.608	0.82	0.63
177	2020-03-13	13:57:52	51	15.5	9.5	161	221	0	0	0	0	4.996	0.6068	0.81	0.62
178	2020-03-13	13:57:53	51	14.3	9.5	161	221	52	1	150	1	4.995	0.6196	0.91	0.79
179	2020-03-13	13:57:54	50	17.9	9.5	162	222	0	0	0	0	4.996	0.6195	0.91	0.79
180	2020-03-13	13:57:55	50	18.5	9.5	162	222	520	10	1420	10	4.995	0.6163	0.82	0.63
181	2020-03-13	13:57:56	50	15.8	9.5	161	222	676	13	1822	13	4.995	0.6502	0.79	0.6
182	2020-03-13	13:57:57	50	8.1	9.5	161	221	52	1	150	1	4.995	0.6304	0.83	0.63
183	2020-03-13	13:57:58	51	18.1	9.5	160	220	0	0	0	0	4.995	0.6251	0.82	0.63
184	2020-03-13	13:57:59	50	7.8	9.5	160	221	0	0	0	0	4.996	0.6318	0.83	0.62
185	2020-03-13	13:58:00	51	7.5	9.5	161	221	208	4	528	4	4.994	0.6129	0.92	0.8
186	2020-03-13	13:58:01	51	7.5	9.5	161	221	728	14	1988	14	4.996	0.6043	0.92	0.8
187	2020-03-13	13:58:02	51	9.2	9.5	162	222	624	12	1570	11	4.997	0.606	0.92	0.8
188	2020-03-13	13:58:03	50	13.7	9.5	162	222	52	1	150	1	4.996	0.6049	0.83	0.62
189	2020-03-13	13:58:04	50	11.3	9.5	162	222	52	1	284	2	4.995	0.6135	0.81	0.61
190	2020-03-13	13:58:05	50	8.1	9.5	162	222	104	2	292	2	4.996	0.6104	0.83	0.62
191	2020-03-13	13:58:06	51	6.9	9.5	162	222	0	0	0	0	4.996	0.5935	0.92	0.8
192	2020-03-13	13:58:07	51	17.5	10.7	162	222	52	1	150	1	4.996	0.6051	0.92	0.8
193	2020-03-13	13:58:08	50	20.4	10.3	162	222	0	0	0	0	4.995	0.6153	0.92	0.8
194	2020-03-13	13:58:10	51	6.8	9.5	162	222	364	7	1136	8	4.992	0.6384	0.83	0.62
195	2020-03-13	13:58:11	51	9.3	9.5	162	222	676	13	1704	12	4.998	0.5988	0.82	0.62
196	2020-03-13	13:58:12	50	17.1	9.5	162	222	728	14	1988	14	4.998	0.6347	0.81	0.61
197	2020-03-13	13:58:13	51	7.4	9.5	162	222	1300	25	3374	25	4.997	0.635	0.83	0.62
198	2020-03-13	13:58:14	49	8.8	9.5	162	222	416	8	1112	8	4.995	0.6096	0.82	0.62

199	2020-03-13	13:58:15	51	12.0	9.5	162	223	156	3	434	3	4.996	0.6096	0.92	0.8
200	2020-03-13	13:58:16	51	13.2	9.5	162	223	0	0	0	0	4.995	0.6095	0.81	0.61
201	2020-03-13	13:58:17	50	7.0	9.5	162	222	0	0	0	0	4.992	0.5941	0.82	0.62
202	2020-03-13	13:58:18	51	7.2	9.5	162	222	208	4	576	4	4.992	0.6186	0.82	0.62
203	2020-03-13	13:58:19	52	18.2	9.5	162	222	0	0	0	0	4.997	0.6308	0.82	0.63
204	2020-03-13	13:58:20	50	16.1	9.5	162	222	52	1	150	1	4.996	0.6039	0.81	0.62
205	2020-03-13	13:58:21	51	13.3	9.5	162	222	156	3	426	3	4.992	0.6039	0.91	0.8
206	2020-03-13	13:58:22	51	19.6	9.5	162	222	728	14	1988	14	4.994	0.6194	0.82	0.62
207	2020-03-13	13:58:23	50	7.3	9.5	162	222	416	8	1136	8	4.996	0.6196	0.82	0.62
208	2020-03-13	13:58:24	51	7.4	9.5	162	222	572	11	1562	11	4.996	0.6416	0.83	0.63
209	2020-03-13	13:58:25	51	6.9	9.5	162	222	0	0	0	0	4.996	0.6106	0.81	0.61
210	2020-03-13	13:58:26	50	6.8	9.5	162	222	364	7	1002	7	4.995	0.6084	0.83	0.62
211	2020-03-13	13:58:27	51	8.4	9.5	161	221	52	1	150	1	4.995	0.6084	0.92	0.8
212	2020-03-13	13:58:28	51	7.4	9.5	161	221	0	0	0	0	4.996	0.6041	0.92	0.8
213	2020-03-13	13:58:29	51	12.8	9.5	161	221	0	0	0	0	4.997	0.6027	0.81	0.61
214	2020-03-13	13:58:30	51	12.2	9.5	161	221	260	5	702	5	4.996	0.6188	0.77	0.59
215	2020-03-13	13:58:31	50	9.9	9.5	161	221	0	0	0	0	4.996	0.6292	0.82	0.62
216	2020-03-13	13:58:32	51	11.8	9.5	163	223	156	3	434	3	4.996	0.6208	0.9	0.78
217	2020-03-13	13:58:33	50	13.3	9.5	163	223	208	4	576	4	4.997	0.6265	0.91	0.79
218	2020-03-13	13:58:34	51	18.3	9.5	163	223	0	0	0	0	4.994	0.6312	0.91	0.79
219	2020-03-13	13:58:35	52	15.5	9.8	163	222	0	0	0	0	4.996	0.6278	0.82	0.62
220	2020-03-13	13:58:36	50	7.1	9.5	163	224	52	1	150	1	4.995	0.6569	0.83	0.63
221	2020-03-13	13:58:37	50	7.7	9.5	163	223	0	0	0	0	4.997	0.6196	0.82	0.63
222	2020-03-13	13:58:38	50	9.4	9.5	163	223	520	10	1562	11	4.996	0.6096	0.8	0.61
223	2020-03-13	13:58:39	51	9.0	9.5	163	224	772	14	2182	15	4.997	0.6021	0.9	0.79

224	2020-03-13	13:58:40	51	13.6	9.5	163	223	452	8	1868	12	4.996	0.6108	0.9	0.78
225	2020-03-13	13:58:41	50	15.0	10.5	164	224	52	1	300	2	4.996	0.6023	0.91	0.79
226	2020-03-13	13:58:42	51	7.9	10.0	164	224	52	1	150	1	4.993	0.6267	0.8	0.61
227	2020-03-13	13:58:43	51	7.2	9.5	164	224	0	0	142	1	4.995	0.6339	0.81	0.62
228	2020-03-13	13:58:44	51	7.9	9.5	164	225	728	14	1996	14	4.995	0.6314	0.82	0.62
229	2020-03-13	13:58:45	51	22.3	9.5	164	224	0	0	0	0	4.995	0.6192	0.91	0.79
230	2020-03-13	13:58:46	51	13.4	9.5	164	224	0	0	0	0	4.996	0.6282	0.91	0.79
231	2020-03-13	13:58:47	51	13.3	9.5	164	224	740	14	1846	13	4.993	0.6202	0.82	0.62
232	2020-03-13	13:58:48	51	13.7	9.5	164	224	780	15	2114	15	4.992	0.6168	0.82	0.62
233	2020-03-13	13:58:49	52	11.4	9.5	164	224	208	4	580	4	4.996	0.6168	0.82	0.61
234	2020-03-13	13:58:50	51	8.2	9.5	164	224	52	1	150	1	4.996	0.6092	0.79	0.6
235	2020-03-13	13:58:51	51	8.4	9.5	164	225	0	0	0	0	4.997	0.6219	0.82	0.62
236	2020-03-13	13:58:52	50	8.2	9.5	164	224	52	1	150	1	4.997	0.6033	0.92	0.8
237	2020-03-13	13:58:53	51	7.9	9.5	164	224	0	0	0	0	4.997	0.6062	0.91	0.79
238	2020-03-13	13:58:54	50	11.1	9.5	164	224	52	1	150	1	4.997	0.6168	0.92	0.8
239	2020-03-13	13:58:55	51	11.6	9.5	164	224	468	9	1420	10	4.998	0.6219	0.83	0.62
240	2020-03-13	13:58:56	52	8.4	9.5	164	224	780	15	1988	14	4.996	0.6188	0.82	0.62
241	2020-03-13	13:58:57	52	14.4	9.5	164	224	728	14	1988	14	4.997	0.6098	0.82	0.62
242	2020-03-13	13:58:58	50	19.9	9.5	164	224	728	14	1988	14	4.997	0.6274	0.91	0.79
243	2020-03-13	13:58:59	52	21.4	9.5	164	224	832	16	2240	16	4.996	0.6343	0.92	0.8
244	2020-03-13	13:59:00	51	18.7	9.5	164	224	364	7	986	7	4.995	0.6342	0.92	0.8
245	2020-03-13	13:59:01	52	17.9	9.5	164	224	312	6	860	6	4.995	0.6265	0.91	0.8
246	2020-03-13	13:59:02	52	16.4	9.5	164	224	0	0	0	0	4.994	0.6206	0.81	0.61
247	2020-03-13	13:59:03	51	18.1	9.5	164	224	0	0	0	0	4.995	0.619	0.82	0.62
248	2020-03-13	13:59:04	51	16.0	9.5	164	224	624	12	1704	12	4.994	0.6193	0.82	0.62

249	2020-03-13	13:59:05	51	15.4	9.5	164	224	676	13	1846	13	4.995	0.6096	0.91	0.8
250	2020-03-13	13:59:06	52	17.3	9.5	164	224	676	13	1846	13	4.995	0.6172	0.92	0.8
251	2020-03-13	13:59:07	51	12.9	9.5	164	224	728	14	1996	14	4.994	0.6212	0.92	0.8
252	2020-03-13	13:59:08	52	12.0	9.5	164	224	0	0	0	0	4.994	0.6121	0.82	0.62
253	2020-03-13	13:59:09	51	11.6	9.5	164	225	52	1	0	0	4.996	0.6045	0.81	0.62
254	2020-03-13	13:59:10	51	7.2	9.5	164	224	0	0	0	0	4.995	0.6045	0.81	0.62
255	2020-03-13	13:59:11	51	12.4	9.5	164	224	260	5	718	5	4.997	0.641	0.82	0.62
256	2020-03-13	13:59:12	52	14.7	9.5	164	224	52	1	150	1	4.996	0.6139	0.82	0.62
257	2020-03-13	13:59:13	51	16.8	9.5	165	225	0	0	0	0	4.996	0.6168	0.91	0.79
258	2020-03-13	13:59:14	52	18.0	10.7	166	226	364	7	994	7	4.994	0.6247	0.82	0.63
259	2020-03-13	13:59:15	53	8.3	10.2	166	226	208	4	576	4	4.997	0.632	0.82	0.63
260	2020-03-13	13:59:16	51	7.1	9.7	166	226	0	0	0	0	4.996	0.632	0.82	0.62
261	2020-03-13	13:59:17	51	18.3	9.5	165	226	468	9	1278	9	4.995	0.6308	0.82	0.63
262	2020-03-13	13:59:18	51	7.5	9.5	165	225	728	14	1988	14	4.992	0.6388	0.91	0.79
263	2020-03-13	13:59:19	52	8.2	9.5	165	225	208	4	576	4	4.998	0.6335	0.92	0.8
264	2020-03-13	13:59:20	51	10.4	9.5	165	225	52	1	150	1	4.997	0.6437	0.92	0.8
265	2020-03-13	13:59:21	52	11.0	9.5	165	226	0	0	0	0	4.996	0.6357	0.82	0.62
266	2020-03-13	13:59:22	52	7.3	9.5	165	225	156	3	434	3	4.997	0.6557	0.82	0.62
267	2020-03-13	13:59:23	52	17.5	9.5	165	225	0	0	0	0	4.997	0.6349	0.8	0.61
268	2020-03-13	13:59:24	52	13.4	9.5	165	225	156	3	434	3	4.994	0.6278	0.83	0.64
269	2020-03-13	13:59:25	52	12.2	9.5	165	225	0	0	0	0	4.996	0.6343	0.88	0.73
270	2020-03-13	13:59:26	53	17.1	9.5	165	225	468	9	1080	8	4.996	0.6375	0.9	0.79
271	2020-03-13	13:59:27	52	8.4	9.5	165	225	0	0	0	0	4.995	0.6349	0.9	0.78
272	2020-03-13	13:59:28	51	9.8	9.5	165	225	376	7	804	6	4.997	0.6001	0.82	0.63
273	2020-03-13	13:59:29	52	14.3	9.5	165	225	52	1	150	1	4.997	0.6017	0.82	0.62

274	2020-03-13	13:59:30	52	13.2	9.5	165	225	0	0	0	0	4.997	0.6153	0.82	0.62
275	2020-03-13	13:59:31	52	8.5	9.5	165	226	52	1	150	1	4.997	0.611	0.88	0.72
276	2020-03-13	13:59:32	51	6.6	9.5	165	225	220	4	584	4	4.996	0.6112	0.83	0.63
277	2020-03-13	13:59:33	51	7.3	9.5	165	225	0	0	0	0	4.996	0.6053	0.82	0.62
278	2020-03-13	13:59:34	51	7.0	9.5	165	226	0	0	0	0	4.996	0.6005	0.81	0.62
279	2020-03-13	13:59:35	52	13.6	9.5	165	225	260	5	702	5	4.995	0.6015	0.77	0.59
280	2020-03-13	13:59:36	52	11.8	9.5	165	225	0	0	0	0	4.997	0.6663	0.82	0.62
281	2020-03-13	13:59:37	51	13.5	9.5	165	225	312	6	852	6	4.997	0.6663	0.83	0.63
282	2020-03-13	13:59:38	52	13.2	9.5	165	225	728	14	1972	14	4.996	0.639	0.89	0.74
283	2020-03-13	13:59:39	52	10.6	9.5	165	225	920	17	2634	19	4.995	0.6243	0.91	0.79
284	2020-03-13	13:59:40	52	7.8	9.5	165	225	188	3	636	4	4.997	0.6255	0.92	0.8
285	2020-03-13	13:59:41	51	12.4	9.5	165	225	52	1	300	2	4.996	0.6037	0.82	0.62
286	2020-03-13	13:59:42	52	10.0	9.8	165	226	52	1	150	1	4.993	0.606	0.82	0.62
287	2020-03-13	13:59:43	51	7.8	9.5	165	225	0	0	0	0	4.997	0.5958	0.81	0.61
288	2020-03-13	13:59:44	51	8.5	9.5	165	226	208	4	568	4	4.997	0.6239	0.91	0.8
289	2020-03-13	13:59:45	52	11.8	9.5	165	225	104	2	276	2	4.997	0.6035	0.91	0.8
290	2020-03-13	13:59:46	51	7.7	9.5	165	225	0	0	0	0	4.997	0.6282	0.92	0.8
291	2020-03-13	13:59:47	52	17.9	9.7	165	225	104	2	292	2	4.997	0.6037	0.8	0.6
292	2020-03-13	13:59:48	51	11.3	10.5	165	226	104	2	576	4	4.993	0.6115	0.82	0.62
293	2020-03-13	13:59:49	51	9.2	10.0	165	225	104	2	0	0	4.992	0.6278	0.82	0.62
294	2020-03-13	13:59:51	52	12.8	9.6	165	225	0	0	0	0	4.996	0.6102	0.91	0.8
295	2020-03-13	13:59:52	51	10.1	9.5	165	226	52	1	150	1	4.994	0.6106	0.91	0.8
296	2020-03-13	13:59:53	52	6.7	9.5	165	225	624	12	1704	12	4.995	0.6153	0.82	0.62
297	2020-03-13	13:59:54	51	8.0	9.5	165	225	676	13	1846	13	4.995	0.5984	0.81	0.62
298	2020-03-13	13:59:55	51	7.9	9.5	165	225	676	13	1846	13	4.995	0.5946	0.8	0.61

299	2020-03-13	13:59:56	52	13.5	9.5	165	225	1352	26	3484	26	4.996	0.6137	0.82	0.62
300	2020-03-13	13:59:57	52	8.8	9.5	165	225	364	7	938	7	4.995	0.63	0.83	0.62
301	2020-03-13	13:59:58	52	7.7	9.5	165	225	0	0	0	0	4.996	0.63	0.92	0.8
302	2020-03-13	13:59:59	52	7.2	9.5	165	225	260	5	710	5	4.996	0.6178	0.81	0.61
303	2020-03-13	14:00:00	51	9.5	9.5	165	225	416	8	1112	8	4.994	0.6129	0.83	0.62
304	2020-03-13	14:00:01	51	8.8	9.5	165	225	0	0	0	0	4.994	0.6111	0.83	0.62
305	2020-03-13	14:00:02	53	19.4	9.6	165	225	52	1	150	1	4.995	0.6163	0.83	0.62
306	2020-03-13	14:00:03	52	18.9	9.5	165	225	0	0	0	0	4.995	0.6347	0.81	0.61
307	2020-03-13	14:00:04	52	19.3	9.5	165	225	676	13	1846	13	4.995	0.6418	0.82	0.63
308	2020-03-13	14:00:05	52	8.9	9.5	165	225	780	15	2130	15	4.995	0.6418	0.9	0.78
309	2020-03-13	14:00:06	52	7.5	9.5	165	225	156	3	434	3	4.998	0.6159	0.91	0.79
310	2020-03-13	14:00:07	52	7.9	9.5	165	225	52	1	150	1	4.997	0.6047	0.82	0.62
311	2020-03-13	14:00:08	51	6.2	9.5	165	226	0	0	0	0	4.996	0.6058	0.8	0.61
312	2020-03-13	14:00:09	52	8.3	9.5	165	225	208	4	576	4	4.997	0.6045	0.82	0.62
313	2020-03-13	14:00:10	52	7.0	9.5	166	226	0	0	0	0	4.995	0.6098	0.83	0.63
314	2020-03-13	14:00:11	51	10.6	9.5	166	227	0	0	0	0	4.997	0.5994	0.91	0.79
315	2020-03-13	14:00:12	52	14.0	9.5	166	227	728	14	1988	14	4.997	0.6076	0.91	0.79
316	2020-03-13	14:00:13	52	7.2	9.5	166	226	728	14	1988	14	4.997	0.6426	0.9	0.79
317	2020-03-13	14:00:14	52	12.7	9.5	166	226	728	14	1988	14	4.996	0.6076	0.82	0.63
318	2020-03-13	14:00:15	53	20.5	9.6	166	226	260	5	702	5	4.996	0.6104	0.81	0.61
319	2020-03-13	14:00:16	52	28.5	9.9	167	227	208	4	576	4	4.995	0.6241	0.79	0.6
320	2020-03-13	14:00:17	53	23.7	9.5	167	227	0	0	0	0	4.993	0.6361	0.9	0.78
321	2020-03-13	14:00:18	53	15.6	9.6	167	228	0	0	0	0	4.993	0.6489	0.9	0.78
322	2020-03-13	14:00:19	52	13.3	9.5	167	227	156	3	434	3	4.995	0.6151	0.91	0.79
323	2020-03-13	14:00:20	51	12.3	9.5	166	226	0	0	0	0	4.995	0.6163	0.83	0.62

324	2020-03-13	14:00:21	52	15.6	10.5	166	227	208	4	576	4	4.995	0.6139	0.82	0.62
325	2020-03-13	14:00:22	52	10.2	10.0	166	226	0	0	0	0	4.995	0.6265	0.81	0.61
326	2020-03-13	14:00:23	53	14.2	9.6	166	226	52	1	284	2	4.995	0.6457	0.83	0.62
327	2020-03-13	14:00:24	53	13.9	9.6	166	227	676	13	1704	12	4.995	0.642	0.78	0.6
328	2020-03-13	14:00:25	52	12.3	9.6	166	226	312	6	718	5	4.998	0.6131	0.82	0.63
329	2020-03-13	14:00:26	53	13.5	9.6	166	226	52	1	150	1	4.996	0.6131	0.91	0.79
330	2020-03-13	14:00:27	52	14.0	9.6	166	226	0	0	0	0	4.995	0.6117	0.81	0.62
331	2020-03-13	14:00:28	52	16.8	9.5	166	227	104	2	284	2	4.996	0.6117	0.8	0.61
332	2020-03-13	14:00:29	52	17.0	9.5	166	226	52	1	150	1	4.996	0.6386	0.8	0.61
333	2020-03-13	14:00:30	53	12.8	9.5	166	226	0	0	0	0	4.996	0.6443	0.91	0.8
334	2020-03-13	14:00:30	53	14.0	9.5	166	226	156	3	434	3	4.996	0.6477	0.91	0.8
335	2020-03-13	14:00:31	52	16.4	9.6	166	226	104	2	292	2	4.996	0.6443	0.92	0.8
336	2020-03-13	14:00:32	53	18.8	9.6	166	226	0	0	0	0	4.996	0.6443	0.92	0.8

Run-DoS ATTACK 24°C												
	Date	T.Stamp	Temp	CPU_Load	Mem_Load	ProNo,	ThreadsNo	Time	Voltage(V)	Current(A)	D+(V)	D-(V)
1	2020-03-16	22:28:36	55	10.9	9.7	173	234	22:28:36	4.984	0.5805	0.8	0.61
2	2020-03-16	22:28:37	56	12.8	9.7	173	233	22:28:37	4.983	0.5728	0.91	0.8
3	2020-03-16	22:28:37	55	15.7	9.7	173	233	22:28:38	4.983	0.5764	0.91	0.8
4	2020-03-16	22:28:39	55	15.2	9.7	173	235	22:28:39	4.983	0.575	0.81	0.63
5	2020-03-16	22:28:40	55	10.4	9.7	174	234	22:28:40	4.983	0.5727	0.81	0.62
6	2020-03-16	22:28:41	55	19.7	9.7	175	236	22:28:41	4.985	0.5701	0.83	0.65
7	2020-03-16	22:28:41	55	19.9	9.7	174	235	22:28:41	4.985	0.5701	0.83	0.65
8	2020-03-16	22:28:42	55	21.1	9.7	174	236	22:28:42	4.984	0.5626	0.9	0.79
9	2020-03-16	22:28:43	56	26.1	9.7	176	236	22:28:43	4.983	0.5713	0.9	0.79
10	2020-03-16	22:28:44	55	29.2	9.8	177	237	22:28:44	4.982	0.5764	0.82	0.63
11	2020-03-16	22:28:45	56	27.3	9.7	175	235	22:28:45	4.984	0.573	0.82	0.63
12	2020-03-16	22:28:46	56	21.3	9.7	175	236	22:28:46	4.985	0.5624	0.9	0.79
13	2020-03-16	22:28:47	56	21.5	9.7	175	236	22:28:47	4.983	0.5699	0.92	0.81
14	2020-03-16	22:28:48	55	18.8	9.8	176	236	22:28:48	4.984	0.5723	0.82	0.63
15	2020-03-16	22:28:49	55	6.9	9.8	176	236	22:28:49	4.982	0.5874	0.82	0.63
16	2020-03-16	22:28:50	55	6.8	9.8	176	236	22:28:50	4.982	0.5897	0.82	0.63
17	2020-03-16	22:28:51	55	15.4	9.8	176	236	22:28:51	4.982	0.5689	0.91	0.79
18	2020-03-16	22:28:52	56	29.6	9.9	188	247	22:28:52	4.985	0.5732	0.9	0.79
19	2020-03-16	22:28:53	55	15.2	9.9	184	244	22:28:53	4.981	0.5689	0.81	0.63
20	2020-03-16	22:28:54	56	15.5	9.9	183	243	22:28:54	4.984	0.5672	0.82	0.63
21	2020-03-16	22:28:55	56	19.7	9.8	179	239	22:28:55	4.984	0.5892	0.88	0.73
22	2020-03-16	22:28:56	55	16.5	9.8	179	238	22:28:56	4.984	0.576	0.9	0.79
23	2020-03-16	22:28:57	56	18.0	9.8	182	242	22:28:57	4.983	0.5642	0.82	0.63

24	2020-03-16	22:28:58	55	14.4	9.8	179	239	22:28:58	4.984	0.5872	0.78	0.59
25	2020-03-16	22:28:59	55	10.1	9.8	180	240	22:28:59	4.985	0.5752	0.82	0.63
26	2020-03-16	22:29:00	55	10.6	9.8	179	240	22:29:00	4.985	0.5809	0.9	0.79
27	2020-03-16	22:29:01	56	17.2	9.8	179	239	22:29:01	4.984	0.5966	0.9	0.79
28	2020-03-16	22:29:02	56	8.6	9.8	179	239	22:29:02	4.983	0.5842	0.82	0.63
29	2020-03-16	22:29:03	55	8.8	9.8	173	234	22:29:03	4.984	0.5927	0.81	0.63
30	2020-03-16	22:29:04	55	21.3	11.0	174	234	22:29:04	4.985	0.5994	0.9	0.79
31	2020-03-16	22:29:05	55	13.2	10.7	179	239	22:29:05	4.985	0.6096	0.9	0.79
32	2020-03-16	22:29:06	56	25.9	10.3	179	239	22:29:06	4.983	0.5837	0.78	0.59
33	2020-03-16	22:29:07	57	30.6	10.0	179	239	22:29:07	4.987	0.5901	0.81	0.63
34	2020-03-16	22:29:08	56	30.8	10.0	179	239	22:29:08	4.986	0.5721	0.82	0.63
35	2020-03-16	22:29:09	57	43.0	10.1	187	247	22:29:09	4.985	0.5837	0.91	0.8
36	2020-03-16	22:29:10	58	38.9	10.1	186	247	22:29:10	4.985	0.618	0.92	0.81
37	2020-03-16	22:29:11	58	38.2	10.1	186	246	22:29:11	4.985	0.573	0.81	0.62
38	2020-03-16	22:29:12	58	31.8	10.0	184	241	22:29:12	4.986	0.5713	0.81	0.63
39	2020-03-16	22:29:13	58	32.4	10.0	179	239	22:29:13	4.985	0.587	0.9	0.79
40	2020-03-16	22:29:14	57	30.9	10.0	179	239	22:29:14	4.986	0.5867	0.9	0.79
41	2020-03-16	22:29:15	58	32.3	10.0	179	239	22:29:15	4.984	0.5966	0.82	0.63
42	2020-03-16	22:29:16	59	31.6	10.0	179	239	22:29:16	4.984	0.5933	0.81	0.61
43	2020-03-16	22:29:17	58	30.9	10.0	179	239	22:29:17	4.983	0.5895	0.81	0.63
44	2020-03-16	22:29:18	58	32.3	10.0	178	237	22:29:18	4.985	0.587	0.9	0.79
45	2020-03-16	22:29:19	58	37.4	9.9	174	234	22:29:19	4.985	0.6206	0.9	0.79
46	2020-03-16	22:29:20	59	31.1	10.0	174	234	22:29:20	4.986	0.5787	0.81	0.63
47	2020-03-16	22:29:20	58	30.2	10.0	174	234	22:29:20	4.986	0.5787	0.81	0.63
48	2020-03-16	22:29:21	60	33.6	10.0	174	235	22:29:21	4.985	0.5899	0.78	0.6

49	2020-03-16	22:29:22	59	42.1	10.0	174	238	22:29:22	4.983	0.5929	0.9	0.78
50	2020-03-16	22:29:23	59	44.3	10.0	178	238	22:29:23	4.981	0.6023	0.9	0.79
51	2020-03-16	22:29:24	57	35.3	10.0	180	240	22:29:24	4.982	0.6318	0.9	0.79
52	2020-03-16	22:29:25	59	31.6	10.0	180	240	22:29:25	4.982	0.6233	0.8	0.6
53	2020-03-16	22:29:26	60	31.3	10.0	180	240	22:29:26	4.982	0.6163	0.81	0.61
54	2020-03-16	22:29:27	59	30.6	10.0	180	240	22:29:27	4.981	0.6257	0.91	0.8
55	2020-03-16	22:29:28	59	38.0	10.1	180	241	22:29:28	4.981	0.6182	0.92	0.8
56	2020-03-16	22:29:29	59	36.4	10.1	180	247	22:29:29	4.98	0.609	0.79	0.6
57	2020-03-16	22:29:30	59	31.0	10.1	187	248	22:29:30	4.982	0.6027	0.79	0.6
58	2020-03-16	22:29:31	59	30.6	10.1	187	248	22:29:31	4.981	0.6058	0.86	0.69
59	2020-03-16	22:29:32	59	38.8	10.4	187	250	22:29:32	4.98	0.6092	0.9	0.79
60	2020-03-16	22:29:33	60	32.5	10.1	184	244	22:29:33	4.98	0.6007	0.9	0.79
61	2020-03-16	22:29:34	59	33.9	10.1	185	246	22:29:34	4.98	0.6027	0.79	0.6
62	2020-03-16	22:29:35	60	38.8	10.1	186	246	22:29:35	4.98	0.6031	0.82	0.63
63	2020-03-16	22:29:36	60	39.8	10.1	186	246	22:29:36	4.978	0.6043	0.91	0.79
64	2020-03-16	22:29:37	60	36.5	10.1	186	248	22:29:37	4.981	0.6045	0.9	0.79
65	2020-03-16	22:29:38	59	36.1	11.2	188	249	22:29:38	4.982	0.6035	0.82	0.64
66	2020-03-16	22:29:39	60	40.8	10.9	193	254	22:29:39	4.982	0.6076	0.81	0.61
67	2020-03-16	22:29:40	59	31.5	10.4	191	251	22:29:40	4.982	0.6377	0.81	0.61
68	2020-03-16	22:29:41	59	35.0	10.2	188	249	22:29:41	4.98	0.6253	0.91	0.8
69	2020-03-16	22:29:42	60	31.1	10.2	187	246	22:29:42	4.981	0.6223	0.91	0.8
70	2020-03-16	22:29:43	60	34.0	10.2	187	247	22:29:43	4.983	0.63	0.81	0.61
71	2020-03-16	22:29:44	60	30.6	10.2	187	247	22:29:44	4.983	0.6247	0.8	0.61
72	2020-03-16	22:29:45	60	31.0	10.2	187	247	22:29:45	4.983	0.6248	0.91	0.8
73	2020-03-16	22:29:45	60	31.4	10.2	187	247	22:29:45	4.983	0.6248	0.91	0.8

74	2020-03-16	22:29:46	60	31.1	10.2	187	247	22:29:46	4.982	0.639	0.91	0.8
75	2020-03-16	22:29:47	60	42.2	10.3	193	253	22:29:47	4.982	0.6449	0.81	0.61
76	2020-03-16	22:29:48	60	39.2	10.3	192	252	22:29:48	4.983	0.6108	0.79	0.6
77	2020-03-16	22:29:49	59	44.9	10.2	191	251	22:29:49	4.982	0.6033	0.81	0.62
78	2020-03-16	22:29:50	60	34.6	10.3	192	254	22:29:50	4.982	0.6284	0.91	0.8
79	2020-03-16	22:29:51	60	30.9	10.2	192	252	22:29:51	4.982	0.6102	0.92	0.8
80	2020-03-16	22:29:52	61	30.9	10.2	192	252	22:29:52	4.982	0.6172	0.81	0.61
81	2020-03-16	22:29:53	60	36.9	10.2	191	251	22:29:53	4.981	0.6157	0.81	0.61
82	2020-03-16	22:29:54	59	32.6	10.2	190	250	22:29:54	4.981	0.616	0.91	0.79
83	2020-03-16	22:29:55	61	37.5	10.2	189	249	22:29:55	4.983	0.628	0.92	0.8
84	2020-03-16	22:29:56	61	32.0	10.2	189	249	22:29:56	4.981	0.6377	0.8	0.6
85	2020-03-16	22:29:57	61	31.2	10.2	189	249	22:29:57	4.98	0.6196	0.8	0.61
86	2020-03-16	22:29:58	62	31.6	10.2	189	249	22:29:58	4.979	0.6086	0.82	0.63
87	2020-03-16	22:29:59	59	40.4	10.2	185	245	22:29:59	4.98	0.6049	0.91	0.79
88	2020-03-16	22:30:00	61	41.1	10.3	186	256	22:30:00	4.981	0.6127	0.9	0.79
89	2020-03-16	22:30:01	60	38.8	10.3	196	256	22:30:01	4.981	0.6019	0.81	0.62
90	2020-03-16	22:30:02	61	38.3	10.3	196	256	22:30:02	4.981	0.6064	0.81	0.62
91	2020-03-16	22:30:03	61	34.0	10.3	196	256	22:30:03	4.982	0.6065	0.91	0.8
92	2020-03-16	22:30:04	60	31.0	10.3	196	256	22:30:04	4.983	0.606	0.9	0.79
93	2020-03-16	22:30:05	61	30.9	10.3	196	256	22:30:05	4.981	0.6375	0.83	0.64
94	2020-03-16	22:30:06	61	32.6	10.3	193	253	22:30:06	4.981	0.6326	0.8	0.62
95	2020-03-16	22:30:07	60	36.7	10.3	193	253	22:30:07	4.98	0.6343	0.8	0.61
96	2020-03-16	22:30:07	61	30.8	10.3	193	253	22:30:08	4.983	0.6353	0.91	0.8
97	2020-03-16	22:30:08	61	31.7	10.3	193	253	22:30:09	4.983	0.6184	0.9	0.79
98	2020-03-16	22:30:09	60	36.6	10.2	187	248	22:30:10	4.983	0.6161	0.8	0.61

99	2020-03-16	22:30:10	60	32.7	10.3	187	247	22:30:11	4.983	0.6147	0.81	0.61
100	2020-03-16	22:30:12	61	39.0	11.0	194	254	22:30:12	4.982	0.6129	0.81	0.62
101	2020-03-16	22:30:13	61	33.2	10.6	194	254	22:30:13	4.983	0.6082	0.91	0.8
102	2020-03-16	22:30:13	61	41.1	10.2	184	243	22:30:13	4.983	0.6082	0.91	0.8
103	2020-03-16	22:30:14	61	54.1	10.4	199	259	22:30:14	4.982	0.6045	0.92	0.8
104	2020-03-16	22:30:15	61	36.4	10.3	198	258	22:30:15	4.982	0.6078	0.81	0.61
105	2020-03-16	22:30:16	62	31.1	10.3	198	258	22:30:16	4.982	0.6194	0.81	0.62
106	2020-03-16	22:30:17	62	31.8	10.4	198	258	22:30:17	4.981	0.6062	0.91	0.8
107	2020-03-16	22:30:18	61	31.0	10.4	198	258	22:30:18	4.977	0.6133	0.92	0.81
108	2020-03-16	22:30:19	62	30.8	10.4	198	258	22:30:19	4.979	0.62	0.82	0.62
109	2020-03-16	22:30:20	62	31.4	10.4	198	258	22:30:20	4.979	0.61	0.81	0.61
110	2020-03-16	22:30:21	61	31.1	10.4	198	258	22:30:21	4.98	0.6017	0.91	0.79
111	2020-03-16	22:30:22	61	30.5	10.4	198	258	22:30:22	4.981	0.6055	0.93	0.81
112	2020-03-16	22:30:23	61	39.9	10.3	195	255	22:30:23	4.983	0.6176	0.88	0.73
113	2020-03-16	22:30:24	62	34.9	10.3	198	258	22:30:24	4.983	0.6212	0.81	0.63
114	2020-03-16	22:30:25	61	31.9	10.3	197	257	22:30:25	4.983	0.6143	0.82	0.63
115	2020-03-16	22:30:26	60	36.2	10.3	197	257	22:30:26	4.983	0.614	0.84	0.66
116	2020-03-16	22:30:27	62	38.7	10.3	197	257	22:30:27	4.983	0.6359	0.9	0.78
117	2020-03-16	22:30:28	62	42.7	10.3	198	258	22:30:28	4.983	0.6358	0.82	0.63
118	2020-03-16	22:30:29	61	31.4	10.3	198	258	22:30:29	4.978	0.6212	0.81	0.63
119	2020-03-16	22:30:30	61	30.5	10.3	198	258	22:30:30	4.981	0.6239	0.81	0.61
120	2020-03-16	22:30:31	61	30.2	10.3	198	257	22:30:31	4.98	0.6271	0.9	0.79
121	2020-03-16	22:30:32	61	32.7	10.3	194	254	22:30:32	4.978	0.6302	0.9	0.79
122	2020-03-16	22:30:33	61	31.0	10.3	194	254	22:30:33	4.982	0.6221	0.78	0.6
123	2020-03-16	22:30:33	60	32.1	10.3	194	254	22:30:33	4.982	0.6221	0.78	0.6

124	2020-03-16	22:30:34	62	31.6	10.3	194	253	22:30:34	4.983	0.6237	0.82	0.63
125	2020-03-16	22:30:35	61	31.5	10.3	193	253	22:30:35	4.983	0.6237	0.9	0.79
126	2020-03-16	22:30:36	61	31.7	10.3	193	253	22:30:36	4.983	0.6239	0.9	0.79
127	2020-03-16	22:30:37	61	31.1	10.3	193	253	22:30:37	4.983	0.6204	0.82	0.63
128	2020-03-16	22:30:38	61	33.2	10.3	193	253	22:30:38	4.983	0.6141	0.81	0.61
129	2020-03-16	22:30:39	61	40.4	10.3	193	253	22:30:39	4.982	0.607	0.81	0.61
130	2020-03-16	22:30:40	62	38.6	10.3	192	252	22:30:40	4.983	0.6365	0.91	0.8
131	2020-03-16	22:30:41	61	33.3	10.3	192	252	22:30:41	4.982	0.621	0.93	0.81
132	2020-03-16	22:30:42	62	30.7	10.3	192	252	22:30:42	4.981	0.6072	0.81	0.61
133	2020-03-16	22:30:43	62	31.3	10.3	192	252	22:30:43	4.981	0.6147	0.81	0.61
134	2020-03-16	22:30:44	61	36.3	11.5	191	251	22:30:44	4.98	0.6219	0.91	0.8
135	2020-03-16	22:30:45	62	31.4	11.0	191	250	22:30:45	4.98	0.6168	0.91	0.8
136	2020-03-16	22:30:46	62	31.2	10.6	190	250	22:30:46	4.979	0.6076	0.91	0.79
137	2020-03-16	22:30:47	62	28.9	10.2	190	250	22:30:47	4.981	0.6058	0.81	0.61
138	2020-03-16	22:30:48	62	30.7	10.2	190	250	22:30:48	4.981	0.6035	0.81	0.61
139	2020-03-16	22:30:49	62	30.9	10.2	190	250	22:30:49	4.983	0.6106	0.91	0.79
140	2020-03-16	22:30:50	61	31.8	10.2	190	250	22:30:50	4.982	0.6086	0.91	0.8
141	2020-03-16	22:30:51	62	35.1	10.2	189	249	22:30:51	4.982	0.6131	0.81	0.61
142	2020-03-16	22:30:52	61	38.6	10.2	189	249	22:30:52	4.983	0.617	0.8	0.61
143	2020-03-16	22:30:53	62	39.5	10.2	189	249	22:30:53	4.982	0.6204	0.91	0.79
144	2020-03-16	22:30:54	62	33.1	10.2	188	248	22:30:54	4.983	0.6257	0.91	0.8
145	2020-03-16	22:30:55	61	31.3	10.2	188	248	22:30:55	4.983	0.6306	0.91	0.8
146	2020-03-16	22:30:56	63	31.0	10.2	188	248	22:30:56	4.982	0.6326	0.8	0.62
147	2020-03-16	22:30:57	62	30.9	10.2	188	248	22:30:57	4.98	0.6163	0.82	0.63
148	2020-03-16	22:30:58	62	30.9	10.2	188	248	22:30:58	4.981	0.6162	0.87	0.71

149	2020-03-16	22:30:59	61	31.0	10.2	188	247	22:30:59	4.983	0.6043	0.9	0.79
150	2020-03-16	22:31:00	62	30.2	10.2	187	247	22:31:00	4.982	0.6041	0.78	0.6
151	2020-03-16	22:31:01	61	31.2	10.2	187	247	22:31:01	4.981	0.6068	0.77	0.59
152	2020-03-16	22:31:02	62	30.4	10.2	186	246	22:31:02	4.979	0.6131	0.91	0.8
153	2020-03-16	22:31:03	62	31.2	10.2	186	246	22:31:03	4.98	0.6131	0.91	0.8
154	2020-03-16	22:31:04	62	31.4	10.2	185	244	22:31:04	4.98	0.6015	0.9	0.79
155	2020-03-16	22:31:05	61	38.1	10.1	184	243	22:31:05	4.983	0.6255	0.81	0.63
156	2020-03-16	22:31:05	62	38.6	10.1	183	243	22:31:05	4.983	0.6255	0.81	0.63
157	2020-03-16	22:31:06	61	34.8	10.1	183	243	22:31:06	4.983	0.6296	0.81	0.63
158	2020-03-16	22:31:07	62	30.4	10.1	183	243	22:31:07	4.983	0.6218	0.9	0.79
159	2020-03-16	22:31:08	62	30.1	10.1	183	243	22:31:08	4.982	0.6206	0.9	0.79
160	2020-03-16	22:31:09	62	31.8	10.2	183	243	22:31:09	4.982	0.6227	0.82	0.62
161	2020-03-16	22:31:10	62	31.6	10.2	183	243	22:31:10	4.981	0.6224	0.8	0.6
162	2020-03-16	22:31:11	62	31.9	10.2	183	243	22:31:11	4.982	0.6163	0.81	0.62
163	2020-03-16	22:31:12	62	33.7	10.2	184	244	22:31:12	4.982	0.6039	0.91	0.8
164	2020-03-16	22:31:13	63	32.1	10.2	184	244	22:31:13	4.982	0.6039	0.92	0.81
165	2020-03-16	22:31:14	63	31.1	10.1	184	244	22:31:14	4.983	0.6025	0.8	0.61
166	2020-03-16	22:31:15	63	31.6	10.1	184	244	22:31:15	4.98	0.6025	0.8	0.61
167	2020-03-16	22:31:16	62	31.1	10.1	184	244	22:31:16	4.98	0.6027	0.91	0.8
168	2020-03-16	22:31:17	62	41.2	11.5	184	244	22:31:17	4.98	0.6106	0.92	0.81
169	2020-03-16	22:31:18	62	38.4	11.0	184	244	22:31:18	4.981	0.6066	0.82	0.62
170	2020-03-16	22:31:19	62	40.7	10.5	184	244	22:31:19	4.981	0.6051	0.79	0.59
171	2020-03-16	22:31:20	62	34.5	10.1	184	244	22:31:20	4.982	0.61	0.81	0.61
172	2020-03-16	22:31:21	62	33.5	10.2	184	245	22:31:21	4.982	0.6021	0.91	0.8
173	2020-03-16	22:31:22	63	34.4	10.2	184	244	22:31:22	4.982	0.6159	0.92	0.81

174	2020-03-16	22:31:23	62	30.6	10.1	184	244	22:31:23	4.982	0.631	0.82	0.63
175	2020-03-16	22:31:24	62	35.5	10.2	186	245	22:31:24	4.982	0.6221	0.82	0.63
176	2020-03-16	22:31:25	63	34.4	10.2	185	245	22:31:25	4.983	0.6237	0.89	0.75
177	2020-03-16	22:31:26	64	30.6	10.2	184	244	22:31:26	4.983	0.6218	0.9	0.79
178	2020-03-16	22:31:26	64	30.9	10.2	184	244	22:31:26	4.983	0.6218	0.9	0.79
179	2020-03-16	22:31:27	63	31.6	10.1	184	244	22:31:27	4.982	0.6245	0.82	0.63
180	2020-03-16	22:31:28	63	34.5	10.2	185	245	22:31:28	4.982	0.6184	0.82	0.63
181	2020-03-16	22:31:29	63	34.0	10.2	186	246	22:31:29	4.982	0.6161	0.79	0.59
182	2020-03-16	22:31:30	63	39.6	10.2	184	244	22:31:30	4.981	0.6165	0.91	0.79
183	2020-03-16	22:31:31	63	41.1	10.2	186	246	22:31:31	4.983	0.6078	0.9	0.78
184	2020-03-16	22:31:32	63	35.3	10.2	186	246	22:31:32	4.981	0.606	0.81	0.63
185	2020-03-16	22:31:33	63	34.2	10.2	188	248	22:31:33	4.981	0.6029	0.82	0.63
186	2020-03-16	22:31:34	63	32.1	10.2	188	248	22:31:34	4.981	0.6072	0.91	0.8
187	2020-03-16	22:31:35	63	32.2	10.2	187	247	22:31:35	4.977	0.6255	0.9	0.79
188	2020-03-16	22:31:36	63	31.1	10.2	184	244	22:31:36	4.978	0.6259	0.82	0.63
189	2020-03-16	22:31:37	64	36.9	10.2	189	249	22:31:37	4.977	0.6164	0.81	0.63
190	2020-03-16	22:31:38	63	32.5	10.2	188	250	22:31:38	4.98	0.6049	0.81	0.61
191	2020-03-16	22:31:39	63	31.4	10.2	190	250	22:31:39	4.98	0.6072	0.91	0.8
192	2020-03-16	22:31:40	63	32.3	10.2	189	249	22:31:40	4.982	0.6027	0.92	0.81
193	2020-03-16	22:31:41	63	30.9	10.2	187	247	22:31:41	4.982	0.6125	0.8	0.61
194	2020-03-16	22:31:42	62	33.6	10.2	185	245	22:31:42	4.982	0.6147	0.81	0.61
195	2020-03-16	22:31:43	64	41.8	10.2	187	247	22:31:43	4.982	0.6113	0.91	0.8
196	2020-03-16	22:31:44	63	38.0	10.2	187	247	22:31:44	4.983	0.6206	0.92	0.8
197	2020-03-16	22:31:45	62	42.2	10.4	190	250	22:31:45	4.983	0.6219	0.92	0.81
198	2020-03-16	22:31:46	64	31.5	10.2	190	250	22:31:46	4.982	0.6249	0.81	0.63

199	2020-03-16	22:31:46	63	31.6	10.2	189	249	22:31:46	4.982	0.6249	0.81	0.63
200	2020-03-16	22:31:47	63	31.4	10.2	189	249	22:31:47	4.982	0.6328	0.82	0.63
201	2020-03-16	22:31:48	63	31.6	10.2	189	249	22:31:48	4.981	0.631	0.91	0.8
202	2020-03-16	22:31:49	62	31.6	10.2	189	249	22:31:49	4.981	0.6184	0.92	0.81
203	2020-03-16	22:31:50	62	36.8	11.2	189	249	22:31:50	4.982	0.6047	0.81	0.61
204	2020-03-16	22:31:53	62	27.6	10.2	189	249	22:31:53	4.982	0.6145	0.93	0.81
205	2020-03-16	22:31:54	63	31.2	10.2	189	249	22:31:54	4.982	0.6076	0.92	0.81
206	2020-03-16	22:31:55	63	33.9	10.2	189	249	22:31:55	4.979	0.606	0.8	0.61
207	2020-03-16	22:31:56	64	38.6	10.2	189	249	22:31:56	4.981	0.609	0.81	0.61
208	2020-03-16	22:31:57	64	38.5	10.2	189	249	22:31:57	4.982	0.6135	0.91	0.8
209	2020-03-16	22:31:58	63	33.3	10.2	189	249	22:31:58	4.982	0.6076	0.91	0.8
210	2020-03-16	22:31:59	63	30.9	10.2	189	249	22:31:59	4.98	0.6076	0.81	0.61
211	2020-03-16	22:32:00	63	30.7	10.2	189	249	22:32:00	4.983	0.6253	0.79	0.6
212	2020-03-16	22:32:01	62	31.1	10.2	189	249	22:32:01	4.982	0.617	0.78	0.59
213	2020-03-16	22:32:02	64	30.9	10.2	189	249	22:32:02	4.98	0.6298	0.91	0.8
214	2020-03-16	22:32:03	63	31.4	10.2	189	249	22:32:03	4.982	0.6141	0.91	0.8
215	2020-03-16	22:32:04	62	31.0	10.2	189	249	22:32:04	4.983	0.617	0.8	0.61
216	2020-03-16	22:32:05	63	30.5	10.2	189	249	22:32:05	4.983	0.6241	0.81	0.61
217	2020-03-16	22:32:05	64	31.4	10.2	189	249	22:32:05	4.983	0.6241	0.81	0.61
218	2020-03-16	22:32:06	64	31.2	10.2	189	249	22:32:06	4.982	0.6172	0.91	0.81
219	2020-03-16	22:32:07	64	32.5	10.2	189	249	22:32:07	4.983	0.6328	0.91	0.8
220	2020-03-16	22:32:08	65	38.2	10.3	189	249	22:32:08	4.982	0.6204	0.81	0.61
221	2020-03-16	22:32:09	64	38.8	10.2	189	249	22:32:09	4.981	0.6033	0.81	0.61
222	2020-03-16	22:32:10	63	38.2	10.2	190	250	22:32:10	4.983	0.6117	0.81	0.63
223	2020-03-16	22:32:11	64	31.0	10.2	190	250	22:32:11	4.983	0.608	0.9	0.78

224	2020-03-16	22:32:12	63	31.2	10.2	190	250	22:32:12	4.982	0.609	0.91	0.8
225	2020-03-16	22:32:13	62	30.6	10.2	189	249	22:32:13	4.981	0.6139	0.78	0.59
226	2020-03-16	22:32:14	64	31.9	10.2	189	249	22:32:14	4.981	0.6157	0.82	0.63
227	2020-03-16	22:32:15	64	30.4	10.2	189	249	22:32:15	4.98	0.61	0.9	0.79
228	2020-03-16	22:32:16	64	31.1	10.2	189	249	22:32:16	4.98	0.6056	0.9	0.78
229	2020-03-16	22:32:17	63	30.9	10.2	189	249	22:32:17	4.981	0.6045	0.82	0.63
230	2020-03-16	22:32:18	64	30.3	10.2	189	249	22:32:18	4.981	0.6098	0.81	0.61
231	2020-03-16	22:32:19	64	32.6	10.3	189	249	22:32:19	4.982	0.6064	0.81	0.61
232	2020-03-16	22:32:20	64	31.2	10.2	189	249	22:32:20	4.982	0.6041	0.91	0.8
233	2020-03-16	22:32:21	63	33.4	10.2	189	249	22:32:21	4.983	0.608	0.91	0.8
234	2020-03-16	22:32:22	64	37.8	10.2	189	249	22:32:22	4.984	0.6108	0.81	0.61
235	2020-03-16	22:32:23	63	38.6	10.1	181	241	22:32:23	4.983	0.6237	0.8	0.61
236	2020-03-16	22:32:24	64	38.5	11.3	177	237	22:32:24	4.983	0.6274	0.91	0.8
237	2020-03-16	22:32:24	64	32.2	10.9	176	236	22:32:25	4.983	0.6261	0.91	0.81
238	2020-03-16	22:32:25	63	31.7	10.4	176	236	22:32:26	4.982	0.6322	0.92	0.81
239	2020-03-16	22:32:27	64	29.6	10.0	171	231	22:32:27	4.982	0.6274	0.8	0.6
240	2020-03-16	22:32:28	63	31.3	10.0	171	231	22:32:28	4.982	0.6186	0.79	0.6
241	2020-03-16	22:32:29	64	30.8	9.9	170	230	22:32:29	4.983	0.6172	0.89	0.76
242	2020-03-16	22:32:30	64	30.3	10.0	170	230	22:32:30	4.983	0.6084	0.92	0.81
243	2020-03-16	22:32:31	64	30.9	9.9	170	230	22:32:31	4.983	0.6104	0.78	0.59
244	2020-03-16	22:32:32	63	31.0	10.0	170	230	22:32:32	4.983	0.606	0.8	0.61
245	2020-03-16	22:32:33	63	30.4	10.0	170	230	22:32:33	4.981	0.6084	0.91	0.8
246	2020-03-16	22:32:34	63	35.3	9.9	170	231	22:32:34	4.981	0.6051	0.92	0.81
247	2020-03-16	22:32:35	63	38.2	9.9	170	230	22:32:35	4.981	0.6102	0.92	0.81
248	2020-03-16	22:32:36	64	38.0	9.9	170	230	22:32:36	4.982	0.6168	0.81	0.61

249	2020-03-16	22:32:36	63	31.4	9.9	170	230	22:32:36	4.982	0.6168	0.81	0.61
250	2020-03-16	22:32:37	63	30.7	9.9	170	230	22:32:37	4.982	0.6068	0.81	0.61
251	2020-03-16	22:32:38	64	30.4	9.9	170	230	22:32:38	4.983	0.611	0.92	0.81
252	2020-03-16	22:32:39	65	30.9	9.9	170	230	22:32:39	4.982	0.6149	0.87	0.73
253	2020-03-16	22:32:40	64	30.9	9.9	170	230	22:32:40	4.982	0.6379	0.81	0.61
254	2020-03-16	22:32:41	64	30.3	9.9	170	230	22:32:41	4.983	0.6367	0.8	0.61
255	2020-03-16	22:32:42	64	31.0	9.9	170	230	22:32:42	4.982	0.6377	0.81	0.61
256	2020-03-16	22:32:43	63	31.0	9.9	170	230	22:32:43	4.982	0.6373	0.91	0.8
257	2020-03-16	22:32:44	63	31.4	9.9	170	230	22:32:44	4.983	0.6088	0.91	0.8
258	2020-03-16	22:32:45	63	31.8	10.0	170	230	22:32:45	4.983	0.6086	0.81	0.61
259	2020-03-16	22:32:46	64	31.6	9.9	170	230	22:32:46	4.982	0.6076	0.8	0.61
260	2020-03-16	22:32:47	63	39.0	10.0	170	230	22:32:47	4.982	0.6078	0.91	0.8
261	2020-03-16	22:32:48	64	38.0	10.0	170	230	22:32:48	4.982	0.6077	0.9	0.79
262	2020-03-16	22:32:49	65	36.2	9.9	170	230	22:32:49	4.981	0.6079	0.79	0.6
263	2020-03-16	22:32:50	64	30.4	9.9	170	230	22:32:50	4.983	0.6062	0.77	0.59
264	2020-03-16	22:32:51	64	30.9	10.0	170	230	22:32:51	4.984	0.6263	0.82	0.64
265	2020-03-16	22:32:52	63	34.5	10.2	170	230	22:32:52	4.982	0.6243	0.9	0.79
266	2020-03-16	22:32:53	62	32.0	10.0	170	230	22:32:53	4.982	0.6288	0.9	0.79
267	2020-03-16	22:32:53	65	30.8	10.0	170	230	22:32:53	4.982	0.6288	0.9	0.79
268	2020-03-16	22:32:54	63	31.4	9.9	170	230	22:32:54	4.984	0.6278	0.82	0.64
269	2020-03-16	22:32:55	65	30.3	10.0	170	230	22:32:55	4.983	0.6241	0.81	0.61
270	2020-03-16	22:32:56	64	35.1	10.8	170	230	22:32:56	4.983	0.6257	0.91	0.8
271	2020-03-16	22:32:57	64	31.2	10.4	170	230	22:32:57	4.984	0.6102	0.92	0.81
272	2020-03-16	22:32:58	63	31.1	10.0	171	231	22:32:58	4.984	0.6098	0.81	0.62
273	2020-03-16	22:32:59	63	34.1	10.0	171	231	22:32:59	4.984	0.6094	0.81	0.61

274	2020-03-16	22:33:00	64	38.0	10.0	171	231	22:33:00	4.983	0.6097	0.81	0.61
275	2020-03-16	22:33:01	65	38.4	9.9	171	231	22:33:01	4.983	0.6093	0.92	0.81
276	2020-03-16	22:33:02	64	32.7	10.0	171	231	22:33:02	4.983	0.6082	0.9	0.78
277	2020-03-16	22:33:03	63	31.0	10.0	171	231	22:33:03	4.982	0.6108	0.81	0.61
278	2020-03-16	22:33:04	63	31.9	10.0	171	231	22:33:04	4.981	0.6184	0.8	0.61
279	2020-03-16	22:33:05	63	32.3	10.0	171	231	22:33:05	4.98	0.6251	0.87	0.7
280	2020-03-16	22:33:06	64	31.4	10.0	171	231	22:33:06	4.98	0.617	0.9	0.79
281	2020-03-16	22:33:07	64	30.3	9.9	171	232	22:33:07	4.982	0.6058	0.9	0.79
282	2020-03-16	22:33:08	64	31.0	10.0	171	231	22:33:08	4.983	0.6123	0.78	0.59
283	2020-03-16	22:33:09	63	30.7	10.0	171	231	22:33:09	4.982	0.6271	0.8	0.63
284	2020-03-16	22:33:10	64	30.8	10.0	171	231	22:33:10	4.982	0.6239	0.9	0.79
285	2020-03-16	22:33:10	64	30.4	10.0	171	231	22:33:10	4.982	0.6239	0.9	0.79
286	2020-03-16	22:33:11	65	30.5	10.0	171	231	22:33:11	4.983	0.6274	0.9	0.79
287	2020-03-16	22:33:12	64	37.6	10.0	171	232	22:33:12	4.984	0.6294	0.79	0.6
288	2020-03-16	22:33:13	65	38.3	10.0	171	231	22:33:13	4.984	0.6241	0.81	0.61
289	2020-03-16	22:33:14	64	37.2	10.0	171	231	22:33:14	4.982	0.6312	0.91	0.8
290	2020-03-16	22:33:15	64	30.9	10.0	171	231	22:33:15	4.983	0.617	0.91	0.81
291	2020-03-16	22:33:16	64	30.7	10.0	171	231	22:33:16	4.982	0.6145	0.92	0.81
292	2020-03-16	22:33:17	63	30.7	10.0	171	231	22:33:17	4.982	0.619	0.81	0.61
293	2020-03-16	22:33:18	64	31.0	10.0	171	231	22:33:18	4.981	0.6191	0.81	0.61
294	2020-03-16	22:33:19	64	31.0	10.0	171	231	22:33:19	4.981	0.6123	0.91	0.8
295	2020-03-16	22:33:20	64	30.6	10.0	171	231	22:33:20	4.982	0.6082	0.92	0.81
296	2020-03-16	22:33:21	64	31.4	10.0	171	231	22:33:21	4.982	0.6104	0.81	0.61
297	2020-03-16	22:33:22	64	31.0	10.0	171	231	22:33:22	4.982	0.61	0.81	0.62
298	2020-03-16	22:33:23	64	31.6	10.0	171	231	22:33:23	4.982	0.6119	0.9	0.79

299	2020-03-16	22:33:24	64	32.9	10.0	171	231	22:33:24	4.983	0.6116	0.9	0.77
300	2020-03-16	22:33:25	64	34.0	10.0	171	232	22:33:25	4.983	0.6151	0.9	0.79
301	2020-03-16	22:33:26	64	38.5	10.0	172	232	22:33:26	4.983	0.6206	0.81	0.63
302	2020-03-16	22:33:27	65	38.8	10.0	172	232	22:33:27	4.984	0.6318	0.79	0.6
303	2020-03-16	22:33:28	64	33.0	10.0	172	232	22:33:28	4.984	0.6355	0.83	0.64
304	2020-03-16	22:33:28	64	30.6	10.0	171	231	22:33:29	4.983	0.6328	0.9	0.79
305	2020-03-16	22:33:29	64	35.8	11.1	171	231	22:33:30	4.982	0.6402	0.79	0.6
306	2020-03-16	22:33:30	65	31.3	10.7	171	231	22:33:31	4.982	0.6341	0.79	0.6
307	2020-03-16	22:33:33	64	28.0	10.0	171	231	22:33:32	4.982	0.6168	0.81	0.62
308	2020-03-16	22:33:34	64	30.6	10.0	171	231	22:33:33	4.984	0.6082	0.9	0.79
309	2020-03-16	22:33:35	63	31.0	10.0	171	231	22:33:34	4.983	0.608	0.9	0.79
310	2020-03-16	22:33:36	65	30.4	10.0	171	231	22:33:35	4.982	0.6108	0.79	0.6
311	2020-03-16	22:33:37	64	30.9	10.0	171	231	22:33:36	4.981	0.6066	0.8	0.62
312	2020-03-16	22:33:37	65	33.6	10.0	171	231	22:33:37	4.982	0.6082	0.9	0.79
313	2020-03-16	22:33:38	64	37.9	10.0	171	231	22:33:38	4.981	0.6081	0.9	0.78
314	2020-03-16	22:33:39	65	38.0	10.0	171	231	22:33:39	4.982	0.6081	0.81	0.62
315	2020-03-16	22:33:40	64	33.4	10.0	171	231	22:33:40	4.982	0.6053	0.77	0.58
316	2020-03-16	22:33:41	64	31.3	10.0	171	231	22:33:41	4.983	0.6282	0.82	0.64
317	2020-03-16	22:33:42	65	31.4	10.0	171	231	22:33:42	4.982	0.6253	0.9	0.79
318	2020-03-16	22:33:43	64	31.9	10.0	169	229	22:33:43	4.982	0.6294	0.91	0.8
319	2020-03-16	22:33:44	65	31.2	9.9	166	226	22:33:44	4.983	0.6349	0.79	0.6
320	2020-03-16	22:33:45	63	30.9	9.9	166	226	22:33:45	4.983	0.6251	0.79	0.6
321	2020-03-16	22:33:46	64	30.7	9.9	166	226	22:33:46	4.983	0.6276	0.9	0.78
322	2020-03-16	22:33:47	64	31.0	9.9	166	226	22:33:47	4.98	0.6369	0.82	0.63
323	2020-03-16	22:33:48	64	30.4	9.9	166	226	22:33:48	4.982	0.6343	0.9	0.79

324	2020-03-16	22:33:49	64	30.4	9.9	166	226	22:33:49	4.983	0.6078	0.81	0.61
325	2020-03-16	22:33:50	64	30.7	9.9	166	226	22:33:50	4.983	0.6092	0.81	0.61
326	2020-03-16	22:33:51	65	37.0	9.9	166	226	22:33:51	4.984	0.6127	0.91	0.8
327	2020-03-16	22:33:52	64	38.4	9.9	166	226	22:33:52	4.983	0.6223	0.91	0.81
328	2020-03-16	22:33:53	64	37.4	9.9	166	226	22:33:53	4.983	0.6226	0.81	0.61
329	2020-03-16	22:33:53	65	31.4	9.9	166	226	22:33:53	4.983	0.6226	0.81	0.61
330	2020-03-16	22:33:54	65	30.9	9.9	166	226	22:33:54	4.983	0.6276	0.8	0.61
331	2020-03-16	22:33:55	64	30.9	9.9	166	226	22:33:55	4.984	0.6388	0.91	0.8
332	2020-03-16	22:33:56	64	30.7	9.9	166	226	22:33:56	4.982	0.6385	0.91	0.8
333	2020-03-16	22:33:57	64	32.6	9.9	166	226	22:33:57	4.983	0.6343	0.92	0.81
334	2020-03-16	22:33:58	65	31.1	9.9	166	226	22:33:58	4.983	0.6155	0.79	0.6
335	2020-03-16	22:33:59	64	30.9	9.9	166	226	22:33:59	4.984	0.6092	0.81	0.61
336	2020-03-16	22:34:00	64	31.9	9.9	166	226	22:34:00	4.983	0.6078	0.91	0.8

Run-Dictionary attack - 25°C												
	Date	T.Stamp	Temp	CPU_Load	Mem_Load	ProNo,	ThreadsNo	Time	Voltage(V)	Current(A)	D+(V)	D-(V)
1	2020-03-21	20:31:30	51	13.8	9.4	164	224	20:31:30	4.993	0.5837	0.8	0.62
2	2020-03-21	20:31:31	51	21.0	9.4	164	224	20:31:31	4.992	0.5966	0.8	0.61
3	2020-03-21	20:31:32	52	17.8	9.4	164	224	20:31:32	4.989	0.6005	0.85	0.68
4	2020-03-21	20:31:33	52	13.3	9.4	164	224	20:31:33	4.991	0.5921	0.79	0.62
5	2020-03-21	20:31:34	52	12.5	9.4	164	224	20:31:34	4.99	0.5835	0.82	0.65
6	2020-03-21	20:31:35	51	12.2	9.4	164	224	20:31:35	4.991	0.5817	0.91	0.8
7	2020-03-21	20:31:36	51	11.9	9.4	164	224	20:31:36	4.991	0.5814	0.91	0.8
8	2020-03-21	20:31:37	51	6.9	9.4	164	224	20:31:37	4.99	0.5774	0.79	0.59
9	2020-03-21	20:31:38	52	6.5	9.4	164	224	20:31:38	4.991	0.5666	0.8	0.61
10	2020-03-21	20:31:39	51	6.9	9.4	164	224	20:31:39	4.99	0.5807	0.79	0.61
11	2020-03-21	20:31:40	52	10.4	9.4	164	224	20:31:40	4.989	0.5974	0.86	0.71
12	2020-03-21	20:31:41	51	7.5	9.4	164	224	20:31:41	4.991	0.5785	0.88	0.73
13	2020-03-21	20:31:42	51	10.0	9.4	164	224	20:31:42	4.991	0.5805	0.79	0.6
14	2020-03-21	20:31:43	53	12.5	9.4	164	224	20:31:43	4.991	0.5929	0.8	0.6
15	2020-03-21	20:31:44	51	16.3	9.4	164	224	20:31:44	4.991	0.5943	0.91	0.8
16	2020-03-21	20:31:45	51	14.8	9.4	164	224	20:31:45	4.991	0.5821	0.91	0.8
17	2020-03-21	20:31:46	52	13.3	9.7	164	224	20:31:46	4.992	0.5852	0.91	0.8
18	2020-03-21	20:31:47	51	7.7	9.4	164	224	20:31:47	4.991	0.5785	0.8	0.6
19	2020-03-21	20:31:48	51	7.4	9.4	164	225	20:31:48	4.992	0.586	0.79	0.59
20	2020-03-21	20:31:49	51	10.3	9.4	164	224	20:31:49	4.991	0.5758	0.86	0.71
21	2020-03-21	20:31:50	51	8.9	9.4	164	224	20:31:50	4.993	0.5921	0.9	0.78
22	2020-03-21	20:31:51	52	7.5	9.4	164	224	20:31:51	4.992	0.5748	0.82	0.64
23	2020-03-21	20:31:52	52	17.8	10.5	164	225	20:31:52	4.99	0.5705	0.78	0.6

24	2020-03-21	20:31:53	50	15.8	10.2	164	225	20:31:53	4.991	0.5966	0.8	0.61
25	2020-03-21	20:31:53	52	18.7	9.9	164	225	20:31:54	4.991	0.5939	0.82	0.64
26	2020-03-21	20:31:54	51	19.5	9.7	163	223	20:31:55	4.991	0.6056	0.91	0.8
27	2020-03-21	20:31:56	52	23.1	9.4	163	223	20:31:56	4.991	0.6055	0.79	0.59
28	2020-03-21	20:31:57	52	24.7	9.4	163	223	20:31:57	4.99	0.6076	0.79	0.6
29	2020-03-21	20:31:58	53	7.5	9.4	164	224	20:31:58	4.991	0.6021	0.88	0.73
30	2020-03-21	20:31:59	52	7.2	9.4	164	225	20:31:59	4.991	0.5846	0.85	0.68
31	2020-03-21	20:32:00	52	13.5	9.4	164	225	20:32:00	4.992	0.5783	0.76	0.58
32	2020-03-21	20:32:01	53	19.0	9.4	164	224	20:32:01	4.991	0.5937	0.78	0.59
33	2020-03-21	20:32:02	52	16.8	9.4	164	225	20:32:02	4.991	0.5923	0.82	0.64
34	2020-03-21	20:32:03	52	16.8	9.4	164	224	20:32:03	4.991	0.589	0.86	0.7
35	2020-03-21	20:32:04	53	14.9	9.4	164	224	20:32:04	4.992	0.5893	0.86	0.7
36	2020-03-21	20:32:05	52	14.2	9.4	164	224	20:32:05	4.992	0.5894	0.8	0.6
37	2020-03-21	20:32:06	52	13.8	9.4	164	225	20:32:06	4.992	0.5872	0.8	0.61
38	2020-03-21	20:32:07	52	13.8	9.4	164	224	20:32:07	4.995	0.5875	0.91	0.8
39	2020-03-21	20:32:08	52	12.0	9.5	164	224	20:32:08	4.994	0.5842	0.91	0.8
40	2020-03-21	20:32:08	53	12.4	9.5	164	224	20:32:09	4.993	0.5756	0.8	0.6
41	2020-03-21	20:32:09	51	13.6	9.5	164	224	20:32:10	4.994	0.5811	0.8	0.61
42	2020-03-21	20:32:10	52	9.1	9.4	164	224	20:32:11	4.994	0.5935	0.8	0.6
43	2020-03-21	20:32:11	52	6.9	9.4	164	224	20:32:12	4.994	0.5907	0.86	0.7
44	2020-03-21	20:32:12	52	7.1	9.4	164	224	20:32:13	4.993	0.5748	0.85	0.68
45	2020-03-21	20:32:13	52	9.0	9.4	164	224	20:32:14	4.994	0.5858	0.81	0.62
46	2020-03-21	20:32:14	52	9.8	9.5	164	224	20:32:15	4.994	0.5742	0.8	0.62
47	2020-03-21	20:32:15	52	30.2	9.4	164	224	20:32:16	4.99	0.5864	0.85	0.67
48	2020-03-21	20:32:16	53	35.8	9.5	164	224	20:32:17	4.99	0.6273	0.84	0.66

49	2020-03-21	20:32:17	54	59.7	9.9	204	264	20:32:18	4.985	0.6359	0.78	0.59
50	2020-03-21	20:32:18	53	32.3	9.9	204	264	20:32:19	4.99	0.6506	0.76	0.59
51	2020-03-21	20:32:19	55	40.0	10.0	204	264	20:32:20	4.988	0.6408	0.8	0.61
52	2020-03-21	20:32:20	55	34.2	9.9	204	265	20:32:21	4.989	0.6557	0.9	0.77
53	2020-03-21	20:32:21	54	41.7	9.9	205	265	20:32:22	4.989	0.675	0.9	0.79
54	2020-03-21	20:32:22	55	42.0	9.9	205	265	20:32:23	4.989	0.6555	0.79	0.59
55	2020-03-21	20:32:23	55	33.7	9.9	205	265	20:32:24	4.989	0.6314	0.8	0.62
56	2020-03-21	20:32:24	55	41.2	10.9	205	265	20:32:25	4.988	0.6312	0.9	0.78
57	2020-03-21	20:32:25	54	32.9	10.7	205	265	20:32:26	4.988	0.6351	0.91	0.8
58	2020-03-21	20:32:27	55	30.1	9.9	209	269	20:32:27	4.989	0.6339	0.91	0.8
59	2020-03-21	20:32:28	55	34.7	9.9	210	270	20:32:28	4.99	0.6227	0.8	0.61
60	2020-03-21	20:32:29	55	30.6	9.9	210	270	20:32:29	4.989	0.6459	0.8	0.6
61	2020-03-21	20:32:30	55	34.2	9.9	210	270	20:32:30	4.99	0.6333	0.92	0.81
62	2020-03-21	20:32:31	55	34.2	9.9	210	270	20:32:31	4.989	0.6302	0.91	0.8
63	2020-03-21	20:32:32	55	30.3	9.9	210	270	20:32:32	4.99	0.632	0.8	0.6
64	2020-03-21	20:32:33	56	43.8	9.5	178	238	20:32:33	4.989	0.6229	0.8	0.6
65	2020-03-21	20:32:34	55	37.8	9.5	178	238	20:32:34	4.988	0.6445	0.92	0.81
66	2020-03-21	20:32:35	55	37.8	9.5	178	238	20:32:35	4.988	0.632	0.82	0.63
67	2020-03-21	20:32:36	57	33.9	9.5	178	238	20:32:36	4.988	0.6316	0.87	0.71
68	2020-03-21	20:32:37	56	31.0	9.5	178	238	20:32:37	4.989	0.6257	0.78	0.59
69	2020-03-21	20:32:38	57	30.8	9.5	178	238	20:32:38	4.989	0.6221	0.75	0.57
70	2020-03-21	20:32:38	56	30.8	9.5	178	238	20:32:38	4.989	0.6221	0.75	0.57
71	2020-03-21	20:32:39	55	30.3	9.5	178	238	20:32:39	4.99	0.6202	0.91	0.8
72	2020-03-21	20:32:40	56	31.0	9.5	178	238	20:32:40	4.991	0.6205	0.91	0.8
73	2020-03-21	20:32:41	57	30.5	9.5	178	238	20:32:41	4.991	0.6349	0.77	0.58

74	2020-03-21	20:32:42	56	31.0	9.5	178	238	20:32:42	4.991	0.6402	0.8	0.6
75	2020-03-21	20:32:43	55	31.0	9.5	178	238	20:32:43	4.99	0.6406	0.8	0.61
76	2020-03-21	20:32:44	56	31.0	9.5	178	238	20:32:44	4.99	0.642	0.91	0.8
77	2020-03-21	20:32:45	55	30.4	9.5	178	238	20:32:45	4.991	0.6294	0.92	0.8
78	2020-03-21	20:32:46	56	34.7	9.5	178	238	20:32:46	4.989	0.6225	0.77	0.59
79	2020-03-21	20:32:47	57	38.5	9.5	178	238	20:32:47	4.989	0.6294	0.77	0.59
80	2020-03-21	20:32:48	56	38.5	9.5	178	238	20:32:48	4.989	0.6341	0.86	0.7
81	2020-03-21	20:32:49	57	32.2	9.5	178	238	20:32:49	4.988	0.6329	0.88	0.74
82	2020-03-21	20:32:50	56	30.4	9.5	178	238	20:32:50	4.99	0.6216	0.77	0.59
83	2020-03-21	20:32:51	55	30.2	9.5	178	238	20:32:51	4.99	0.6219	0.81	0.63
84	2020-03-21	20:32:52	56	30.3	9.5	178	238	20:32:52	4.991	0.6196	0.77	0.58
85	2020-03-21	20:32:52	56	30.4	9.5	178	238	20:32:52	4.991	0.6196	0.77	0.58
86	2020-03-21	20:32:53	56	32.2	9.6	178	238	20:32:53	4.991	0.6229	0.91	0.79
87	2020-03-21	20:32:54	56	30.5	9.5	178	238	20:32:54	4.991	0.6245	0.82	0.63
88	2020-03-21	20:32:55	55	30.5	9.5	178	238	20:32:55	4.991	0.6473	0.81	0.63
89	2020-03-21	20:32:56	56	30.2	9.5	178	238	20:32:56	4.991	0.641	0.81	0.62
90	2020-03-21	20:32:57	56	30.6	9.5	178	238	20:32:57	4.991	0.6412	0.82	0.63
91	2020-03-21	20:32:58	57	32.3	10.0	178	238	20:32:58	4.991	0.629	0.89	0.75
92	2020-03-21	20:32:59	56	40.7	10.4	178	238	20:32:59	4.991	0.6219	0.77	0.58
93	2020-03-21	20:33:00	57	38.2	10.0	178	238	20:33:00	4.988	0.6489	0.77	0.59
94	2020-03-21	20:33:01	56	37.5	9.5	178	238	20:33:01	4.988	0.6439	0.77	0.59
95	2020-03-21	20:33:02	58	30.4	9.5	178	238	20:33:02	4.988	0.6442	0.85	0.68
96	2020-03-21	20:33:03	57	60.6	9.9	210	270	20:33:03	4.989	0.6229	0.87	0.71
97	2020-03-21	20:33:04	57	30.9	9.9	210	270	20:33:04	4.987	0.6599	0.79	0.62
98	2020-03-21	20:33:05	57	34.0	10.0	210	270	20:33:05	4.99	0.6223	0.81	0.61

99	2020-03-21	20:33:06	58	35.0	10.0	210	270	20:33:06	4.99	0.6351	0.91	0.8
100	2020-03-21	20:33:07	58	31.0	10.0	210	270	20:33:07	4.99	0.6216	0.91	0.8
101	2020-03-21	20:33:07	57	38.1	9.9	210	270	20:33:07	4.99	0.6216	0.91	0.8
102	2020-03-21	20:33:08	57	31.6	10.0	210	270	20:33:08	4.991	0.6204	0.81	0.61
103	2020-03-21	20:33:09	58	38.8	10.0	210	270	20:33:09	4.991	0.6312	0.8	0.61
104	2020-03-21	20:33:10	57	30.7	10.0	210	270	20:33:10	4.989	0.6371	0.8	0.61
105	2020-03-21	20:33:11	58	36.6	10.0	210	270	20:33:11	4.991	0.6489	0.9	0.79
106	2020-03-21	20:33:12	57	42.0	10.0	210	270	20:33:12	4.991	0.6388	0.88	0.72
107	2020-03-21	20:33:13	57	38.6	10.0	210	270	20:33:13	4.989	0.653	0.78	0.59
108	2020-03-21	20:33:14	57	43.3	10.0	212	272	20:33:14	4.99	0.6544	0.78	0.59
109	2020-03-21	20:33:15	58	30.7	10.0	212	272	20:33:15	4.99	0.6455	0.86	0.7
110	2020-03-21	20:33:16	58	40.3	9.6	180	240	20:33:16	4.991	0.6251	0.83	0.64
111	2020-03-21	20:33:17	58	30.5	9.5	180	240	20:33:17	4.989	0.6386	0.84	0.66
112	2020-03-21	20:33:18	58	30.5	9.5	179	239	20:33:18	4.99	0.6263	0.81	0.63
113	2020-03-21	20:33:19	57	30.7	9.5	179	239	20:33:19	4.989	0.6237	0.8	0.6
114	2020-03-21	20:33:20	57	30.5	9.5	179	239	20:33:20	4.99	0.63	0.91	0.8
115	2020-03-21	20:33:21	57	30.3	9.5	179	239	20:33:21	4.989	0.6237	0.91	0.8
116	2020-03-21	20:33:22	58	30.3	9.5	179	239	20:33:22	4.991	0.6236	0.8	0.61
117	2020-03-21	20:33:23	56	31.1	9.5	179	239	20:33:23	4.991	0.6231	0.8	0.6
118	2020-03-21	20:33:23	57	30.1	9.5	179	239	20:33:23	4.991	0.6231	0.8	0.6
119	2020-03-21	20:33:24	57	35.4	9.5	179	239	20:33:24	4.991	0.6269	0.91	0.8
120	2020-03-21	20:33:25	57	37.9	9.5	179	239	20:33:25	4.99	0.6324	0.91	0.8
121	2020-03-21	20:33:26	58	39.2	9.6	180	240	20:33:26	4.989	0.6485	0.89	0.76
122	2020-03-21	20:33:27	58	31.5	9.5	180	240	20:33:27	4.989	0.6612	0.77	0.58
123	2020-03-21	20:33:28	58	30.8	9.5	180	240	20:33:28	4.991	0.6687	0.77	0.58

124	2020-03-21	20:33:29	58	30.6	9.5	180	240	20:33:29	4.991	0.6386	0.88	0.73
125	2020-03-21	20:33:30	57	30.5	9.5	180	240	20:33:30	4.991	0.6333	0.85	0.67
126	2020-03-21	20:33:31	58	30.7	9.5	179	239	20:33:31	4.99	0.6367	0.78	0.6
127	2020-03-21	20:33:32	58	35.8	10.5	179	239	20:33:32	4.989	0.6239	0.78	0.59
128	2020-03-21	20:33:33	58	32.7	10.0	180	240	20:33:33	4.988	0.6349	0.82	0.63
129	2020-03-21	20:33:34	57	31.8	9.5	180	240	20:33:34	4.988	0.635	0.91	0.8
130	2020-03-21	20:33:35	57	30.7	9.5	180	240	20:33:35	4.99	0.6335	0.91	0.8
131	2020-03-21	20:33:36	57	31.0	9.5	180	240	20:33:36	4.989	0.6202	0.8	0.6
132	2020-03-21	20:33:37	58	30.9	9.5	180	240	20:33:37	4.991	0.6192	0.8	0.61
133	2020-03-21	20:33:37	58	37.4	9.6	180	240	20:33:37	4.991	0.6192	0.8	0.61
134	2020-03-21	20:33:38	58	38.0	9.6	180	240	20:33:38	4.989	0.6194	0.92	0.8
135	2020-03-21	20:33:39	58	36.6	9.5	180	240	20:33:39	4.99	0.6373	0.91	0.8
136	2020-03-21	20:33:40	58	30.9	9.5	180	240	20:33:40	4.989	0.6502	0.81	0.61
137	2020-03-21	20:33:41	58	30.8	9.5	180	240	20:33:41	4.991	0.6396	0.8	0.61
138	2020-03-21	20:33:42	58	30.2	9.5	180	240	20:33:42	4.991	0.6397	0.79	0.6
139	2020-03-21	20:33:43	58	31.1	9.6	180	240	20:33:43	4.991	0.6253	0.91	0.8
140	2020-03-21	20:33:44	58	31.2	9.5	180	240	20:33:44	4.99	0.6214	0.91	0.8
141	2020-03-21	20:33:45	58	31.5	9.5	180	240	20:33:45	4.989	0.6216	0.8	0.6
142	2020-03-21	20:33:46	58	52.2	10.0	198	271	20:33:46	4.989	0.6196	0.79	0.6
143	2020-03-21	20:33:47	59	33.6	10.0	212	272	20:33:47	4.985	0.6192	0.91	0.8
144	2020-03-21	20:33:48	59	30.6	10.0	212	272	20:33:48	4.99	0.6386	0.91	0.8
145	2020-03-21	20:33:49	59	37.5	10.0	212	272	20:33:49	4.989	0.6221	0.8	0.61
146	2020-03-21	20:33:50	58	34.1	10.0	212	272	20:33:50	4.989	0.6324	0.78	0.59
147	2020-03-21	20:33:51	59	41.7	10.0	212	272	20:33:51	4.988	0.6237	0.81	0.61
148	2020-03-21	20:33:52	59	37.9	10.0	213	273	20:33:52	4.988	0.6326	0.91	0.8

149	2020-03-21	20:33:53	59	44.5	10.0	207	271	20:33:53	4.989	0.6349	0.9	0.79
150	2020-03-21	20:33:54	59	36.4	10.0	213	273	20:33:54	4.987	0.6229	0.79	0.6
151	2020-03-21	20:33:55	59	32.9	10.0	213	273	20:33:55	4.99	0.6314	0.81	0.61
152	2020-03-21	20:33:56	59	32.5	10.0	212	272	20:33:56	4.99	0.631	0.91	0.8
153	2020-03-21	20:33:57	58	31.0	10.0	212	272	20:33:57	4.991	0.6233	0.92	0.8
154	2020-03-21	20:33:58	59	51.2	10.0	212	273	20:33:58	4.991	0.6273	0.81	0.61
155	2020-03-21	20:33:59	59	31.8	10.0	212	272	20:33:59	4.991	0.6913	0.8	0.6
156	2020-03-21	20:34:00	59	35.2	10.0	212	272	20:34:00	4.991	0.6269	0.8	0.6
157	2020-03-21	20:34:00	59	33.2	10.0	212	272	20:34:00	4.991	0.6269	0.8	0.6
158	2020-03-21	20:34:01	58	31.5	10.0	212	272	20:34:01	4.99	0.6536	0.89	0.74
159	2020-03-21	20:34:02	59	34.1	10.0	212	272	20:34:02	4.991	0.6345	0.85	0.69
160	2020-03-21	20:34:03	59	39.2	10.0	212	272	20:34:03	4.991	0.6398	0.77	0.58
161	2020-03-21	20:34:04	60	43.7	11.3	212	272	20:34:04	4.989	0.6508	0.78	0.59
162	2020-03-21	20:34:05	59	40.4	11.0	212	272	20:34:05	4.989	0.6544	0.89	0.75
163	2020-03-21	20:34:06	59	31.4	10.5	212	272	20:34:06	4.988	0.6608	0.85	0.68
164	2020-03-21	20:34:07	58	33.3	10.1	212	272	20:34:07	4.989	0.6439	0.82	0.63
165	2020-03-21	20:34:08	58	36.1	10.0	212	272	20:34:08	4.989	0.6351	0.77	0.59
166	2020-03-21	20:34:09	59	30.7	10.0	212	272	20:34:09	4.99	0.6377	0.77	0.58
167	2020-03-21	20:34:10	59	34.1	10.0	212	272	20:34:10	4.989	0.6204	0.83	0.64
168	2020-03-21	20:34:11	58	31.2	10.0	212	272	20:34:11	4.989	0.6269	0.9	0.78
169	2020-03-21	20:34:12	59	36.5	10.0	210	270	20:34:12	4.988	0.6212	0.8	0.6
170	2020-03-21	20:34:13	58	31.6	10.0	208	268	20:34:13	4.989	0.6253	0.81	0.61
171	2020-03-21	20:34:14	59	35.0	9.9	208	258	20:34:14	4.99	0.6218	0.91	0.8
172	2020-03-21	20:34:15	60	32.8	9.8	198	258	20:34:15	4.99	0.6214	0.91	0.8
173	2020-03-21	20:34:16	59	35.2	9.8	198	258	20:34:16	4.991	0.6255	0.92	0.81

174	2020-03-21	20:34:17	60	42.3	9.6	180	240	20:34:17	4.99	0.6337	0.8	0.61
175	2020-03-21	20:34:17	59	39.0	9.6	180	240	20:34:17	4.99	0.6337	0.8	0.61
176	2020-03-21	20:34:18	60	31.1	9.6	180	240	20:34:18	4.99	0.6534	0.81	0.61
177	2020-03-21	20:34:19	59	30.5	9.6	180	240	20:34:19	4.991	0.6449	0.91	0.8
178	2020-03-21	20:34:20	60	31.0	9.6	180	240	20:34:20	4.991	0.6412	0.89	0.75
179	2020-03-21	20:34:21	60	30.3	9.6	180	240	20:34:21	4.991	0.6424	0.81	0.63
180	2020-03-21	20:34:22	60	30.4	9.6	180	240	20:34:22	4.991	0.6392	0.81	0.63
181	2020-03-21	20:34:23	60	30.6	9.6	180	240	20:34:23	4.99	0.6239	0.85	0.67
182	2020-03-21	20:34:24	60	30.6	9.6	180	240	20:34:24	4.99	0.6206	0.91	0.79
183	2020-03-21	20:34:25	59	30.3	9.6	180	240	20:34:25	4.989	0.6202	0.9	0.78
184	2020-03-21	20:34:26	60	30.7	9.6	180	240	20:34:26	4.988	0.6218	0.82	0.63
185	2020-03-21	20:34:27	59	30.6	9.6	180	240	20:34:27	4.988	0.6269	0.77	0.59
186	2020-03-21	20:34:28	60	30.5	9.6	180	240	20:34:28	4.989	0.6237	0.82	0.63
187	2020-03-21	20:34:29	60	37.2	9.6	180	240	20:34:29	4.989	0.6276	0.91	0.8
188	2020-03-21	20:34:30	61	37.5	9.6	180	240	20:34:30	4.99	0.6379	0.8	0.6
189	2020-03-21	20:34:31	59	36.7	9.6	180	240	20:34:31	4.989	0.6378	0.8	0.6
190	2020-03-21	20:34:31	59	30.5	9.6	180	240	20:34:31	4.989	0.6378	0.8	0.6
191	2020-03-21	20:34:32	60	32.6	9.6	180	240	20:34:32	4.99	0.6457	0.81	0.61
192	2020-03-21	20:34:33	59	30.5	9.6	180	240	20:34:33	4.989	0.6432	0.91	0.8
193	2020-03-21	20:34:34	61	30.9	9.6	180	240	20:34:34	4.99	0.651	0.91	0.8
194	2020-03-21	20:34:35	60	30.3	9.6	180	240	20:34:35	4.99	0.6441	0.8	0.6
195	2020-03-21	20:34:36	60	31.3	9.6	180	240	20:34:36	4.99	0.6353	0.8	0.61
196	2020-03-21	20:34:37	59	34.8	10.6	180	240	20:34:37	4.99	0.6302	0.9	0.77
197	2020-03-21	20:34:38	58	32.3	10.4	180	240	20:34:38	4.988	0.6284	0.91	0.8
198	2020-03-21	20:34:39	59	31.0	10.0	180	240	20:34:39	4.988	0.6404	0.92	0.81

199	2020-03-21	20:34:40	60	30.5	9.7	180	240	20:34:40	4.987	0.6422	0.8	0.6
200	2020-03-21	20:34:41	59	33.3	9.6	180	240	20:34:41	4.988	0.6367	0.8	0.61
201	2020-03-21	20:34:42	60	40.3	9.6	183	243	20:34:42	4.989	0.6269	0.91	0.8
202	2020-03-21	20:34:43	60	40.1	9.7	185	245	20:34:43	4.987	0.643	0.91	0.8
203	2020-03-21	20:34:44	61	48.4	9.9	203	264	20:34:44	4.988	0.6426	0.81	0.61
204	2020-03-21	20:34:45	59	34.3	9.9	205	265	20:34:45	4.985	0.6271	0.8	0.61
205	2020-03-21	20:34:46	60	38.0	10.0	204	271	20:34:46	4.988	0.6257	0.91	0.8
206	2020-03-21	20:34:47	60	35.6	10.0	212	272	20:34:47	4.986	0.6339	0.91	0.8
207	2020-03-21	20:34:48	59	30.7	10.0	212	272	20:34:48	4.99	0.629	0.91	0.8
208	2020-03-21	20:34:49	60	37.7	10.0	212	272	20:34:49	4.99	0.6267	0.8	0.61
209	2020-03-21	20:34:50	60	31.4	10.0	212	272	20:34:50	4.991	0.6363	0.81	0.63
210	2020-03-21	20:34:51	59	36.0	10.0	212	273	20:34:51	4.99	0.6241	0.88	0.72
211	2020-03-21	20:34:52	60	32.6	10.0	212	272	20:34:52	4.989	0.6328	0.86	0.7
212	2020-03-21	20:34:53	60	31.6	10.0	212	272	20:34:53	4.99	0.6325	0.79	0.59
213	2020-03-21	20:34:53	60	36.3	10.0	212	272	20:34:53	4.99	0.6325	0.79	0.59
214	2020-03-21	20:34:54	61	38.2	10.0	212	272	20:34:54	4.99	0.642	0.78	0.59
215	2020-03-21	20:34:55	61	40.9	10.0	212	272	20:34:55	4.989	0.653	0.82	0.64
216	2020-03-21	20:34:56	60	38.0	10.0	212	272	20:34:56	4.989	0.6563	0.9	0.78
217	2020-03-21	20:34:57	60	30.6	10.0	212	272	20:34:57	4.989	0.6473	0.87	0.71
218	2020-03-21	20:34:58	61	38.5	9.7	190	250	20:34:58	4.99	0.6296	0.78	0.59
219	2020-03-21	20:34:59	61	32.0	9.7	190	250	20:34:59	4.989	0.6296	0.81	0.61
220	2020-03-21	20:35:00	61	30.5	9.7	190	250	20:35:00	4.99	0.6282	0.91	0.8
221	2020-03-21	20:35:01	60	31.7	9.7	190	250	20:35:01	4.989	0.6263	0.91	0.8
222	2020-03-21	20:35:02	59	30.5	9.7	190	250	20:35:02	4.988	0.6273	0.81	0.61
223	2020-03-21	20:35:03	59	29.8	9.7	190	250	20:35:03	4.989	0.6241	0.82	0.63

224	2020-03-21	20:35:04	60	32.5	9.6	180	240	20:35:04	4.989	0.6267	0.78	0.59
225	2020-03-21	20:35:05	62	31.3	9.9	180	240	20:35:05	4.99	0.6316	0.88	0.74
226	2020-03-21	20:35:06	60	30.6	9.6	180	240	20:35:06	4.989	0.6263	0.91	0.8
227	2020-03-21	20:35:07	60	33.2	9.6	180	240	20:35:07	4.99	0.6296	0.81	0.61
228	2020-03-21	20:35:08	60	37.8	9.6	180	240	20:35:08	4.989	0.6428	0.8	0.61
229	2020-03-21	20:35:08	62	37.9	9.6	180	240	20:35:08	4.989	0.6428	0.8	0.61
230	2020-03-21	20:35:09	61	33.3	9.6	180	240	20:35:09	4.989	0.6502	0.92	0.8
231	2020-03-21	20:35:10	60	35.6	10.7	180	240	20:35:10	4.989	0.6524	0.91	0.8
232	2020-03-21	20:35:11	61	30.8	10.2	180	240	20:35:11	4.988	0.6451	0.81	0.62
233	2020-03-21	20:35:12	60	31.6	9.8	180	240	20:35:12	4.989	0.6418	0.8	0.61
234	2020-03-21	20:35:13	60	31.1	9.6	180	240	20:35:13	4.989	0.6367	0.8	0.6
235	2020-03-21	20:35:14	60	31.0	9.6	180	240	20:35:14	4.989	0.6368	0.91	0.8
236	2020-03-21	20:35:15	60	31.0	9.6	180	240	20:35:15	4.989	0.6247	0.91	0.8
237	2020-03-21	20:35:16	60	30.5	9.6	180	240	20:35:16	4.988	0.629	0.81	0.61
238	2020-03-21	20:35:17	60	30.3	9.6	180	240	20:35:17	4.988	0.6259	0.79	0.6
239	2020-03-21	20:35:18	60	31.9	9.6	180	240	20:35:18	4.988	0.6225	0.91	0.8
240	2020-03-21	20:35:19	60	31.2	9.6	180	240	20:35:19	4.989	0.6259	0.91	0.8
241	2020-03-21	20:35:20	60	36.9	9.6	180	240	20:35:20	4.99	0.6274	0.82	0.63
242	2020-03-21	20:35:21	60	38.4	9.6	180	240	20:35:21	4.989	0.6353	0.78	0.61
243	2020-03-21	20:35:22	60	38.9	9.6	180	240	20:35:22	4.989	0.6479	0.78	0.59
244	2020-03-21	20:35:22	60	31.6	9.6	180	240	20:35:22	4.989	0.6479	0.78	0.59
245	2020-03-21	20:35:23	59	31.4	9.6	180	240	20:35:23	4.991	0.6573	0.86	0.7
246	2020-03-21	20:35:24	60	30.7	9.6	180	240	20:35:24	4.99	0.6471	0.9	0.79
247	2020-03-21	20:35:25	60	30.8	9.6	180	240	20:35:25	4.991	0.6443	0.81	0.62
248	2020-03-21	20:35:26	61	30.7	9.6	180	240	20:35:26	4.99	0.6388	0.78	0.59

249	2020-03-21	20:35:27	60	30.7	9.6	180	240	20:35:27	4.99	0.6361	0.87	0.72
250	2020-03-21	20:35:28	61	37.3	9.7	180	242	20:35:28	4.99	0.6282	0.92	0.81
251	2020-03-21	20:35:29	61	46.0	9.9	202	262	20:35:29	4.987	0.6306	0.91	0.8
252	2020-03-21	20:35:30	61	30.6	9.9	202	262	20:35:30	4.988	0.6807	0.8	0.6
253	2020-03-21	20:35:31	61	39.9	10.0	210	270	20:35:31	4.988	0.6239	0.8	0.61
254	2020-03-21	20:35:32	61	35.6	10.0	212	272	20:35:32	4.988	0.6373	0.92	0.81
255	2020-03-21	20:35:33	61	39.2	10.0	212	272	20:35:33	4.988	0.6273	0.91	0.8
256	2020-03-21	20:35:34	60	41.7	10.0	212	272	20:35:34	4.988	0.6349	0.82	0.63
257	2020-03-21	20:35:35	61	36.0	10.0	212	272	20:35:35	4.988	0.6377	0.8	0.61
258	2020-03-21	20:35:36	62	36.2	10.1	212	272	20:35:36	4.99	0.632	0.81	0.63
259	2020-03-21	20:35:37	60	30.9	10.0	212	272	20:35:37	4.99	0.6249	0.84	0.67
260	2020-03-21	20:35:38	61	33.2	10.2	212	272	20:35:38	4.989	0.6273	0.87	0.72
261	2020-03-21	20:35:38	61	33.5	10.1	212	272	20:35:39	4.989	0.6559	0.78	0.59
262	2020-03-21	20:35:39	61	30.4	10.1	212	272	20:35:40	4.99	0.6455	0.79	0.61
263	2020-03-21	20:35:40	60	31.5	10.0	212	272	20:35:41	4.989	0.6485	0.87	0.72
264	2020-03-21	20:35:41	61	61.2	10.0	212	272	20:35:42	4.989	0.6683	0.9	0.79
265	2020-03-21	20:35:42	62	38.1	10.2	210	272	20:35:43	4.988	0.6341	0.81	0.63
266	2020-03-21	20:35:43	62	38.9	10.9	212	272	20:35:44	4.99	0.6604	0.81	0.61
267	2020-03-21	20:35:44	61	32.5	10.6	212	272	20:35:45	4.99	0.6461	0.8	0.61
268	2020-03-21	20:35:45	62	35.6	10.4	212	272	20:35:46	4.986	0.6371	0.91	0.8
269	2020-03-21	20:35:47	62	38.8	10.1	212	272	20:35:47	4.989	0.6573	0.92	0.81
270	2020-03-21	20:35:48	62	39.8	10.1	212	272	20:35:48	4.989	0.6377	0.81	0.61
271	2020-03-21	20:35:49	62	31.3	10.1	212	272	20:35:49	4.99	0.6351	0.81	0.61
272	2020-03-21	20:35:50	62	33.3	10.1	211	271	20:35:50	4.991	0.6286	0.86	0.7
273	2020-03-21	20:35:51	62	34.0	10.1	211	271	20:35:51	4.99	0.6322	0.9	0.79

274	2020-03-21	20:35:52	61	31.0	10.1	211	271	20:35:52	4.99	0.6359	0.81	0.62
275	2020-03-21	20:35:53	61	35.0	10.1	211	271	20:35:53	4.99	0.6358	0.8	0.61
276	2020-03-21	20:35:53	61	30.7	10.1	211	271	20:35:53	4.99	0.6358	0.8	0.61
277	2020-03-21	20:35:54	61	31.6	10.1	211	271	20:35:54	4.99	0.6502	0.81	0.61
278	2020-03-21	20:35:55	62	33.2	10.1	211	271	20:35:55	4.99	0.6473	0.92	0.81
279	2020-03-21	20:35:56	62	31.0	10.1	211	271	20:35:56	4.991	0.6418	0.91	0.8
280	2020-03-21	20:35:57	62	35.2	10.1	211	271	20:35:57	4.99	0.6341	0.8	0.61
281	2020-03-21	20:35:58	62	37.6	10.1	211	271	20:35:58	4.99	0.6306	0.8	0.61
282	2020-03-21	20:35:59	62	42.9	10.1	210	270	20:35:59	4.989	0.6333	0.83	0.64
283	2020-03-21	20:36:00	61	40.3	10.1	209	269	20:36:00	4.988	0.6355	0.86	0.69
284	2020-03-21	20:36:01	61	31.5	10.0	209	269	20:36:01	4.988	0.6369	0.86	0.69
285	2020-03-21	20:36:02	62	32.2	10.0	203	263	20:36:02	4.989	0.6282	0.81	0.63
286	2020-03-21	20:36:03	61	33.1	9.9	202	262	20:36:03	4.988	0.6328	0.81	0.62
287	2020-03-21	20:36:04	62	30.9	10.0	202	262	20:36:04	4.989	0.628	0.9	0.78
288	2020-03-21	20:36:05	62	36.1	9.6	178	238	20:36:05	4.99	0.6284	0.91	0.8
289	2020-03-21	20:36:06	61	30.6	9.6	178	238	20:36:06	4.991	0.6296	0.79	0.6
290	2020-03-21	20:36:07	63	30.3	9.6	178	238	20:36:07	4.991	0.6263	0.8	0.61
291	2020-03-21	20:36:08	61	30.5	9.6	178	238	20:36:08	4.991	0.6318	0.91	0.8
292	2020-03-21	20:36:09	60	30.3	9.6	178	238	20:36:09	4.991	0.6349	0.91	0.8
293	2020-03-21	20:36:09	61	30.6	9.6	178	238	20:36:09	4.991	0.6349	0.91	0.8
294	2020-03-21	20:36:10	62	33.2	9.9	179	239	20:36:10	4.991	0.6416	0.92	0.81
295	2020-03-21	20:36:11	61	38.3	9.6	179	239	20:36:11	4.99	0.6491	0.81	0.61
296	2020-03-21	20:36:12	61	38.0	9.6	179	239	20:36:12	4.989	0.6734	0.79	0.59
297	2020-03-21	20:36:13	62	34.1	9.6	179	239	20:36:13	4.989	0.641	0.9	0.79
298	2020-03-21	20:36:14	61	30.7	9.6	179	239	20:36:14	4.99	0.6377	0.91	0.79

299	2020-03-21	20:36:15	61	30.5	9.6	178	238	20:36:15	4.989	0.6259	0.77	0.59
300	2020-03-21	20:36:16	61	35.3	10.7	178	238	20:36:16	4.989	0.6263	0.81	0.63
301	2020-03-21	20:36:17	60	30.5	10.3	178	238	20:36:17	4.988	0.6551	0.9	0.78
302	2020-03-21	20:36:18	61	30.7	10.1	178	238	20:36:18	4.988	0.6392	0.82	0.62
303	2020-03-21	20:36:19	61	31.2	9.6	178	238	20:36:19	4.988	0.6371	0.91	0.8
304	2020-03-21	20:36:20	61	30.2	9.6	178	238	20:36:20	4.991	0.6406	0.8	0.6
305	2020-03-21	20:36:21	62	30.6	9.6	177	237	20:36:21	4.991	0.632	0.8	0.6
306	2020-03-21	20:36:22	62	30.8	9.6	177	237	20:36:22	4.99	0.6388	0.91	0.8
307	2020-03-21	20:36:23	62	31.0	9.6	177	237	20:36:23	4.991	0.6461	0.91	0.8
308	2020-03-21	20:36:23	61	34.5	9.6	177	237	20:36:23	4.991	0.6461	0.91	0.8
309	2020-03-21	20:36:24	62	38.0	9.6	177	237	20:36:24	4.991	0.65	0.8	0.61
310	2020-03-21	20:36:25	61	38.1	9.6	177	237	20:36:25	4.99	0.6504	0.8	0.6
311	2020-03-21	20:36:26	62	33.3	9.6	177	237	20:36:26	4.989	0.6471	0.81	0.61
312	2020-03-21	20:36:27	61	30.8	9.6	177	237	20:36:27	4.991	0.6496	0.9	0.78
313	2020-03-21	20:36:28	61	31.6	9.6	177	237	20:36:28	4.99	0.6361	0.92	0.8
314	2020-03-21	20:36:29	61	33.4	9.6	179	239	20:36:29	4.989	0.6329	0.79	0.6
315	2020-03-21	20:36:30	61	31.6	9.6	179	239	20:36:30	4.989	0.63	0.81	0.61
316	2020-03-21	20:36:31	63	31.2	9.6	179	239	20:36:31	4.989	0.6276	0.91	0.8
317	2020-03-21	20:36:32	62	45.1	9.9	187	262	20:36:32	4.99	0.6273	0.91	0.8
318	2020-03-21	20:36:33	63	42.9	10.0	206	267	20:36:33	4.986	0.6326	0.92	0.81
319	2020-03-21	20:36:34	62	33.3	10.0	209	269	20:36:34	4.99	0.6328	0.81	0.61
320	2020-03-21	20:36:35	59	11.0	10.0	209	269	20:36:35	4.994	0.6345	0.78	0.59
321	2020-03-21	20:36:36	61	15.2	10.1	210	270	20:36:36	4.994	0.5958	0.9	0.79
322	2020-03-21	20:36:37	62	41.5	10.1	210	270	20:36:37	4.994	0.5852	0.91	0.8
323	2020-03-21	20:36:38	61	41.4	10.1	210	271	20:36:38	4.995	0.5892	0.81	0.61

324	2020-03-21	20:36:39	63	37.6	10.1	210	270	20:36:39	4.995	0.6035	0.8	0.61
325	2020-03-21	20:36:40	62	34.4	10.1	210	270	20:36:40	4.995	0.5929	0.91	0.8
326	2020-03-21	20:36:41	62	33.6	10.1	210	270	20:36:41	4.996	0.5968	0.91	0.8
327	2020-03-21	20:36:41	62	33.1	10.1	210	270	20:36:41	4.996	0.5968	0.91	0.8
328	2020-03-21	20:36:42	62	33.2	10.1	210	271	20:36:42	4.996	0.5992	0.82	0.63
329	2020-03-21	20:36:43	62	33.4	10.2	210	270	20:36:43	4.996	0.5939	0.79	0.59
330	2020-03-21	20:36:44	61	16.9	10.1	210	270	20:36:44	4.994	0.5866	0.81	0.63
331	2020-03-21	20:36:45	61	7.8	10.1	210	270	20:36:45	4.998	0.5884	0.84	0.67
332	2020-03-21	20:36:46	61	29.0	10.2	211	271	20:36:46	5	0.5428	0.9	0.79
333	2020-03-21	20:36:47	60	31.6	10.2	211	271	20:36:47	4.995	0.5503	0.82	0.63
334	2020-03-21	20:36:48	61	37.2	10.9	209	269	20:36:48	4.995	0.5732	0.77	0.58
335	2020-03-21	20:36:49	61	42.6	10.7	193	247	20:36:49	4.992	0.5731	0.81	0.63
336	2020-03-21	20:36:50	62	38.9	10.1	187	247	20:36:50	4.992	0.6027	0.83	0.65

Run-RCE - 25°C													
	Date	T.Stamp	Temp	CPU_Load	Mem_Load	ProNo,	ThreadsNo	RX_bit	RX_pkt	TX_bit	TX_pkt	Voltage(V)	Current(A)
1	2020-04-26	01:58:10	59	29	9.9	173	226	0	0	0	0	4.995	0.6161
2	2020-04-26	01:58:11	59	28.9	9.9	173	226	52	1	142	1	4.993	0.6139
3	2020-04-26	01:58:11	59	29	9.9	173	226	0	0	0	0	4.993	0.6139
4	2020-04-26	01:58:12	59	28.9	9.9	173	226	52	1	142	1	4.994	0.6192
5	2020-04-26	01:58:13	58	29.4	9.9	173	226	0	0	0	0	4.995	0.6204
6	2020-04-26	01:58:14	60	29.5	9.9	173	226	52	1	142	1	4.995	0.6271
7	2020-04-26	01:58:15	59	29.6	9.9	173	226	0	0	0	0	4.995	0.6386
8	2020-04-26	01:58:16	59	29.4	9.9	173	226	0	0	0	0	4.995	0.6341
9	2020-04-26	01:58:17	59	29.2	9.9	173	226	52	1	142	1	4.995	0.6227
10	2020-04-26	01:58:18	58	30.9	9.9	173	226	0	0	0	0	4.995	0.6115
11	2020-04-26	01:58:19	60	36.4	9.9	173	226	52	1	142	1	4.994	0.6188
12	2020-04-26	01:58:20	59	36.3	9.9	173	226	0	0	0	0	4.992	0.6263
13	2020-04-26	01:58:21	59	34.3	9.9	173	226	52	1	142	1	4.993	0.631
14	2020-04-26	01:58:21	58	29.4	9.9	173	226	0	0	0	0	4.993	0.631
15	2020-04-26	01:58:22	60	28.8	9.9	173	226	52	1	142	1	4.992	0.6188
16	2020-04-26	01:58:23	59	29.4	9.9	173	226	0	0	0	0	4.994	0.6133
17	2020-04-26	01:58:24	59	28.7	9.9	173	226	52	1	142	1	4.995	0.6216
18	2020-04-26	01:58:25	59	29	9.9	173	226	0	0	0	0	4.994	0.6351
19	2020-04-26	01:58:26	59	28.9	9.9	168	222	52	1	142	1	4.995	0.6322
20	2020-04-26	01:58:27	59	29.3	9.9	168	221	0	0	0	0	4.995	0.6188
21	2020-04-26	01:58:28	59	29.2	9.9	167	220	52	1	142	1	4.994	0.6119
22	2020-04-26	01:58:29	59	29.1	9.9	167	220	0	0	0	0	4.995	0.618
23	2020-04-26	01:58:30	60	29	9.9	167	220	0	0	142	1	4.993	0.6196

24	2020-04-26	01:58:31	60	29.9	9.9	167	220	52	1	0	0	4.994	0.617
25	2020-04-26	01:58:32	60	37.1	9.9	165	218	0	0	0	0	4.994	0.6184
26	2020-04-26	01:58:32	59	36.6	9.9	166	219	52	1	142	1	4.994	0.6184
27	2020-04-26	01:58:33	59	34.2	9.9	166	219	0	0	0	0	4.994	0.6269
28	2020-04-26	01:58:34	60	28.9	9.9	164	217	52	1	142	1	4.994	0.6365
29	2020-04-26	01:58:35	60	29.4	9.9	163	216	0	0	0	0	4.995	0.6434
30	2020-04-26	01:58:36	60	28.8	9.9	162	215	52	1	142	1	4.994	0.6314
31	2020-04-26	01:58:37	59	29.5	9.9	162	215	0	0	0	0	4.994	0.6278
32	2020-04-26	01:58:38	59	28.9	9.9	162	215	52	1	142	1	4.995	0.6188
33	2020-04-26	01:58:39	59	28.8	9.9	162	215	0	0	0	0	4.995	0.6184
34	2020-04-26	01:58:40	59	28.7	9.9	162	215	0	0	142	1	4.994	0.6127
35	2020-04-26	01:58:41	59	29.2	9.9	163	216	52	1	0	0	4.993	0.6192
36	2020-04-26	01:58:42	58	29.5	9.9	163	216	0	0	0	0	4.993	0.618
37	2020-04-26	01:58:42	59	29.3	9.9	163	216	52	1	142	1	4.993	0.618
38	2020-04-26	01:58:43	59	30.1	9.9	163	216	0	0	0	0	4.994	0.6125
39	2020-04-26	01:58:44	59	35.3	9.9	163	216	52	1	142	1	4.995	0.6329
40	2020-04-26	01:58:45	58	31.1	9.9	163	216	156	3	568	4	4.995	0.6463
41	2020-04-26	01:58:46	58	11.5	9.9	163	216	156	3	292	2	4.994	0.6329
42	2020-04-26	01:58:47	58	6.6	9.9	163	216	0	0	0	0	4.995	0.565
43	2020-04-26	01:58:48	57	7	9.9	163	216	208	4	576	4	5.003	0.5448
44	2020-04-26	01:58:49	56	6.9	9.9	163	216	0	0	0	0	5.003	0.531
45	2020-04-26	01:58:50	56	8.9	9.9	163	216	208	4	568	4	5.003	0.5259
46	2020-04-26	01:58:51	57	12.9	9.9	163	216	624	12	1704	12	5.004	0.5281
47	2020-04-26	01:58:52	57	13	9.9	163	216	740	14	2130	15	5.001	0.563
48	2020-04-26	01:58:53	56	11.6	9.9	163	216	676	13	1846	13	5.001	0.5479

49	2020-04-26	01:58:54	56	9.5	9.9	163	217	624	12	1696	12	5	0.5442
50	2020-04-26	01:58:55	56	6.2	9.9	163	216	0	0	0	0	5	0.5493
51	2020-04-26	01:58:56	56	6.9	9.9	164	217	312	6	804	6	5.001	0.5216
52	2020-04-26	01:58:57	57	10.6	9.9	164	217	52	1	150	1	5.001	0.5269
53	2020-04-26	01:58:58	56	12.8	9.9	164	217	52	1	150	1	4.999	0.5526
54	2020-04-26	01:58:59	55	11.2	9.9	164	217	0	0	0	0	4.997	0.551
55	2020-04-26	01:59:00	55	9.4	9.9	164	218	416	8	1278	9	4.997	0.5524
56	2020-04-26	01:59:01	56	17.1	9.9	164	217	780	15	2114	15	4.998	0.541
57	2020-04-26	01:59:02	56	7.6	9.9	164	217	816	15	2346	17	4.999	0.5373
58	2020-04-26	01:59:03	56	8.4	9.9	164	217	364	7	938	7	5.001	0.5377
59	2020-04-26	01:59:04	55	6.4	9.9	164	217	0	0	0	0	5.003	0.5344
60	2020-04-26	01:59:04	55	6.5	9.9	164	217	0	0	0	0	5.003	0.5344
61	2020-04-26	01:59:05	56	13	9.9	163	217	728	14	1972	14	5.004	0.5218
62	2020-04-26	01:59:06	55	9.5	9.9	163	216	416	8	1112	8	5.003	0.5477
63	2020-04-26	01:59:07	55	6.2	9.9	163	216	156	3	434	3	5.001	0.5505
64	2020-04-26	01:59:08	55	6	9.9	163	216	0	0	0	0	5.003	0.5208
65	2020-04-26	01:59:09	56	15	9.9	163	216	0	0	0	0	5.003	0.5245
66	2020-04-26	01:59:10	55	17.5	9.9	164	217	260	5	702	5	5.004	0.574
67	2020-04-26	01:59:11	55	12.9	9.9	164	217	0	0	0	0	5.001	0.641
68	2020-04-26	01:59:12	56	7.1	9.9	164	217	52	1	150	1	5	0.5783
69	2020-04-26	01:59:13	55	6.8	9.9	164	216	0	0	0	0	5.001	0.564
70	2020-04-26	01:59:14	55	6.5	9.9	164	217	52	1	150	1	5.003	0.544
71	2020-04-26	01:59:15	55	6.8	9.9	164	217	52	1	150	1	5.003	0.5438
72	2020-04-26	01:59:16	56	5.5	9.9	164	217	0	0	142	1	5.002	0.5371
73	2020-04-26	01:59:17	55	7	9.9	164	217	156	3	292	2	5.003	0.5571

74	2020-04-26	01:59:18	55	6.3	9.9	164	217	0	0	0	0	5.003	0.5228
75	2020-04-26	01:59:19	55	6.4	9.9	164	217	52	1	150	1	5.003	0.5279
76	2020-04-26	01:59:20	55	6.8	9.9	164	217	0	0	0	0	5.002	0.5234
77	2020-04-26	01:59:21	55	6.8	9.9	164	217	52	1	150	1	5.003	0.5277
78	2020-04-26	01:59:22	55	9.9	9.9	164	217	208	4	576	4	5.003	0.5278
79	2020-04-26	01:59:23	55	11.9	9.9	164	217	0	0	0	0	5.001	0.5467
80	2020-04-26	01:59:24	56	17.5	9.9	164	217	0	0	0	0	5.002	0.5489
81	2020-04-26	01:59:25	56	12	9.9	164	217	208	4	576	4	5	0.5528
82	2020-04-26	01:59:26	55	6.8	9.9	164	217	0	0	0	0	4.994	0.5224
83	2020-04-26	01:59:27	55	7	9.9	164	217	52	1	150	1	5	0.5245
84	2020-04-26	01:59:28	55	10.2	9.9	164	217	364	7	994	7	5	0.5281
85	2020-04-26	01:59:29	55	11.8	9.9	164	217	624	12	1846	13	5	0.5283
86	2020-04-26	01:59:30	56	21.1	9.9	164	218	598	10	852	6	4.998	0.5459
87	2020-04-26	01:59:31	55	16.5	9.9	164	217	764	14	2196	16	4.996	0.5579
88	2020-04-26	01:59:31	55	9.6	9.9	164	217	688	13	1988	14	4.996	0.5579
89	2020-04-26	01:59:32	55	10.5	9.9	164	218	728	14	1988	14	4.995	0.5404
90	2020-04-26	01:59:33	55	8.1	9.9	164	217	572	11	1412	10	5.001	0.5318
91	2020-04-26	01:59:34	54	6.5	9.9	164	217	116	2	552	4	5.001	0.5391
92	2020-04-26	01:59:35	55	17.6	9.9	164	217	0	0	394	3	5.002	0.5689
93	2020-04-26	01:59:36	55	13.1	9.9	164	217	220	4	432	2	5.002	0.5766
94	2020-04-26	01:59:37	55	11	9.9	164	217	0	0	0	0	5	0.6194
95	2020-04-26	01:59:38	56	13.7	9.9	164	217	208	4	576	4	5.001	0.5882
96	2020-04-26	01:59:39	55	6.2	9.9	164	217	0	0	0	0	5	0.5689
97	2020-04-26	01:59:40	55	6.8	9.9	165	218	0	0	0	0	4.998	0.5461
98	2020-04-26	01:59:41	55	7.4	9.9	165	218	52	1	150	1	5.004	0.5518

99	2020-04-26	01:59:42	54	7.5	9.9	165	218	0	0	0	0	5.003	0.5546
100	2020-04-26	01:59:43	54	7.7	9.9	165	218	208	4	576	4	5.004	0.5522
101	2020-04-26	01:59:44	54	6.7	9.9	166	219	0	0	0	0	5.004	0.5249
102	2020-04-26	01:59:45	55	12.4	9.9	166	219	468	9	1278	9	5.003	0.5312
103	2020-04-26	01:59:46	54	11.5	9.9	166	219	624	12	1846	13	5.004	0.5475
104	2020-04-26	01:59:47	55	11.3	9.9	166	219	804	15	2280	16	5.002	0.5607
105	2020-04-26	01:59:48	54	12	9.9	167	220	0	0	0	0	5	0.56085
106	2020-04-26	01:59:49	55	11.6	9.9	167	220	52	1	150	1	5	0.561
107	2020-04-26	01:59:50	55	11.4	9.9	167	220	0	0	0	0	5.002	0.5611
108	2020-04-26	01:59:51	55	6.3	9.9	168	221	220	4	576	4	5	0.5495
109	2020-04-26	01:59:52	55	5.7	9.9	168	221	0	0	0	0	5.001	0.5554
110	2020-04-26	01:59:53	54	6.6	9.9	168	221	52	1	150	1	5.002	0.5239
111	2020-04-26	01:59:54	55	6.2	9.9	168	221	0	0	0	0	5.003	0.5314
112	2020-04-26	01:59:55	54	8.8	9.9	167	220	260	5	710	5	4.998	0.5232
113	2020-04-26	01:59:56	54	10.8	9.9	167	220	728	14	1988	14	4.998	0.5247
114	2020-04-26	01:59:57	55	8.7	9.9	167	220	416	8	1144	8	4.998	0.5399
115	2020-04-26	01:59:58	55	16.9	9.9	167	220	52	1	284	2	4.998	0.541
116	2020-04-26	01:59:59	55	5.5	9.9	167	220	156	3	292	2	4.998	0.5249
117	2020-04-26	02:00:00	54	6.2	9.9	167	220	0	0	0	0	4.998	0.5756
118	2020-04-26	02:00:01	55	15.5	9.9	167	220	52	1	150	1	4.999	0.5078
119	2020-04-26	02:00:02	55	12.1	9.9	167	220	52	1	150	1	5	0.5216
120	2020-04-26	02:00:02	55	12.1	9.9	167	220	0	0	0	0	5	0.5216
121	2020-04-26	02:00:03	55	7	9.9	167	220	52	1	150	1	4.997	0.5465
122	2020-04-26	02:00:04	54	6.9	9.9	167	220	0	0	0	0	5	0.5509
123	2020-04-26	02:00:05	55	8.1	9.9	167	220	208	4	568	4	5	0.5736

124	2020-04-26	02:00:06	54	12.8	9.9	167	220	624	12	1704	12	5.002	0.5344
125	2020-04-26	02:00:07	55	12.4	9.9	167	220	740	14	2130	15	5.004	0.531
126	2020-04-26	02:00:08	55	11.3	9.9	167	220	832	16	2130	15	5.003	0.5589
127	2020-04-26	02:00:09	55	7.4	9.9	167	220	156	3	434	3	5	0.5562
128	2020-04-26	02:00:10	54	6.9	9.9	167	220	52	1	150	1	5.003	0.5787
129	2020-04-26	02:00:11	53	5.9	9.9	167	220	0	0	0	0	5	0.5799
130	2020-04-26	02:00:12	54	10.4	9.9	167	220	104	2	292	2	5.003	0.5776
131	2020-04-26	02:00:13	55	10.4	9.9	167	220	0	0	0	0	5.003	0.5673
132	2020-04-26	02:00:14	55	11.7	9.9	167	220	52	1	150	1	5.004	0.5723
133	2020-04-26	02:00:15	54	12.3	9.9	167	220	0	0	0	0	5.001	0.5634
134	2020-04-26	02:00:16	53	9.1	9.9	167	220	0	0	142	1	5.002	0.6017
135	2020-04-26	02:00:17	54	11.5	9.9	167	220	740	14	2130	15	5	0.5675
136	2020-04-26	02:00:18	55	12.5	9.9	167	220	780	15	1988	14	5	0.5567
137	2020-04-26	02:00:19	54	9.7	9.9	167	220	780	15	1988	14	5.003	0.5454
138	2020-04-26	02:00:20	55	10.2	9.9	167	220	676	13	1988	14	5.001	0.5412
139	2020-04-26	02:00:21	55	8.8	9.9	167	220	572	11	1554	11	5.001	0.5385
140	2020-04-26	02:00:22	54	7.4	9.9	167	220	52	1	150	1	5	0.5434
141	2020-04-26	02:00:23	54	6.3	9.9	167	220	0	0	0	0	5.001	0.5379
142	2020-04-26	02:00:24	54	10.4	9.9	167	220	0	0	0	0	5.001	0.5137
143	2020-04-26	02:00:25	53	12.4	9.9	167	221	260	5	702	5	5.002	0.5202
144	2020-04-26	02:00:26	55	6.2	9.9	167	220	0	0	0	0	5.002	0.5245
145	2020-04-26	02:00:27	55	12.6	9.9	167	220	104	2	276	2	4.997	0.5383
146	2020-04-26	02:00:28	55	12.2	9.9	167	220	0	0	0	0	4.998	0.5241
147	2020-04-26	02:00:29	54	11	9.9	167	220	52	1	284	2	4.998	0.5514
148	2020-04-26	02:00:30	54	13.3	9.9	167	221	740	14	1988	14	4.999	0.5552

149	2020-04-26	02:00:31	53	9.3	9.9	167	220	584	11	1712	12	4.999	0.5322
150	2020-04-26	02:00:32	55	6.2	9.9	167	220	52	1	150	1	5	0.5261
151	2020-04-26	02:00:33	54	6.4	9.9	167	220	0	0	0	0	5	0.5262
152	2020-04-26	02:00:34	54	9.6	9.9	167	220	0	0	0	0	5.002	0.521
153	2020-04-26	02:00:34	53	11.6	9.9	168	221	272	5	868	6	5.002	0.521
154	2020-04-26	02:00:35	55	6.6	9.9	168	221	0	0	0	0	5.002	0.5165
155	2020-04-26	02:00:36	54	6.4	9.9	168	221	0	0	462	3	5.002	0.5868
156	2020-04-26	02:00:37	54	8	9.9	168	221	260	5	754	5	5	0.5528
157	2020-04-26	02:00:38	53	10.7	9.9	168	221	832	16	2256	16	5.002	0.5652
158	2020-04-26	02:00:39	54	12.4	9.9	168	221	208	4	434	3	5.001	0.5638
159	2020-04-26	02:00:40	55	23	9.9	168	222	208	4	576	4	5.002	0.5641
160	2020-04-26	02:00:41	54	9.9	9.9	168	221	0	0	0	0	5	0.5852
161	2020-04-26	02:00:42	53	6.8	9.9	168	221	0	0	0	0	5	0.5819
162	2020-04-26	02:00:43	54	5.7	9.9	168	221	52	1	150	1	4.995	0.5876
163	2020-04-26	02:00:44	54	6.5	9.9	168	221	0	0	0	0	5	0.5546
164	2020-04-26	02:00:45	54	15.2	9.9	168	221	156	3	584	4	5.002	0.5534
165	2020-04-26	02:00:46	53	6.4	9.9	168	221	0	0	0	0	5.003	0.5538
166	2020-04-26	02:00:47	55	7.9	9.9	168	221	208	4	568	4	5.001	0.607
167	2020-04-26	02:00:48	54	12.7	9.9	168	221	624	12	1704	12	5.002	0.5459
168	2020-04-26	02:00:49	54	12.2	9.9	168	221	740	14	2272	16	5.002	0.5416
169	2020-04-26	02:00:50	53	5.7	9.9	168	221	104	2	150	1	5	0.5617
170	2020-04-26	02:00:51	54	6.9	9.9	168	221	52	1	150	1	5.001	0.5393
171	2020-04-26	02:00:52	54	12.7	9.9	168	221	52	1	150	1	5.003	0.5408
172	2020-04-26	02:00:53	54	12.2	9.9	168	221	0	0	0	0	5.002	0.512
173	2020-04-26	02:00:54	54	11	9.9	169	222	52	1	150	1	5.004	0.5471

174	2020-04-26	02:00:55	55	6	9.9	169	222	0	0	0	0	5.001	0.5569
175	2020-04-26	02:00:56	53	6.5	9.9	169	222	52	1	150	1	5.001	0.5499
176	2020-04-26	02:00:57	54	6.2	9.9	169	222	0	0	0	0	5.001	0.5247
177	2020-04-26	02:00:58	53	8.5	9.9	168	221	312	6	852	6	5	0.5243
178	2020-04-26	02:00:59	53	6.9	9.9	168	221	260	5	718	5	5.001	0.5228
179	2020-04-26	02:01:00	54	5.9	9.9	168	221	0	0	0	0	5.001	0.5269
180	2020-04-26	02:01:01	53	17.1	9.9	168	221	156	3	434	3	4.997	0.5069
181	2020-04-26	02:01:02	54	6.7	9.9	168	221	0	0	0	0	4.999	0.5234
182	2020-04-26	02:01:03	54	10.3	9.9	168	221	0	0	0	0	4.998	0.5795
183	2020-04-26	02:01:04	55	14.6	9.9	168	221	260	5	718	5	4.999	0.5069
184	2020-04-26	02:01:05	54	11	9.9	168	221	0	0	0	0	4.998	0.5228
185	2020-04-26	02:01:06	54	12.1	9.9	168	221	52	1	150	1	4.995	0.5228
186	2020-04-26	02:01:07	54	12	9.9	168	221	0	0	142	1	5	0.5505
187	2020-04-26	02:01:08	54	8.5	9.9	168	221	676	13	1522	11	4.998	0.5506
188	2020-04-26	02:01:09	54	6.4	9.9	168	221	52	1	150	1	5	0.5463
189	2020-04-26	02:01:10	54	8.5	9.9	169	223	208	4	568	4	5.003	0.5267
190	2020-04-26	02:01:11	54	12.3	9.9	169	222	740	14	2130	15	5.003	0.5344
191	2020-04-26	02:01:12	54	10.4	9.9	169	223	676	13	1846	13	5.003	0.552
192	2020-04-26	02:01:12	53	11.6	9.9	169	223	740	14	2272	16	5.003	0.552
193	2020-04-26	02:01:13	53	13	9.9	169	222	728	14	1988	14	5.003	0.5416
194	2020-04-26	02:01:14	53	10.5	9.9	169	222	520	10	1428	10	5.001	0.552
195	2020-04-26	02:01:15	54	7.7	9.9	169	222	156	3	426	3	5.001	0.5521
196	2020-04-26	02:01:16	53	8.1	9.9	169	222	260	5	718	5	5.001	0.552
197	2020-04-26	02:01:17	54	9.5	9.9	169	222	52	1	150	1	5.001	0.562
198	2020-04-26	02:01:18	54	12.1	9.9	169	222	0	0	0	0	5.004	0.5803

199	2020-04-26	02:01:19	55	21.8	9.9	169	223	116	2	142	1	5.003	0.5689
200	2020-04-26	02:01:20	53	7.9	9.9	169	222	104	2	292	2	5.001	0.5837
201	2020-04-26	02:01:21	53	5.3	9.9	169	222	0	0	0	0	5	0.5801
202	2020-04-26	02:01:22	54	8.1	9.9	169	222	468	9	1286	9	4.995	0.5434
203	2020-04-26	02:01:23	53	7.8	9.9	169	223	0	0	142	1	5.003	0.5306
204	2020-04-26	02:01:24	53	8.1	9.9	169	222	168	3	434	3	5.003	0.5383
205	2020-04-26	02:01:25	54	6	9.9	169	222	0	0	0	0	5.003	0.5283
206	2020-04-26	02:01:26	54	7.5	9.9	169	222	104	2	292	2	5.003	0.5202
207	2020-04-26	02:01:27	53	7	9.9	169	222	0	0	0	0	5.004	0.5241
208	2020-04-26	02:01:28	53	11	9.9	169	222	364	7	1136	8	5.002	0.5363
209	2020-04-26	02:01:29	54	11.4	9.9	169	223	780	15	1846	13	5.003	0.5239
210	2020-04-26	02:01:30	54	12	9.9	169	223	740	14	2216	16	5.003	0.5279
211	2020-04-26	02:01:31	54	11.8	9.9	169	222	52	1	402	3	5.002	0.5438
212	2020-04-26	02:01:32	53	12.3	9.9	169	222	0	0	0	0	5.001	0.5391
213	2020-04-26	02:01:33	54	9.2	9.9	170	223	0	0	0	0	5	0.5528
214	2020-04-26	02:01:34	54	16.6	9.9	170	223	208	4	576	4	4.998	0.5503
215	2020-04-26	02:01:35	54	6.6	9.9	170	223	0	0	0	0	4.999	0.5236
216	2020-04-26	02:01:36	55	5.9	9.9	170	223	0	0	150	1	4.995	0.5314
217	2020-04-26	02:01:37	52	6.8	9.9	169	223	168	3	300	2	5	0.534
218	2020-04-26	02:01:38	53	6.5	9.9	169	222	0	0	0	0	4.999	0.5338
219	2020-04-26	02:01:39	53	8.7	9.9	169	222	0	0	0	0	5	0.551
220	2020-04-26	02:01:40	53	10.4	9.9	169	222	260	5	702	5	5	0.5184
221	2020-04-26	02:01:41	53	7.1	9.9	169	222	0	0	0	0	5.001	0.5275
222	2020-04-26	02:01:42	53	6.5	9.9	169	222	52	1	150	1	4.999	0.5149
223	2020-04-26	02:01:43	53	7.5	9.9	169	222	52	1	150	1	5.003	0.5104

224	2020-04-26	02:01:44	53	12.6	9.9	169	222	0	0	0	0	5.002	0.5257
225	2020-04-26	02:01:45	53	18.2	9.9	169	222	52	1	142	1	5.002	0.5326
226	2020-04-26	02:01:46	53	10.1	9.9	169	222	260	5	722	5	5.001	0.5593
227	2020-04-26	02:01:46	54	6.2	9.9	169	223	0	0	0	0	5.001	0.5593
228	2020-04-26	02:01:47	54	9.7	9.9	169	222	832	16	2144	16	5.001	0.6182
229	2020-04-26	02:01:48	54	11.2	9.9	169	223	884	17	2508	18	5.002	0.5487
230	2020-04-26	02:01:49	54	8.7	9.9	169	222	364	7	860	6	5.004	0.5597
231	2020-04-26	02:01:50	53	9.5	9.9	169	222	208	4	576	4	5.002	0.5728
232	2020-04-26	02:01:51	54	6.3	9.9	169	222	0	0	0	0	5.003	0.5583
233	2020-04-26	02:01:52	53	8.4	9.9	169	222	156	3	426	3	5.004	0.5677
234	2020-04-26	02:01:53	53	6	9.9	169	222	52	1	150	1	5.004	0.5707
235	2020-04-26	02:01:54	53	6.7	9.9	169	222	0	0	0	0	5.004	0.573
236	2020-04-26	02:01:55	52	8.1	9.9	169	221	52	1	150	1	5.003	0.5734
237	2020-04-26	02:01:56	53	12.5	9.9	168	221	0	0	0	0	5.003	0.5721
238	2020-04-26	02:01:57	54	17.1	9.9	168	221	572	11	1562	11	5.004	0.5719
239	2020-04-26	02:01:58	53	12.9	9.9	168	221	804	15	2102	15	5.004	0.5923
240	2020-04-26	02:01:59	53	7.2	9.9	168	221	104	2	292	2	5	0.5956
241	2020-04-26	02:02:00	53	6.8	9.9	168	221	52	1	150	1	5	0.5935
242	2020-04-26	02:02:01	54	13.3	9.9	168	221	0	0	0	0	5.002	0.5536
243	2020-04-26	02:02:02	53	16.8	9.9	168	221	208	4	576	4	5.004	0.5516
244	2020-04-26	02:02:03	53	5.3	9.9	168	221	28	1	66	1	5.004	0.5774
245	2020-04-26	02:02:04	54	7.2	9.9	168	221	104	2	276	2	5.004	0.6092
246	2020-04-26	02:02:05	53	6.8	9.9	168	221	0	0	0	0	5.003	0.5347
247	2020-04-26	02:02:06	54	11.8	9.9	168	222	832	16	1988	14	5.004	0.5348
248	2020-04-26	02:02:07	53	6.4	9.9	168	221	156	3	434	3	5.004	0.5336

249	2020-04-26	02:02:08	52	12.1	9.9	168	221	572	11	1562	11	5.005	0.5624
250	2020-04-26	02:02:09	54	18.7	9.9	168	221	676	13	1704	12	5.002	0.523
251	2020-04-26	02:02:10	53	16.1	9.9	168	222	740	14	1988	14	5.001	0.5534
252	2020-04-26	02:02:11	54	13.3	9.9	168	221	1416	27	3508	26	5.001	0.5662
253	2020-04-26	02:02:12	54	5.5	9.9	168	221	0	0	0	0	5	0.5689
254	2020-04-26	02:02:13	54	16.9	9.9	168	221	520	10	1332	10	5	0.5615
255	2020-04-26	02:02:14	55	6.9	9.9	168	222	0	0	0	0	5.001	0.5241
256	2020-04-26	02:02:15	53	7	9.9	168	221	156	3	402	3	5	0.5721
257	2020-04-26	02:02:16	53	5.7	9.9	168	221	0	0	0	0	5.001	0.5084
258	2020-04-26	02:02:17	53	11.4	9.9	168	221	52	1	142	1	5.002	0.5239
259	2020-04-26	02:02:18	54	7.7	9.9	168	221	104	2	292	2	5.003	0.5196
260	2020-04-26	02:02:19	53	6.6	9.9	168	221	0	0	0	0	5	0.5149
261	2020-04-26	02:02:20	54	11.6	9.9	168	221	468	9	1278	9	4.997	0.5145
262	2020-04-26	02:02:21	53	8.2	9.9	168	222	312	6	860	6	4.998	0.5239
263	2020-04-26	02:02:22	54	12.4	9.9	168	221	0	0	0	0	4.999	0.5522
264	2020-04-26	02:02:23	53	15.2	9.9	168	221	324	6	994	7	4.998	0.5188
265	2020-04-26	02:02:24	55	15.1	9.9	168	221	780	15	1988	14	4.998	0.551
266	2020-04-26	02:02:25	54	8	9.9	168	221	492	9	1286	9	4.998	0.5673
267	2020-04-26	02:02:26	53	6	9.9	168	221	52	1	150	1	4.997	0.5501
268	2020-04-26	02:02:27	52	7.2	9.9	168	221	0	0	0	0	5.002	0.5241
269	2020-04-26	02:02:28	53	8.6	9.9	168	221	260	5	710	5	5.003	0.521
270	2020-04-26	02:02:29	53	10.6	9.9	168	221	728	14	1988	14	5.004	0.5157
271	2020-04-26	02:02:30	53	7.2	9.9	168	221	364	7	1002	7	5.003	0.5385
272	2020-04-26	02:02:31	53	12.6	9.9	168	221	208	4	576	4	5.003	0.5237
273	2020-04-26	02:02:32	52	6.1	9.9	168	221	0	0	0	0	5.001	0.519

274	2020-04-26	02:02:33	53	5.9	9.9	168	221	0	0	0	0	5.002	0.5393
275	2020-04-26	02:02:34	53	13.2	9.9	168	221	568	10	2002	13	5.003	0.5226
276	2020-04-26	02:02:35	52	15.7	9.9	168	221	336	6	1300	8	5.002	0.563
277	2020-04-26	02:02:35	53	11.8	9.9	168	221	0	0	0	0	5.002	0.563
278	2020-04-26	02:02:36	53	13.5	9.9	168	222	156	3	568	4	5	0.5837
279	2020-04-26	02:02:37	54	13.4	9.9	168	221	780	15	1988	14	4.999	0.6011
280	2020-04-26	02:02:38	54	10.2	9.9	168	221	676	13	1854	13	4.999	0.5939
281	2020-04-26	02:02:39	53	6.7	9.9	168	221	52	1	150	1	4.998	0.5831
282	2020-04-26	02:02:40	54	6.2	9.9	168	221	0	0	0	0	5.002	0.5833
283	2020-04-26	02:02:41	54	6.4	9.9	168	221	0	0	0	0	5.001	0.5732
284	2020-04-26	02:02:42	53	6.9	9.9	168	221	52	1	150	1	5.003	0.5662
285	2020-04-26	02:02:43	53	6.9	9.9	168	221	0	0	0	0	5.003	0.5455
286	2020-04-26	02:02:44	52	6.6	9.9	168	222	168	3	410	3	5.003	0.5422
287	2020-04-26	02:02:45	54	16.9	9.9	169	222	260	5	686	5	5.003	0.5375
288	2020-04-26	02:02:46	53	4.9	9.9	169	223	0	0	0	0	5.004	0.552
289	2020-04-26	02:02:47	54	14.1	9.9	169	222	0	0	0	0	5.003	0.6074
290	2020-04-26	02:02:48	54	17	9.9	170	224	260	5	702	5	5.002	0.5192
291	2020-04-26	02:02:49	52	12.6	9.9	170	224	0	0	0	0	5.004	0.5465
292	2020-04-26	02:02:50	53	6.5	9.9	170	223	104	2	276	2	4.999	0.5638
293	2020-04-26	02:02:51	53	13.7	9.9	170	222	0	0	142	1	5.001	0.5503
294	2020-04-26	02:02:52	54	8.8	9.9	169	222	208	4	434	3	5.002	0.5285
295	2020-04-26	02:02:53	54	8.1	9.9	169	222	0	0	0	0	5	0.5503
296	2020-04-26	02:02:54	54	7.3	9.9	169	222	208	4	576	4	4.994	0.519
297	2020-04-26	02:02:55	53	7.8	9.9	169	222	156	3	426	3	4.999	0.5106
298	2020-04-26	02:02:56	53	11.6	9.9	169	222	676	13	1846	13	4.998	0.532

299	2020-04-26	02:02:57	54	11.2	9.9	169	222	676	13	1988	14	4.998	0.5321
300	2020-04-26	02:02:58	53	10.6	9.9	169	223	780	15	1972	14	4.998	0.5432
301	2020-04-26	02:02:59	53	11.5	9.9	169	222	728	14	1988	14	4.997	0.5412
302	2020-04-26	02:03:00	54	17.7	9.9	169	222	364	7	1002	7	4.998	0.5347
303	2020-04-26	02:03:01	54	13.1	9.9	169	222	0	0	0	0	5	0.5371
304	2020-04-26	02:03:02	55	14.6	9.9	169	222	260	5	710	5	5.001	0.5901
305	2020-04-26	02:03:03	52	8.8	9.9	169	222	520	10	1364	10	5.001	0.555
306	2020-04-26	02:03:04	54	16.9	9.9	169	222	468	9	1206	9	5	0.5693
307	2020-04-26	02:03:05	53	5	9.9	169	222	0	0	0	0	5.003	0.5406
308	2020-04-26	02:03:06	53	6.7	9.9	169	222	0	0	0	0	5	0.5583
309	2020-04-26	02:03:07	53	6.7	9.9	169	222	52	1	150	1	5.003	0.5491
310	2020-04-26	02:03:08	53	6.5	9.9	169	222	0	0	0	0	5.001	0.575
311	2020-04-26	02:03:09	53	11.7	9.9	169	222	416	8	1080	8	5.003	0.5666
312	2020-04-26	02:03:09	53	6.3	9.9	169	222	0	0	0	0	5.003	0.5666
313	2020-04-26	02:03:10	52	9.5	9.9	169	222	416	8	1340	10	5.004	0.5768
314	2020-04-26	02:03:12	53	11.5	9.9	169	223	936	18	2114	15	5.003	0.5703
315	2020-04-26	02:03:12	53	12.5	9.9	169	222	844	17	2634	19	5.003	0.5723
316	2020-04-26	02:03:13	53	13.2	9.9	169	222	104	2	292	2	5.002	0.5874
317	2020-04-26	02:03:14	53	22.1	9.9	169	222	260	5	702	5	5.003	0.5844
318	2020-04-26	02:03:15	53	6.3	9.9	169	222	0	0	0	0	5	0.5892
319	2020-04-26	02:03:16	53	6	9.9	169	223	0	0	402	3	5.002	0.6078
320	2020-04-26	02:03:17	53	7.4	9.9	169	222	168	3	0	0	4.999	0.53
321	2020-04-26	02:03:18	52	17.4	9.9	169	222	260	5	702	5	5.004	0.5243
322	2020-04-26	02:03:19	53	5.5	9.9	169	222	0	0	0	0	5.002	0.5243
323	2020-04-26	02:03:20	53	6.4	9.9	169	222	52	1	150	1	5.003	0.5872

324	2020-04-26	02:03:21	54	6.3	9.9	169	222	0	0	0	0	5.003	0.5192
325	2020-04-26	02:03:22	52	6.7	9.9	169	222	0	0	142	1	5.002	0.5245
326	2020-04-26	02:03:23	54	12.2	9.9	169	222	756	13	2182	15	5.003	0.5192
327	2020-04-26	02:03:24	53	13.3	9.9	169	222	780	15	1988	14	5.003	0.5261
328	2020-04-26	02:03:25	53	8.6	9.9	169	222	416	8	1002	7	5.001	0.5463
329	2020-04-26	02:03:26	54	12.7	9.9	169	222	468	9	1206	9	4.998	0.5232
330	2020-04-26	02:03:27	52	13	9.9	169	223	0	0	0	0	4.999	0.5263
331	2020-04-26	02:03:28	54	10.4	9.9	169	223	0	0	0	0	4.997	0.5703
332	2020-04-26	02:03:29	53	13.8	9.9	169	223	364	7	1026	7	4.998	0.5304
333	2020-04-26	02:03:30	53	6.4	9.9	169	223	0	0	0	0	4.997	0.523
334	2020-04-26	02:03:31	53	6.9	9.9	169	223	208	4	528	4	4.994	0.5186
335	2020-04-26	02:03:32	54	9	9.9	169	223	272	5	836	6	5	0.5298
336	2020-04-26	02:03:33	53	10.1	9.9	168	222	908	17	2130	15	5	0.5251

MITM/APT Attack - 25°C													
	Date	T.Stamp	Temp	CPU_Load	Mem_Load	ProNo,	ThreadsNo	RX_bit	RX_pkt	TX_bit	TX_pkt	Voltage(V)	Current(A)
1	2020-04-26	02:12:48	55	28.7	10.5	177	245	0	0	338338	247	4.996	0.6288
2	2020-04-26	02:12:49	55	28.9	10.5	170	238	132	2	286373	207	4.998	0.6204
3	2020-04-26	02:12:50	55	29.4	10.5	170	238	0	0	299031	215	4.994	0.6612
4	2020-04-26	02:12:50	56	30.4	10.5	168	236	52	1	321637	234	4.994	0.6612
5	2020-04-26	02:12:51	56	31.2	10.5	168	236	0	0	326410	238	4.993	0.6795
6	2020-04-26	02:12:52	56	31.1	10.5	168	236	52	1	302407	217	4.991	0.6508
7	2020-04-26	02:12:53	56	32.3	10.5	168	236	0	0	344838	249	4.994	0.6508
8	2020-04-26	02:12:54	56	36.8	10.5	168	236	132	2	333182	239	4.993	0.6443
9	2020-04-26	02:12:55	57	38.9	10.5	169	237	1144	22	135523	116	4.993	0.6432
10	2020-04-26	02:12:56	57	33	10.5	169	237	0	0	142	1	4.992	0.652
11	2020-04-26	02:12:57	56	29.9	10.5	169	237	52	1	49024	37	4.99	0.6504
12	2020-04-26	02:12:58	57	30.4	10.5	168	236	80	1	306798	222	4.991	0.6439
13	2020-04-26	02:12:59	57	30.9	10.5	167	235	52	1	326562	238	4.991	0.6457
14	2020-04-26	02:13:00	57	30.2	10.5	167	235	0	0	337011	239	4.993	0.6579
15	2020-04-26	02:13:01	56	34.7	10.5	167	235	52	1	298018	212	4.993	0.6595
16	2020-04-26	02:13:02	58	31.6	10.5	167	235	337	3	352821	255	4.993	0.6655
17	2020-04-26	02:13:02	58	30.5	10.5	168	236	52	1	342342	243	4.993	0.6655
18	2020-04-26	02:13:03	57	30.2	10.5	168	236	1196	23	140655	122	4.993	0.6681
19	2020-04-26	02:13:04	56	29.3	10.5	168	236	52	1	142	1	4.993	0.654
20	2020-04-26	02:13:05	58	30.4	10.5	168	236	0	0	171735	123	4.993	0.6449
21	2020-04-26	02:13:06	58	33.2	10.5	169	237	0	0	301636	213	4.993	0.6402
22	2020-04-26	02:13:07	59	37.6	10.5	169	237	132	2	319773	229	4.992	0.6426
23	2020-04-26	02:13:08	59	38.4	10.5	169	237	76	1	345586	250	4.99	0.6506

24	2020-04-26	02:13:09	59	32.6	10.5	169	237	52	1	325207	235	4.99	0.654
25	2020-04-26	02:13:10	59	31.7	10.5	169	237	0	0	316264	226	4.99	0.6542
26	2020-04-26	02:13:11	58	30.2	10.5	169	237	52	1	367552	263	4.991	0.6451
27	2020-04-26	02:13:12	58	30.6	10.5	169	237	1692	32	140495	127	4.992	0.6608
28	2020-04-26	02:13:13	57	29.5	10.5	169	237	80	2	208	2	4.993	0.6669
29	2020-04-26	02:13:14	59	30.9	10.5	169	237	0	0	252353	183	4.992	0.6628
30	2020-04-26	02:13:14	58	31.3	10.5	169	237	52	1	317354	230	4.992	0.6628
31	2020-04-26	02:13:15	58	29.8	10.5	169	237	0	0	328314	237	4.994	0.6632
32	2020-04-26	02:13:16	57	30.7	10.5	169	237	0	0	308361	225	4.993	0.651
33	2020-04-26	02:13:17	59	30.2	10.5	169	237	132	2	312574	227	4.992	0.6479
34	2020-04-26	02:13:18	58	31.2	10.5	169	237	0	0	344550	250	4.993	0.6494
35	2020-04-26	02:13:19	59	34.7	10.5	169	237	52	1	325088	236	4.993	0.6494
36	2020-04-26	02:13:20	58	37.7	10.5	169	237	1636	31	195846	171	4.992	0.6512
37	2020-04-26	02:13:21	58	37.2	10.5	169	237	104	2	54963	43	4.991	0.6601
38	2020-04-26	02:13:22	59	31.3	10.5	169	237	0	0	280310	208	4.991	0.6522
39	2020-04-26	02:13:23	57	16.5	10.5	169	237	456	8	306889	236	4.992	0.6526
40	2020-04-26	02:13:24	58	16.1	10.5	169	237	1000	19	538305	396	4.994	0.6282
41	2020-04-26	02:13:25	58	13.9	10.5	170	238	676	13	572352	414	4.997	0.6229
42	2020-04-26	02:13:26	57	13.3	10.5	170	238	780	15	511278	379	4.997	0.6155
43	2020-04-26	02:13:27	57	11.5	10.5	170	238	728	14	518223	380	4.997	0.6221
44	2020-04-26	02:13:28	57	9.6	10.5	170	238	496	9	478763	350	4.997	0.6168
45	2020-04-26	02:13:29	56	10.4	10.5	168	236	2116	40	161327	151	4.997	0.6251
46	2020-04-26	02:13:30	56	8.1	10.5	168	236	416	8	143827	119	4.997	0.6227
47	2020-04-26	02:13:31	56	6.6	10.5	168	236	104	2	62409	57	4.997	0.6111
48	2020-04-26	02:13:32	56	10	10.5	168	237	0	0	25209	34	4.998	0.6094

49	2020-04-26	02:13:32	56	17.2	10.5	169	237	300	5	81377	75	4.998	0.6094
50	2020-04-26	02:13:33	56	19.2	10.5	169	237	676	13	214954	172	4.999	0.6033
51	2020-04-26	02:13:34	57	16	10.5	170	238	832	16	350016	268	4.998	0.6196
52	2020-04-26	02:13:35	57	20.3	10.5	170	238	364	7	404808	297	4.994	0.6251
53	2020-04-26	02:13:36	57	29.1	10.5	169	237	104	2	412353	297	4.996	0.6237
54	2020-04-26	02:13:37	56	10.8	10.5	169	237	1468	28	305828	246	4.997	0.6047
55	2020-04-26	02:13:38	56	7.6	10.5	169	237	548	10	1682	9	4.994	0.6339
56	2020-04-26	02:13:39	57	11.1	10.5	169	237	780	15	271122	207	4.995	0.6056
57	2020-04-26	02:13:40	56	12.4	10.5	169	237	728	14	581056	428	4.996	0.6031
58	2020-04-26	02:13:41	55	9.8	10.5	169	237	364	7	598111	426	4.997	0.5982
59	2020-04-26	02:13:42	55	10.6	10.5	169	237	364	7	609425	434	4.996	0.6051
60	2020-04-26	02:13:43	56	11.2	10.5	169	237	808	15	593066	435	4.995	0.6021
61	2020-04-26	02:13:44	56	7.1	10.5	169	237	156	3	587239	423	4.995	0.6074
62	2020-04-26	02:13:45	56	18.4	10.5	170	238	532	10	619045	454	4.995	0.6029
63	2020-04-26	02:13:46	56	18.7	10.5	170	238	2444	47	226899	203	4.994	0.6019
64	2020-04-26	02:13:47	56	15.9	10.5	170	238	676	13	44772	48	4.993	0.6186
65	2020-04-26	02:13:48	55	8.9	10.5	170	238	416	8	130225	104	4.994	0.6053
66	2020-04-26	02:13:49	55	7.2	10.5	170	239	132	2	205295	153	4.996	0.5996
67	2020-04-26	02:13:50	56	7.6	10.5	170	238	52	1	247170	184	4.996	0.5915
68	2020-04-26	02:13:51	55	7.3	10.5	170	238	0	0	102387	84	4.997	0.6001
69	2020-04-26	02:13:52	56	11.9	10.5	170	238	52	1	95766	89	4.997	0.5964
70	2020-04-26	02:13:53	56	5.5	10.5	170	238	104	2	71333	71	4.996	0.5909
71	2020-04-26	02:13:54	56	7.6	10.5	170	238	0	0	96737	87	4.997	0.6168
72	2020-04-26	02:13:55	56	8	10.5	170	238	1276	24	47472	57	4.998	0.5886
73	2020-04-26	02:13:56	55	8.4	10.5	170	238	0	0	385134	280	4.998	0.5905

74	2020-04-26	02:13:57	55	11.9	10.5	170	238	104	2	547764	394	4.997	0.5837
75	2020-04-26	02:13:58	55	14.8	10.5	170	238	52	1	440059	314	4.997	0.5994
76	2020-04-26	02:13:59	57	12.6	10.5	170	238	0	0	412790	296	4.996	0.6041
77	2020-04-26	02:14:00	56	14.4	10.5	170	238	389	4	362687	267	4.995	0.6072
78	2020-04-26	02:14:01	55	12.6	10.5	170	238	0	0	333627	243	4.996	0.6245
79	2020-04-26	02:14:02	55	7.3	10.5	171	239	52	1	184766	146	4.997	0.5982
80	2020-04-26	02:14:03	55	6.9	10.5	171	239	1300	25	99164	105	4.996	0.6227
81	2020-04-26	02:14:04	55	9.5	10.5	171	239	780	15	2806	15	4.998	0.609
82	2020-04-26	02:14:05	55	12.8	10.5	171	239	832	16	15613	27	4.999	0.6157
83	2020-04-26	02:14:06	55	12.7	10.5	171	239	780	15	556006	407	4.999	0.6108
84	2020-04-26	02:14:07	56	7.4	10.5	171	239	288	5	756116	533	4.998	0.617
85	2020-04-26	02:14:08	55	15.8	10.5	171	239	208	4	680758	484	4.997	0.6282
86	2020-04-26	02:14:09	56	7.4	10.5	171	239	0	0	609782	428	4.997	0.6247
87	2020-04-26	02:14:10	56	8.4	10.5	171	239	104	2	475679	340	4.995	0.6274
88	2020-04-26	02:14:11	55	13.7	10.5	171	239	0	0	197868	153	4.996	0.6245
89	2020-04-26	02:14:12	55	16.7	10.5	171	239	1548	29	64336	78	4.998	0.6233
90	2020-04-26	02:14:12	56	15.7	10.5	171	239	208	4	560	4	4.998	0.6233
91	2020-04-26	02:14:13	56	7.9	10.5	172	240	0	0	106521	89	4.997	0.6255
92	2020-04-26	02:14:14	56	9.2	10.5	172	240	416	8	189608	153	4.997	0.6491
93	2020-04-26	02:14:15	55	8.7	10.5	172	240	104	2	244755	185	4.997	0.6078
94	2020-04-26	02:14:16	55	6.5	10.5	172	240	0	0	110523	89	4.999	0.6135
95	2020-04-26	02:14:17	56	7.4	10.5	171	239	80	1	137805	109	4.998	0.6204
96	2020-04-26	02:14:18	55	14.7	10.5	171	239	208	4	109212	90	4.998	0.6088
97	2020-04-26	02:14:19	55	7.5	10.5	171	239	0	0	152956	132	4.998	0.6149
98	2020-04-26	02:14:20	56	7.6	10.5	171	239	1300	25	46810	61	4.998	0.6544

99	2020-04-26	02:14:21	55	6	10.5	171	239	184	3	341224	244	4.999	0.5882
100	2020-04-26	02:14:22	55	9.5	10.5	171	239	0	0	650837	456	4.998	0.5933
101	2020-04-26	02:14:23	55	13.3	10.5	171	239	52	1	659727	463	4.999	0.5934
102	2020-04-26	02:14:24	55	15.1	10.5	171	239	0	0	756026	530	4.998	0.5911
103	2020-04-26	02:14:25	55	15.3	10.5	171	239	132	2	630347	450	4.998	0.6278
104	2020-04-26	02:14:26	55	14.3	10.5	171	240	676	13	619877	443	4.995	0.6147
105	2020-04-26	02:14:27	56	15.1	10.5	171	239	676	13	554701	402	4.996	0.6284
106	2020-04-26	02:14:28	55	15.4	10.5	171	239	1248	24	634375	467	4.997	0.6108
107	2020-04-26	02:14:29	56	12.2	10.5	171	239	1560	30	32004	49	4.997	0.6123
108	2020-04-26	02:14:30	55	9.9	10.5	171	239	624	12	1680	12	4.997	0.6111
109	2020-04-26	02:14:31	56	7	10.5	171	239	132	2	286998	207	4.997	0.5998
110	2020-04-26	02:14:32	55	7.5	10.5	171	239	0	0	587016	415	4.998	0.5962
111	2020-04-26	02:14:33	55	7	10.5	171	239	52	1	563220	399	4.997	0.5986
112	2020-04-26	02:14:34	56	11.3	10.5	172	240	0	0	555439	392	4.996	0.6015
113	2020-04-26	02:14:35	56	11.7	10.5	172	241	260	5	488714	352	4.997	0.5998
114	2020-04-26	02:14:36	55	12.8	10.5	172	240	0	0	523848	369	4.996	0.6045
115	2020-04-26	02:14:37	56	23.3	10.5	172	240	1588	30	611542	462	4.992	0.5937
116	2020-04-26	02:14:38	56	12.6	10.5	172	240	884	17	3134	17	4.996	0.6249
117	2020-04-26	02:14:39	56	7.2	10.5	172	240	0	0	120553	87	4.994	0.6587
118	2020-04-26	02:14:40	55	9.9	10.5	172	240	52	1	658609	464	4.996	0.5919
119	2020-04-26	02:14:41	55	12.5	10.5	172	240	600	11	668398	485	4.997	0.5962
120	2020-04-26	02:14:42	55	11.7	10.5	172	240	676	13	497783	369	4.996	0.5886
121	2020-04-26	02:14:43	55	12	10.5	172	240	832	16	297783	231	4.995	0.6082
122	2020-04-26	02:14:44	56	6.7	10.5	172	240	104	2	250793	185	4.995	0.599
123	2020-04-26	02:14:45	56	12.7	10.5	172	240	1144	22	524481	397	4.996	0.5976

124	2020-04-26	02:14:46	56	12.4	10.5	172	240	1924	37	419027	325	4.997	0.5948
125	2020-04-26	02:14:47	56	25.6	10.5	172	240	496	9	77815	64	4.997	0.6035
126	2020-04-26	02:14:48	56	18.2	10.5	172	240	520	10	677787	487	4.995	0.5929
127	2020-04-26	02:14:49	56	14.2	10.5	172	240	208	4	638974	462	4.994	0.6485
128	2020-04-26	02:14:50	55	15.4	10.5	172	240	468	9	459413	333	4.995	0.6072
129	2020-04-26	02:14:51	55	17	10.5	172	240	884	17	570881	422	4.995	0.6274
130	2020-04-26	02:14:52	56	11.6	10.5	172	240	780	15	519881	379	4.995	0.6331
131	2020-04-26	02:14:53	56	13.1	10.5	172	240	1144	22	662261	487	4.995	0.6306
132	2020-04-26	02:14:54	56	14.3	10.5	172	240	1484	28	635438	468	4.996	0.6284
133	2020-04-26	02:14:55	55	11.4	10.5	172	240	1624	31	422715	329	4.996	0.6188
134	2020-04-26	02:14:55	56	13.5	10.5	172	240	208	4	493699	355	4.996	0.6188
135	2020-04-26	02:14:56	56	15.8	10.5	172	240	272	5	531450	383	4.996	0.6212
136	2020-04-26	02:14:57	55	7.1	10.5	172	240	0	0	543546	385	4.997	0.6025
137	2020-04-26	02:14:58	55	10.9	10.5	172	240	462	3	591765	419	4.995	0.6483
138	2020-04-26	02:14:59	55	10.2	10.5	172	240	324	6	499100	364	4.995	0.6041
139	2020-04-26	02:15:00	56	8.3	10.5	172	240	0	0	598848	430	4.997	0.6005
140	2020-04-26	02:15:01	56	26.3	10.5	172	240	236	4	628946	450	4.995	0.6031
141	2020-04-26	02:15:02	56	13	10.5	172	240	52	1	564789	407	4.997	0.6032
142	2020-04-26	02:15:03	56	15.3	10.5	172	240	1196	23	482339	362	4.996	0.6284
143	2020-04-26	02:15:04	56	15.4	10.5	172	240	964	18	2870	17	4.994	0.6115
144	2020-04-26	02:15:05	55	7.4	10.5	172	240	104	2	190549	139	4.992	0.609
145	2020-04-26	02:15:06	55	10.1	10.5	172	241	208	4	423287	311	4.994	0.5974
146	2020-04-26	02:15:07	56	8.2	10.5	172	240	0	0	489545	348	4.996	0.5988
147	2020-04-26	02:15:08	57	20.4	10.5	172	240	104	2	615200	442	4.993	0.5929
148	2020-04-26	02:15:09	55	5.3	10.5	172	240	132	2	544672	385	4.995	0.6023

149	2020-04-26	02:15:10	56	7.9	10.5	172	240	0	0	626645	447	4.994	0.6465
150	2020-04-26	02:15:11	55	9.3	10.5	172	240	52	1	732429	521	4.995	0.588
151	2020-04-26	02:15:12	55	7	10.5	172	240	988	19	405467	305	4.995	0.6019
152	2020-04-26	02:15:13	56	9.3	10.5	172	240	444	8	99804	80	4.997	0.5948
153	2020-04-26	02:15:14	55	8.8	10.5	172	240	52	1	635604	448	4.996	0.598
154	2020-04-26	02:15:15	56	15.1	10.5	172	240	0	0	559379	395	4.997	0.5952
155	2020-04-26	02:15:16	55	17.4	10.5	172	241	416	7	676892	481	4.997	0.6017
156	2020-04-26	02:15:17	56	15.6	10.5	173	241	676	13	629806	457	4.996	0.6202
157	2020-04-26	02:15:18	55	11.9	10.5	173	241	728	14	473484	352	4.995	0.6235
158	2020-04-26	02:15:19	55	10.9	10.5	173	241	780	15	325168	249	4.996	0.6072
159	2020-04-26	02:15:20	56	12.1	10.5	172	241	676	13	441097	326	4.997	0.6
160	2020-04-26	02:15:21	56	12.6	10.5	172	240	2864	55	295040	258	4.997	0.6273
161	2020-04-26	02:15:22	55	7.8	10.5	172	241	364	7	605294	432	4.997	0.6272
162	2020-04-26	02:15:23	56	8.4	10.5	173	241	52	1	744691	523	4.997	0.6223
163	2020-04-26	02:15:24	55	8.7	10.5	173	241	0	0	488707	350	4.997	0.6265
164	2020-04-26	02:15:25	55	10.1	10.5	173	241	340	6	140934	117	4.997	0.6314
165	2020-04-26	02:15:26	55	8.8	10.5	173	241	0	0	139678	110	4.999	0.6153
166	2020-04-26	02:15:27	55	7.4	10.5	173	241	52	1	183920	145	4.998	0.6225
167	2020-04-26	02:15:28	56	14.8	10.5	173	241	0	0	228670	168	4.999	0.62
168	2020-04-26	02:15:29	55	14.7	10.5	173	241	156	3	469510	339	4.998	0.6241
169	2020-04-26	02:15:29	56	17.1	10.5	173	241	2168	41	337671	275	4.998	0.6241
170	2020-04-26	02:15:30	55	11.1	10.5	173	241	912	17	2496	16	4.996	0.6198
171	2020-04-26	02:15:31	56	7.6	10.5	173	241	0	0	436446	309	4.995	0.6326
172	2020-04-26	02:15:32	55	10.9	10.5	173	241	156	3	560049	399	4.997	0.5998
173	2020-04-26	02:15:33	55	7.5	10.5	173	241	0	0	544170	390	4.999	0.6019

174	2020-04-26	02:15:34	56	12.7	10.5	173	241	364	7	615663	442	4.997	0.6015
175	2020-04-26	02:15:35	55	10.8	10.5	173	241	444	8	575199	411	4.997	0.6051
176	2020-04-26	02:15:36	55	7.6	10.5	173	241	0	0	579061	413	4.998	0.6084
177	2020-04-26	02:15:37	56	10.8	10.5	173	241	416	8	552219	400	4.997	0.6064
178	2020-04-26	02:15:38	55	11.5	10.5	173	241	2496	48	135396	137	4.998	0.6062
179	2020-04-26	02:15:39	56	11.4	10.5	173	241	884	17	294760	228	4.998	0.6106
180	2020-04-26	02:15:40	56	14.2	10.5	173	241	104	2	462182	334	4.997	0.5986
181	2020-04-26	02:15:41	56	13.3	10.5	173	241	80	1	525596	378	4.997	0.6041
182	2020-04-26	02:15:42	56	11.6	10.5	173	241	0	0	456422	323	4.996	0.6149
183	2020-04-26	02:15:43	55	8.5	10.5	173	241	52	1	507517	367	4.995	0.6094
184	2020-04-26	02:15:44	55	7.9	10.5	173	241	0	0	460735	330	4.995	0.6198
185	2020-04-26	02:15:45	56	6.8	10.5	173	241	52	1	502429	360	4.995	0.596
186	2020-04-26	02:15:46	55	6.5	10.5	173	242	0	0	623477	440	4.996	0.6041
187	2020-04-26	02:15:47	55	7.7	10.5	173	241	1484	28	195326	162	4.995	0.5962
188	2020-04-26	02:15:48	55	10.3	10.5	173	241	480	9	1278	9	4.996	0.6051
189	2020-04-26	02:15:49	55	9.9	10.5	173	241	728	14	170292	136	4.995	0.5878
190	2020-04-26	02:15:50	55	11.1	10.5	173	241	584	11	358488	270	4.997	0.6035
191	2020-04-26	02:15:51	55	7.3	10.5	173	241	52	1	159135	122	4.996	0.6007
192	2020-04-26	02:15:52	55	9	10.5	173	241	104	2	160661	129	4.995	0.598
193	2020-04-26	02:15:53	55	19.4	10.5	173	241	780	15	252283	200	4.996	0.5921
194	2020-04-26	02:15:54	55	20.2	10.5	173	242	728	14	462382	346	4.997	0.5905
195	2020-04-26	02:15:55	55	17.3	10.5	174	243	572	11	704970	510	4.996	0.6125
196	2020-04-26	02:15:56	55	14.2	10.5	174	242	1572	30	134057	120	4.995	0.6123
197	2020-04-26	02:15:57	55	5.8	10.5	174	242	309	3	61829	48	4.995	0.5998
198	2020-04-26	02:15:58	56	6.3	10.5	174	242	0	0	481509	340	4.998	0.6194

199	2020-04-26	02:15:59	55	7.5	10.5	173	241	132	2	222550	170	4.997	0.6041
200	2020-04-26	02:16:00	56	13.9	10.5	173	241	0	0	102837	82	4.997	0.6039
201	2020-04-26	02:16:01	55	16.4	10.5	173	241	156	3	106736	88	4.998	0.6013
202	2020-04-26	02:16:02	55	5.5	10.5	173	241	0	0	107674	85	4.998	0.6011
203	2020-04-26	02:16:03	55	7.4	10.5	173	242	52	1	159966	131	4.994	0.6092
204	2020-04-26	02:16:04	55	8.1	10.5	173	241	0	0	297133	221	4.999	0.6129
205	2020-04-26	02:16:05	55	10.9	10.5	173	241	2108	39	124022	123	4.998	0.6131
206	2020-04-26	02:16:06	56	12.9	10.5	173	241	52	1	393237	281	4.998	0.6223
207	2020-04-26	02:16:07	55	13.7	10.5	173	242	0	0	419500	298	4.997	0.6108
208	2020-04-26	02:16:08	55	14.4	10.5	173	242	104	2	469994	334	4.996	0.6369
209	2020-04-26	02:16:09	55	11.6	10.5	173	241	572	11	544257	399	4.996	0.6243
210	2020-04-26	02:16:10	55	8	10.5	173	241	0	0	465042	331	4.995	0.6245
211	2020-04-26	02:16:11	56	10	10.5	173	241	236	4	581566	417	4.997	0.6218
212	2020-04-26	02:16:12	55	13.5	10.5	173	241	676	13	471997	349	4.997	0.6108
213	2020-04-26	02:16:12	55	13.1	10.5	173	241	728	14	509042	371	4.997	0.6108
214	2020-04-26	02:16:13	55	9.3	10.5	173	241	1952	37	207184	182	4.997	0.6139
215	2020-04-26	02:16:14	55	6.5	10.5	173	241	52	1	150	1	4.997	0.61
216	2020-04-26	02:16:15	56	7.2	10.5	173	241	0	0	340891	249	4.998	0.6064
217	2020-04-26	02:16:16	56	9.6	10.5	173	241	116	2	516303	369	4.999	0.5886
218	2020-04-26	02:16:17	55	14.7	10.5	173	241	676	13	476014	348	4.998	0.6007
219	2020-04-26	02:16:18	56	13.6	10.5	173	241	404	7	495598	359	4.997	0.5978
220	2020-04-26	02:16:19	55	16	10.5	173	241	156	3	426277	310	4.997	0.6064
221	2020-04-26	02:16:20	55	14.1	10.5	173	241	128	2	500509	358	4.997	0.6096
222	2020-04-26	02:16:21	56	9.7	10.5	173	241	0	0	515111	370	4.996	0.6055
223	2020-04-26	02:16:22	55	8.7	10.5	173	241	1248	24	285746	224	4.996	0.6149

224	2020-04-26	02:16:23	55	7.4	10.5	173	241	444	8	264114	199	4.996	0.5966
225	2020-04-26	02:16:24	55	7.6	10.5	173	241	52	1	474398	340	4.995	0.6019
226	2020-04-26	02:16:25	54	8.3	10.5	173	241	28	1	434044	313	4.997	0.5815
227	2020-04-26	02:16:26	54	9.4	10.5	173	241	260	5	428240	311	4.996	0.6025
228	2020-04-26	02:16:27	56	7.9	10.5	173	241	208	4	345876	257	4.997	0.6013
229	2020-04-26	02:16:28	55	8.3	10.5	173	241	0	0	369183	267	4.997	0.6108
230	2020-04-26	02:16:29	55	7.3	10.5	173	241	104	2	583585	416	4.995	0.5978
231	2020-04-26	02:16:30	55	6.8	10.5	173	241	80	1	542258	388	4.995	0.6033
232	2020-04-26	02:16:31	56	11.7	10.5	173	241	1196	23	377512	292	4.996	0.6036
233	2020-04-26	02:16:32	56	20.3	10.5	173	241	1508	29	4224	28	4.995	0.6032
234	2020-04-26	02:16:33	56	16.1	10.5	173	241	652	12	248302	185	4.995	0.6029
235	2020-04-26	02:16:34	55	7.9	10.5	173	241	0	0	575466	403	4.995	0.6119
236	2020-04-26	02:16:35	56	10.1	10.5	173	241	208	4	556903	400	4.995	0.621
237	2020-04-26	02:16:36	55	11.2	10.5	173	241	780	15	389414	297	4.995	0.6025
238	2020-04-26	02:16:37	55	10.3	10.5	173	241	416	8	196037	160	4.996	0.6135
239	2020-04-26	02:16:38	57	7.7	10.5	173	241	184	3	128904	99	4.996	0.5954
240	2020-04-26	02:16:39	55	7.2	10.5	173	241	0	0	226075	168	4.997	0.5886
241	2020-04-26	02:16:40	55	7.5	10.5	173	241	988	19	372767	285	4.997	0.5811
242	2020-04-26	02:16:41	55	7.5	10.5	173	241	572	11	75404	63	4.998	0.5921
243	2020-04-26	02:16:42	55	13.2	10.5	173	241	156	3	724761	512	4.997	0.5813
244	2020-04-26	02:16:43	55	12.5	10.5	173	241	912	17	644926	469	4.997	0.5909
245	2020-04-26	02:16:44	55	10.5	10.5	173	241	0	0	462262	325	4.997	0.6145
246	2020-04-26	02:16:45	56	15.6	10.5	173	241	52	1	495636	356	4.996	0.6013
247	2020-04-26	02:16:46	55	13.7	10.5	173	241	0	0	453427	320	4.997	0.6202
248	2020-04-26	02:16:47	55	19.2	10.5	173	241	208	4	467449	335	4.997	0.6508

249	2020-04-26	02:16:48	56	8.8	10.5	173	241	0	0	602366	423	4.996	0.6492
250	2020-04-26	02:16:49	56	10.4	10.5	173	241	704	13	908956	646	4.995	0.6263
251	2020-04-26	02:16:50	55	6.8	10.5	173	241	1092	21	10338	26	4.997	0.6262
252	2020-04-26	02:16:51	55	7.6	10.5	173	241	52	1	150	1	4.996	0.6194
253	2020-04-26	02:16:52	55	7.5	10.5	173	241	0	0	638959	451	4.998	0.6231
254	2020-04-26	02:16:53	55	8.6	10.5	173	241	52	1	709119	500	4.998	0.6371
255	2020-04-26	02:16:54	55	8.9	10.5	173	241	338	3	748674	526	4.997	0.6306
256	2020-04-26	02:16:55	55	13.5	10.5	173	241	480	9	535029	388	4.997	0.61
257	2020-04-26	02:16:56	55	12.8	10.5	173	241	752	14	554899	407	4.996	0.6219
258	2020-04-26	02:16:57	55	15.8	10.5	173	241	676	13	609606	448	4.996	0.6137
259	2020-04-26	02:16:57	55	15.1	10.5	173	241	244	4	647289	468	4.996	0.6137
260	2020-04-26	02:16:58	55	18.6	10.5	173	241	2168	40	103443	108	4.995	0.6108
261	2020-04-26	02:16:59	55	13.2	10.5	173	241	440	8	396681	295	4.995	0.6239
262	2020-04-26	02:17:00	56	17.5	10.5	173	241	0	0	622768	442	4.995	0.6186
263	2020-04-26	02:17:01	55	16.7	10.5	173	241	208	4	549826	397	4.996	0.6027
264	2020-04-26	02:17:02	56	8	10.5	173	241	0	0	605345	428	4.997	0.6314
265	2020-04-26	02:17:03	55	7.8	10.5	173	241	52	1	552073	399	4.996	0.5988
266	2020-04-26	02:17:04	55	8.4	10.5	173	241	0	0	595909	424	4.995	0.6049
267	2020-04-26	02:17:05	56	8.6	10.5	173	241	132	2	644065	457	4.995	0.6027
268	2020-04-26	02:17:06	55	7.7	10.5	173	241	0	0	676800	481	4.995	0.6078
269	2020-04-26	02:17:07	55	11	10.5	173	241	1716	33	205197	175	4.996	0.6055
270	2020-04-26	02:17:08	55	11.5	10.5	173	241	676	13	1846	13	4.995	0.6055
271	2020-04-26	02:17:09	55	14.4	10.5	173	241	780	15	306911	232	4.996	0.5966
272	2020-04-26	02:17:10	55	16.7	10.5	173	242	652	12	552395	402	4.995	0.5962
273	2020-04-26	02:17:11	57	20.7	10.5	174	242	0	0	504022	358	4.995	0.6021

274	2020-04-26	02:17:12	57	33.4	10.5	174	242	0	0	621033	440	4.994	0.6153
275	2020-04-26	02:17:13	56	30	10.5	174	242	52	1	603975	422	4.995	0.6384
276	2020-04-26	02:17:14	58	30.4	10.5	173	241	52	1	620664	435	4.991	0.6585
277	2020-04-26	02:17:15	58	30.2	10.5	173	241	0	0	691220	488	4.991	0.6614
278	2020-04-26	02:17:16	58	31.4	10.5	173	241	1484	28	596167	443	4.988	0.6948
279	2020-04-26	02:17:17	58	30.3	10.5	173	241	936	18	2904	16	4.991	0.6795
280	2020-04-26	02:17:18	58	31.3	10.5	173	241	0	0	584955	411	4.991	0.6724
281	2020-04-26	02:17:19	59	30.7	10.5	173	241	52	1	634882	439	4.992	0.6727
282	2020-04-26	02:17:19	59	31.9	10.5	173	241	0	0	599458	418	4.992	0.6727
283	2020-04-26	02:17:20	58	30.2	10.5	173	241	132	2	588403	408	4.992	0.6561
284	2020-04-26	02:17:21	58	33.2	10.5	173	241	0	0	637125	444	4.991	0.6587
285	2020-04-26	02:17:22	59	34.4	10.5	173	241	52	1	650877	452	4.991	0.6709
286	2020-04-26	02:17:23	60	37.7	10.5	173	241	0	0	600268	417	4.991	0.6587
287	2020-04-26	02:17:24	58	37.5	10.5	173	241	52	1	682480	475	4.99	0.6767
288	2020-04-26	02:17:25	59	33.7	10.5	173	241	1900	36	487490	371	4.99	0.6728
289	2020-04-26	02:17:26	59	29.3	10.5	173	241	520	10	2044	10	4.99	0.6742
290	2020-04-26	02:17:27	60	30.1	10.5	173	241	52	1	93064	69	4.991	0.6559
291	2020-04-26	02:17:28	60	30.2	10.5	173	241	0	0	589623	408	4.994	0.6693
292	2020-04-26	02:17:29	59	31.7	10.5	173	241	52	1	640732	447	4.992	0.6805
293	2020-04-26	02:17:30	59	29.8	10.5	173	241	0	0	628310	438	4.992	0.6815
294	2020-04-26	02:17:31	60	31.4	10.6	173	241	132	2	569665	395	4.992	0.6679
295	2020-04-26	02:17:31	60	31.1	10.5	173	241	0	0	651510	452	4.992	0.6679
296	2020-04-26	02:17:32	60	31	10.5	173	241	52	1	625081	435	4.992	0.6683
297	2020-04-26	02:17:33	59	32.1	10.5	173	241	0	0	696446	495	4.993	0.6661
298	2020-04-26	02:17:34	60	30.4	10.5	173	241	1336	25	362201	281	4.993	0.6683

299	2020-04-26	02:17:35	59	34.9	10.5	173	241	260	5	275051	198	4.992	0.6705
300	2020-04-26	02:17:36	58	12.3	10.5	173	241	184	3	558971	398	4.991	0.653
301	2020-04-26	02:17:37	58	12.9	10.5	173	241	0	0	522120	373	4.992	0.6491
302	2020-04-26	02:17:38	58	19.7	10.5	173	241	208	4	642104	457	4.995	0.6074
303	2020-04-26	02:17:39	59	19.6	10.5	173	241	480	9	593728	426	4.996	0.6035
304	2020-04-26	02:17:40	59	30.3	10.5	173	241	52	1	627217	444	4.99	0.6
305	2020-04-26	02:17:41	59	21.6	10.5	173	241	444	8	597669	434	4.993	0.6379
306	2020-04-26	02:17:42	60	25.1	10.5	173	241	208	4	701839	501	4.989	0.651
307	2020-04-26	02:17:43	58	29.4	10.5	173	241	624	12	736628	533	4.991	0.6227
308	2020-04-26	02:17:44	59	22	10.5	173	241	1976	38	59162	75	4.99	0.6204
309	2020-04-26	02:17:45	57	11.5	10.5	173	241	676	13	1846	13	4.989	0.597
310	2020-04-26	02:17:46	57	12	10.5	173	241	808	15	546338	395	4.993	0.5656
311	2020-04-26	02:17:46	58	22.6	10.5	173	241	364	7	613279	439	4.993	0.5656
312	2020-04-26	02:17:47	58	28.9	10.5	173	241	104	2	562576	403	4.991	0.573
313	2020-04-26	02:17:48	58	33.4	10.5	173	241	156	3	380452	275	4.992	0.5948
314	2020-04-26	02:17:49	58	23.9	10.5	173	241	468	9	327087	246	4.989	0.6445
315	2020-04-26	02:17:50	57	13.5	10.5	173	241	808	15	382228	291	4.991	0.6163
316	2020-04-26	02:17:51	57	6.5	10.5	173	242	156	3	167712	134	4.988	0.5727
317	2020-04-26	02:17:52	57	8.1	10.5	173	242	1610	28	53134	66	4.986	0.5711
318	2020-04-26	02:17:53	57	7.4	10.5	173	242	312	6	146349	113	4.989	0.5603
319	2020-04-26	02:17:54	57	12	10.5	173	242	52	1	400790	292	4.989	0.5697
320	2020-04-26	02:17:55	58	17.9	10.5	173	242	132	2	315083	229	4.988	0.5338
321	2020-04-26	02:17:56	57	9.3	10.5	173	242	240	4	267763	197	4.979	0.5444
322	2020-04-26	02:17:57	56	7.1	10.5	173	243	0	0	464281	333	4.979	0.5632
323	2020-04-26	02:17:58	56	8.2	10.5	173	242	168	3	453328	326	4.978	0.5346

324	2020-04-26	02:17:59	57	7.9	10.5	173	242	80	1	339698	247	4.98	0.5428
325	2020-04-26	02:18:00	57	18.4	10.5	173	242	52	1	123545	98	4.979	0.5271
326	2020-04-26	02:18:01	57	24.6	10.5	173	243	912	18	80474	83	4.98	0.5575
327	2020-04-26	02:18:02	56	12.1	10.5	173	242	832	16	3204	16	4.992	0.6239
328	2020-04-26	02:18:03	56	11.8	10.5	174	243	52	1	11005	12	4.991	0.5911
329	2020-04-26	02:18:04	56	7	10.5	174	243	208	4	124235	103	4.994	0.5937
330	2020-04-26	02:18:05	57	12.6	10.5	174	243	884	17	311085	241	4.993	0.5846
331	2020-04-26	02:18:06	55	9.9	10.5	172	242	392	7	635562	453	4.994	0.5899
332	2020-04-26	02:18:07	56	12.1	10.5	172	240	364	7	637073	455	4.993	0.5962
333	2020-04-26	02:18:08	56	8.7	10.5	172	240	156	3	663696	473	4.992	0.6009
334	2020-04-26	02:18:09	56	9.4	10.5	172	240	0	0	591785	417	4.992	0.6041
335	2020-04-26	02:18:10	56	13.2	10.5	172	241	468	9	755699	540	4.994	0.5874
336	2020-04-26	02:18:11	56	13.7	10.5	171	239	2368	45	236775	204	4.989	0.5958