IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 13 June 2023, accepted 6 July 2023, date of publication 17 July 2023, date of current version 31 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3296311

RESEARCH ARTICLE

5G Aviation Networks Using Novel AI Approach for DDoS Detection

HUW WHITWORTH[1], SABA AL-RUBAYE[1], (Life Senior Member, IEEE), ANTONIOS TSOURDOS[1], AND JULIA JIGGINS[2]

[1]School of Aerospace, Cranfield University, MK43 0AL Cranfield, U.K.
[2]Thales Avionics, Thales UK, RH10 9HA Crawley, U.K.

Corresponding author: Huw Whitworth (h.t.whitworth@cranfield.ac.uk)

This work was supported in part by the grant received from the Department for Transport (DfT), U.K. Government under the Future Aviation Security Solutions Industrial Ph.D. Partnerships (FASS IPPs), and in part by Thales, U.K.

ABSTRACT The advent of Fifth Generation (5G) technology has ushered in a new era of advancements in the aviation sector. However, the introduction of smart infrastructure has significantly altered the threat landscape at airports, leading to an increased vulnerability due to the proliferation of endpoints. Consequently, there is an urgent requirement for an automated detection system capable of promptly identifying and thwarting network intrusions. This research paper proposes a deep learning methodology that merges a Convolutional Neural Network (CNN) with a Gated Recurrent Unit (GRU) to effectively detect various types of cyber threats using tabular-based image data. To transform time series features into 2D texture images, Gramian Angular Fields (GAFs) are utilized. These images are then stacked to form an N-channel image, which is fed into the CNN-GRU architecture for sequence analysis and identification of potential threats. The provide solution GAF-CNN-GRU achieved an accuracy of 98.6% on the Cranfield Embedded Systems Attack Dataset. We further achieved Precision, Recall and F1-scores of 97.84%, 91% and 94.3%. To evaluate model robustness we further tested this approach, using a benchmark random selection of input features, on the Canadian Institute for Cyber-Security (CIC) 2019 Distributed Denial-of-service attack (DDoS) Dataset achieving an Accuracy of 89.08%. Following feature optimisation our approach was able to achieve an accuracy of 98.36% with Precision, Recall and F1 scores of 93.09%, 95.45% and 94.56% respectively.

INDEX TERMS Aviation, cyber security, denial-of-service attack (DoS), fifth generation (5G), digital aviation, neural network, time series.

I. INTRODUCTION

The future aviation communications topology is one based on rapid, network centric operations. Traditional communications methods such as Very High Frequency (VHF) and the Aircraft Communications, Addressing and Reporting System (ACARS) are no longer suitable for the high rate, low latency communications expected by both Airline Service Providers and Passengers. To meet this expectation standard Internet Protocol (IP) based systems are deployed for both air-side and land-side operation for services ranging from Electronic Flight Bags (EFBs) to real time passenger infotainment. The migration from legacy systems to IP driven topologies has allowed Airline Service Providers and the wider airport domain to automate previously manual processes. This has been done through a heterogeneous, real time, omnipresent data exchange structure that enables data exchanges between the airport, aircraft, and ground crews. This provides a medium to transfer performance, safety and entertainment data in a fast efficient manner [1]. The core benefits of IP system deployment are:

- Real Time Data Transfer
- Access to Performance Data in flight
- Access to Safety Data in flight

The associate editor coordinating the review of this manuscript and approving it for publication was Peng-Yong Kong.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

- Reduction in Aircraft downtime due to expedited data transfer rates
- Potential performance and efficiency increase

Despite the advantages of next gen systems, those utilising Internet Protocol Version 6 (IPV6) or based on 5G architecture, such as increased transmission rate, performance and efficiency [2], [3]; deployment of open loop wireless topologies results in the expansion of the aviation threat landscape.

The proliferation of smart technology within the aviation domain has generated an increase in the number of potential attack points for cyber criminals [4]. Unprotected terminals and networks can be accessed and misused by malicious actors to gain access, edit or delete data. Therefore, any host device deployed to a public or shared area network should be viewed as a target for cyber criminals. Given the evolution of attacker strategies [5] detection methods must adjust accordingly – focusing on the intricacies and inter-dependencies of the user network interaction. The development of novel attack stratagems is a constant issue within the cyber and information security domain. While researchers and industry develop new methods of detection and mitigation, threat actors work to find flaws in defensive solutions through both novel and modified attack vectors. A current method that is gaining popularity within the domain is the modified Distributed Denial of Service (DDoS) attack, Distributed Reflective Denial of Service (DrDoS) - depicted in Figure 1.

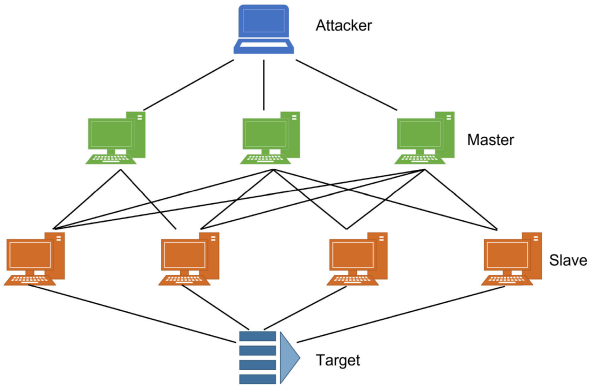


FIGURE 1. Structure of a DrDoS attack.

Attacks against system availability for a broad scope of services that utilise IP or 5G cellular protocols have become a popular attack vector [6]. To facilitate a DrDoS attack the malicious actor sends a forged request from a victim's spoofed IP address to multiple servers. The server in question then transmits replies to the victim node in much greater quantity than the initial request. The optimal result for the attacker is the bandwidth or other targeted system resource depleted and the victim unable to function within the bounds of standard operation.

While the flexibility given by 5G sliced cellular networks promotes the ideal solution for intra-environment aviation connectivity, there are several fundamental security concerns that need to be addressed. Standard DRDoS detection methods operate for specific protocols, evaluating the statistical relationship between client server pairs looking for asymmetry [7]. Unfortunately, while effective in a niche environment, protocol driven Intrusion Detection Systems (IDSs) often fail to detect novel DrDoS attacks which utilises a different protocol. As such protocol agnostic solutions are required.

The principal issue with AI deployment within cyber security is the need for much higher accuracy and discriminatory ability than is currently being achieved. The automatic segregation and filtering that is a hallmark of machine learning has the potential to be just as disruptive as a deployed cyber attack. Wherein the incorrect detection of normal traffic as malicious results in obtaining a high false positive rate within the system. In this instance the system will often block or drop benign user traffic. Traditional methods of anomalous behaviour detection based on statistical methods can be prone to identifying sufficiently diverged legitimate traffic as anomalous. Existing deep learning approaches primarily utilise convolutional Neural Networks (CNNs) [8] or some derivation of the Recurrent Neural Network (RNN) architecture. The use of convolutional methods to classify non-image data does not utilise the full advantage CNN capability as methods that operate on tabular data are unable to learn and use the feature relationships to improve the prediction performance and therein their accuracy. We propose a novel solution - inspired from work done by [9] who used the Python Matplotlib functionality to map IEEE 14-bus and IEEE 1180-bus system states to 2D images to detect cyber anomalies. The innovative contribution of this paper lies in its exploration of a new aspect by focusing on classifying the transition in network state from benign to attack. The novelty is achieved through the development of a unique approach that combines benign and attack traffic types, simulating the sudden change in network performance metrics during a DDoS attack. This hybrid approach is then fed into a CNN-GRU architecture, enabling the classification of network traffic state by analysing multivariate time series and extracting spatial and temporal features simultaneously. Given the background research and existing literature regarding DDoS attack detection the contribution of this paper is as follows:

- Unlike previous work this paper explores classifying the change in network state from benign to attack. This has been achieved by splicing together benign and attack traffic types in order to simulate the sudden change in network performance metrics that occur when a system is under DDoS attack and fed in to a CNN-GRU architecture.
- We propose a novel framework for the classification of network traffic state via multivariate time series analysis of dynamic network statistics in the form a hybrid CNN-GRU model. The hybrid approach combines the benefits of the CNN such as noise filtering of the input data and automatic feature extraction, with the GRU ability for effective learning. In addition, the GRU relies on

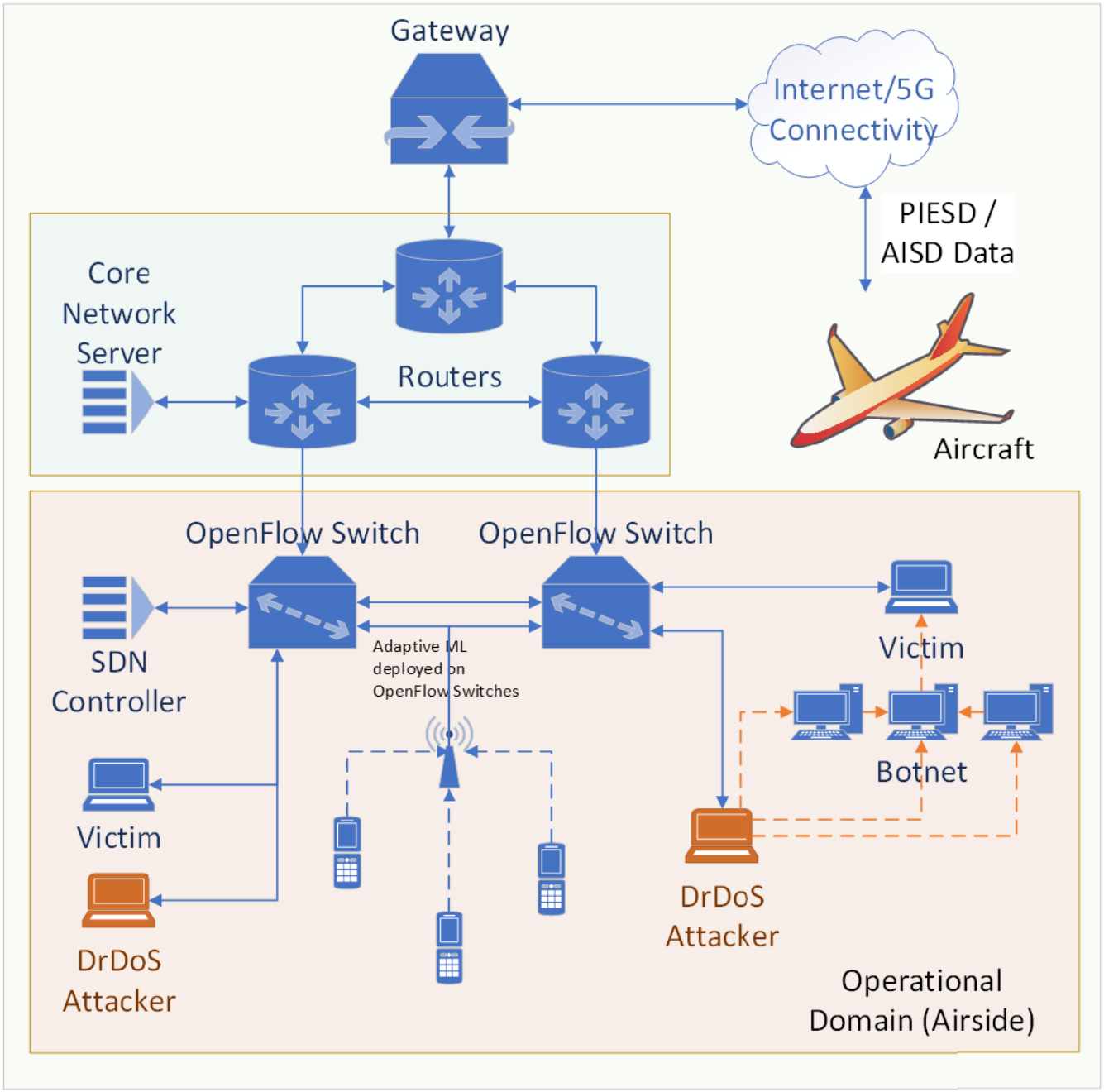


FIGURE 2. Aviation 5G SDN enabling airport environment architecture design.

sequential data and can be used to extract temporal features. This combination of CNN and RNN allows evaluation of spatial and temporal features simultaneously. This is achieved as the GRU is able to maintain temporal features while the CNN extracts the spatial and global components.

- We use Gramian Angular Fields to construct a unique image of a localised frame; preserving both temporal dependency and highlighting temporal correlations.
- We have exceeded the accuracy of both singular and hybrid topology state of the art methods using a dataset that has been reduced by 96.59% when using our optimised feature subset.

The rest of the paper is laid out thus; Section II explores and identifies various security vulnerabilities and cyber threats to 5G driven aviation networks. Section III examines existing literature and techniques for D(D)oS detection, ranging from statistical methods to deep learning. Section IV presents our proposed methodology. Section V comprises

results and discussion. Concluding remarks are given in Section VI.

II. RELATED WORK

Working with SDN-Edge-IoT networks is challenging for multiple reasons including but not limited to large volumes of data combined with heterogeneous sensor inputs and outputs, high dimensionality and multi-modality of data. In this paper, anomaly detection refers to the task of identifying data in which attributes are statistical outliers from the expected. Classical approaches for anomaly and intrusion based detection are based on signature-based detection systems [10]. These systems detect attacks by comparing incoming patterns against databases of known attack patterns and predefined rules. These reactive methods are incapable of detecting zero-day attacks as they rely on a pre-existing set of rules. To create an effective system there are several key network characteristics that must be taken in account prior to designing any Intrusion Detection System:

- Speed
- Adaptability
- Reduced Overhead
- Lightweight
- System/Protocol Agnostic

Any model developed should be able to detect and classify threats within an acceptable time period and be able to detect novel attack patterns and stratagems. While doing so the IDS should be seamless, via techniques such as minimising system resource requirements, in order not to take a negative toll on the front end system. Finally, the diverse IoT environment that is prevalent within aviation requires any IDS to be able to analyse differing architectures linking back to the need for any solution to be protocol agnostic. This section explores and evaluates anomaly based D(D)oS detection methods - evaluating both traditional statistical methods and machine learning applications.

A. STATISTICAL APPROACHES FOR INTRUSION DETECTION

A common approach for network analysis and D(D)oS detection is by measuring the statistical properties of various network traffic variables - evaluating entropy variation for a given network feature [11]. Information Entropy (IE) is a statistical technique used to measure the information uncertainty for a given variable. When applied to network traffic, IE evaluates the change in distribution of traffic. A high entropy score indicates high variation; conversely low entropy values indicate less variation in the traffic packets' origins or behaviour. In theory, volumetric D(D)oS attacks are typically characterised by a significantly larger number of traffic packets compared to standard operational traffic. These attackers send huge quantities of traffic to one or more targets causing a drop in distribution of known traffic attributes. Entropy methods have been used with varying degrees of success.

Literature [12] utilised entropy statistics to detect DDoS attacks by evaluating the rate at which packet drops occur in order to classify the occurrence of DDoS attack in quasi-real time - achieving an accuracy of between 97-100% dependent on the percentage attack rate. Reference [13] implemented a D(D)oS detection method based on Chi-Square analysis of port number and source IP address. Reference [14] proposes an entropy technique using randomness to calculate the number of incoming packets to defined hosts and compares the flow rate against a threshold value. Reference [15] similarly uses time duration to detect DDoS attacks. A flow controller evaluates the accumulation on packets determined 'non valid' over a given time frame to determine if a DDoS attack is occurring. Entropy based detection has been used for lightweight edge network deployment; [16] utilised analysis of flow statistics and entropy calculations deployed on switches to detect anomalies in networks similar to the lightweight solution presented in [14]. Reference [17] proposes a novel Network Intrusion Detection System (NIDS) combining both Genetic Algorithms and Fuzzy Logic with the approach achieving an accuracy of 96.53% on real time network data.

A consistent issue with both statistical and entropy based techniques is the requirement to select a relevant detection threshold. Due to the heterogeneous sensor feeds that are pervasive throughout both the aviation topology and the variation in traffic type and volume. This fluctuation means it is difficult to ascertain an acceptable detection threshold that will minimise false classifications under attack conditions.

B. MACHINE LEARNING FOR INTRUSION DETECTION

Machine learning explores hidden patterns and relationships to give predictions for new data. Supervised machine learning algorithms need labelled data, while unsupervised machine learning algorithms can describe data structure with unlabelled data. Data used as input for machine learning algorithms are considered features, and should be chosen carefully to improve accuracy and reduce computation time. Feature selection is a necessary phase to analyse high dimensional and noisy data. Algorithms in common circulation are Support Vector Machine, K-Nearest Neighbour, Neural Network, Decision Tree, Naive Bayes etc. Within their literature [18] has conducted a comparative study; utilising the J48, Multi-Layer Perception (MLP), Random Forest and Naive Bayes algorithms to classify D(D)oS attacks achieving an accuracy of 98.64%, 98.63%, 98.10% and 96.93% respectively. Within this work we see the benefits of the J48 decision tree as there is no need for prepossessing data. Furthermore the algorithm is able to efficiently Handel co-linearity of data. Interestingly, the J48 decision tree (DT) achieves high scores across all classification metrics despite the DT tendency to lose information when utilised on continuous data. The paper also evaluates the potential of Naive Bayes as a Cyber Attack classifier as it has the ability to handle both discreet and continuous data allowing it to operate over all

aspects of cyber network statistics. This, combined with its ability for real-time classification and insensitivity to irrelevant features promote Naive Bayes as a rapid deployment method for cyber-threat detection. However, the assumption of Conditional Independence between each variable excludes the Naive Bayes model from evaluating possible solutions based on possibility of co-linearity. The final two approaches are Random Forest and a Multi-Layer Perceptron (MLP). As with Naive Bayes the Random Forest approach is able to work well with both categorical and numerical data. Furthermore, they operate a form of feature selection to optimise their methodology. However, a major drawback is the high computational intensity for large datasets, an attribute which is not explored within the paper. Finally the authors propose the use of multi-class classification using a Multi-layer Perceptron model. The core advantage of the MLP is its able to be applied to complex non linear problems. However it has high computational time and the functionality of the model is dependent on the quality of the training. Reference [19] explored the use of stateless features to detect DDoS attacks in IoT network traffic. Varying machine learning method have been used to detect and mitigate cyber-attacks. Reference [20] utilised anomaly-based methods combined with XGBoost and Adaboost on the NSL-KDD dataset achieving 84.2% accuracy. The relatively low accuracy compared to literature can be explained by the dataset description where minority classes in training are seen as majority elements within the testing domain - this discrepancy results in a large number of false positives within the binary classifier. Several ensemble learning methods have been proposed such as [21] and [22]. As would be expected for an ensemble classifier, accuracy exceeds that of a singular network. The authors of [23] have proposed an approach utilising ID3, Random Forest, Naïve Bayes and Logistic Regression; achieving 78%, 65% and 69% on Precision, Recall and F1-score respectively. Reference [24] proposed a near real-time SDN environment utilising the CNN DL and multi-dimensional IP flow analysis accuracy of: 95.4%, Precision - 93.3%, Recall - 95.7% and F-measure - 92.8%. Similarly, [25] presented a methodology based on a Restricted Boltzman Machine (RBM) and Deep Belief Network (DBN). The method achieved a detection rate of 97.90% on the NSL-KDD Cup'99 dataset with a false negative rate of 2.47%. Reference [26] propose a deep learning structure trained on the NSL-KDD'99 dataset attaining a 99% accuracy. The authors of [27] propose the use of a Self Organising Map (SOM) to be deployed within an openflow environment. The lightweight DDoS attack detection operates with a low computational overhead. While obtaining a relative number of false positives the detection rate is on par with other ML approaches.

C. DEEP LEARNING FOR INTRUSION DETECTION

Deep Learning is a subset of machine learning; utilising multiple layers of neural network structures to extract, refine and classify input vectors. The authors of [28] propose a Deep Learning algorithm which utilises a recurrent Neural Network to extract learnt patterns from network traffic sequences and evaluate network attack activities. In this model LSTM-based approach attains the highest accuracy of 97.96%, while the combination of CNN and LSTM achieves an accuracy of 95.90%. Reference [29] combines statistical approaches with deep learning; combining entropy features with DL-based classifiers. The evaluation demonstrates improved performance over the threshold-based approach with higher precision and recall; furthermore, this approach addresses the problem of threshold setting in entropy-based techniques mentioned previously. Reference [30] have attempted to generate a holistic solution by integrating deep convolutional layers with advanced probabilistic layers focusing on the minimisation of false positives and false negatives to enhance and improve detection accuracy. Reference [31] use a regularised CNN combined with L1 and L2 in order to reduce over-fitting by the Convolutional architectures. The work indicates that the L1 and L2 regularisation helps to address performance short comings on unseen data by assigning penalty term to the loss function. Reference [32] utilize a novel Transformer based network intrusion detection system. The benefits of which are that transformers will efficiently extract high dimensional data in to its low dimensional representation; furthermore the method employs a self attention mechanism to capture contextual information between network traffic for detection.

D. TIME SERIES IMAGES

CNNs have achieved a great success in image recognition due to their inherent ability to learn hierarchical feature representation from raw data. A time series sequence is one which as natural temporal ordering. Existing Time series classification (TSC) are usually based on varying perspectives. Frequency domain methods such as spectral analysis [33] and wavelet analysis [34] are commonplace as are time domain approaches such as auto-correlation and regression [35]. Reference [9] utilised Time Series Images (TSI) to detect False Data Injection Attacks (FDIA) within power networks. The results and analysis shows that TSI is able reliably detect and localise most of the FDIA over the networks. Furthermore, comparative analysis shows that this approach is superior to standard ML approaches such as Support Vector Machines (SVM).

In this work we have chosen to use a 2-Dimensional (TSI) representation of our data rather than the traditional 1-Dimensional representation. Image representation of time-series generates varying feature types that are not available for 1D signals; through this we are able to migrate the problem into the realm of convolutional network texture analysis. Furthermore, the combination fusion of the CNN and GRU methodologies promote several advantages over existing techniques discussed. Compared to traditional machine learning methods such as the MLP image analysis via CNN experiences better data fitting and generalised

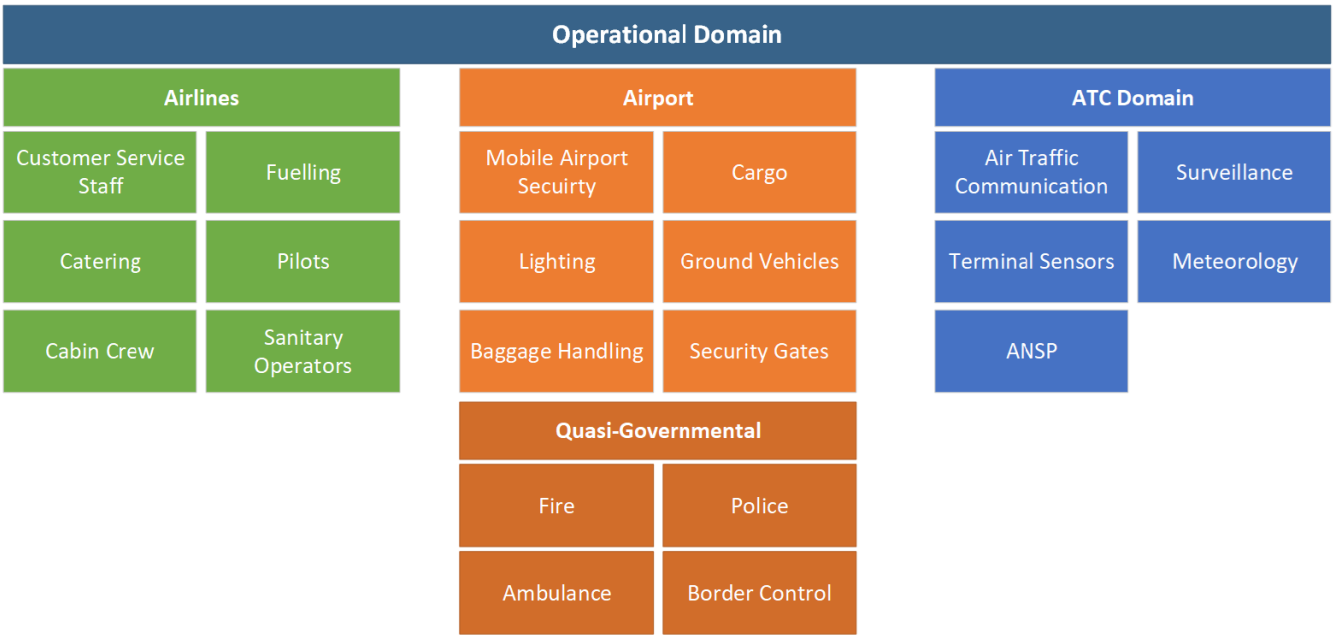


FIGURE 3. Aviation operational domain systems and sub-systems.

performance [36], [37], [38]. Additionally, CNNs are more location invariant, utilising only a small subset of the image at any one time. Furthermore, the automatic feature analysis and selection makes it an obvious choice. In tandem, the Recurrent Neural Network (RNN) is unique in its ability to correlate contextual information effectively and is suitable for modelling sequence data. The hybrid CNN-GRU is adapted to making use of the multi-scale spatiotemporal characteristics to classify network operation to a higher accuracy and a lower false positive rate than the current state of the art.

III. AVIATION ECOSYSTEM AND CYBER VULNERABILITIES

Figures 3 and 4 show the aviation ecosystem as a fusion of multiple silo-ed sub-networks, made up from heterogeneous devices and connectivity capabilities communicating to provide seamless operation within the air side domain.

The co-existence of different generations of network technologies is due to legacy motivations and differing system requirements and specifications across network sub-domains.

A. NETWORK ARCHITECTURE

The aviation safety and operational ecosystem is still evolving as the smart airport concept continues to develop. Recent regulatory definitions are given in ARINC 858 [39]. High rates of development have occurred in the domains of Airline Operation Control (AOC) and Air Traffic Services (ATC) related to integration within the Software Defined Network (SDN) infrastructure. The core architecture comprises a series of aircraft (mobile nodes) geographically distributed over the airport where messages are exchanged between the Aircraft, Airport Operation ControlCentre(AOCC) and Air

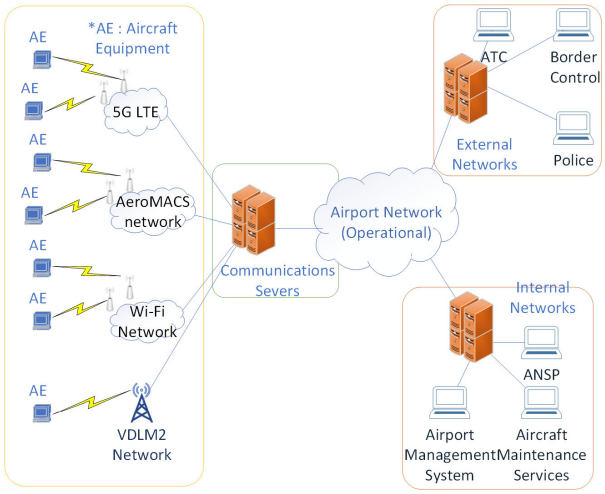


FIGURE 4. Aviation domain presented as a global system of systems.

Navigation Service Provider (ANSP). Any aircraft is capable of either generating or receiving data to/from the varying ANSPs or ground actors. Incorporating an SDN architecture promises to significantly simplify and reduce network management and thereby enable evolution and development within cyber operations due to the logically centralised network intelligence based in the control plane. In this scenario network devices and nodes operate solely as packet forwarding devices. However, the segregation of the control plane and data plane inadvertently facilitates the option of availability driven cyber attacks. D(D)oS style attacks are able to flood the control plane, the data plane, or the communication channel. A successful attack against the control plane is highly likely to cause complete network failure. Similarly, an attack

perpetrated against the data plane or the communication link would most likely entail a combination of packet drop and general network inaccessibility. In order to mitigate these scenarios there is a need for a solution that is able to ensure availability and robustness of the communication channel between network switches and the SDN controller, as shown in Figure 2. It is of critical importance that any deployed solution maintains the functionality of forwarding legitimate traffic while effectively and efficiently being able to discern between malicious and benign traffic all while maintaining an overall acceptable system operational performance.

1) SOFTWARE DEFINED NETWORKING

The increased deployment of software using Software-Defined Networking (SDN) and Network Function Virtualisation (NFV) in 5G networks are expected to facilitate increased coordination and optimisation of heterogeneous resources [2] to enable resource management within the 5G IoT environment. The core aspect of the SDN environment [41] is the decoupling of the control and data planes thereby migrating all network and control intelligence to the centralised logic network controller. Within this architecture all forwarding devices become packet forwarding elements. For south bound interfaces it is assumed OpenFlow is used. As with standard IP topologies every protocol, device or layer participating in a SDN can be utilised maliciously. In order to mitigate attacks and defend systems Intrusion Detection Systems need to be put in place. Figure 2 shows the proposed location for system implementation within the SDN aviation environment. SDN comprises two main segments: Control Plane and Data Plane.

2) CONTROL PLANE

The control plane collects and maintains the data corresponding to all the connected aircraft and ground nodes. It is used for forwarding and routing decisions dependant on aircraft status. Implementation of SDN requires control of the network to be transferred from an individual access network to the core network. This plane also maintains information pertaining to the current state of the network topology, node and aircraft location, network connectivity and Quality of Service (QoS) preferences.

3) DATA PLANE

The Data plane comprises all data transmitting network devices for the various end user domains as shown in Figure 3. The lack of a uniform connectivity infrastructure further divides the data domain into the IP Application Data Domain and the Legacy Application Data Plane. The interoperability required by the data plane to manage the IP and legacy technology introduces several challenges into the system.

B. CYBER SECURITY WITHIN AVIATION

The increased economic, social and environmental factors that come with smart airport concepts leads to increased system vulnerability due to the exponential increase in potentially unsecured connected devices [42], [43], and [44]. In addition, the deployment of IoT-enabled technologies such as EFBs and field loadable data has generated a highly integrated framework and environment of information and communication systems. The combination of multiple systems and architectures allows information to be shared quickly and dynamically, agnostic of system demand. However, the introduction of this combined infrastructures on top of an already diverse architecture increases susceptibility to cyber-attacks. Increased data migration, processing and links between devices and systems also bring susceptibility to the airport operators, policy makers, vendors, airlines and contracted entities providing airport services. A breakdown of common cyber attacks against network infrastructure is given in Table 1.

TABLE 1. Prevalent threats to future aviation connectivity [40].

T. DENIAL	System resources may become exhausted due to system error or denial-of-service (DoS) attack.
T. DENIAL.INJECT	An attacker injects malformed messages into a communications segment of the system in order to reduce the availability of the system.
T. ENTRY	An individual other than an authorized user may gain access via technical or non-technical attack for malicious purposes.
T. ENTRY. ALTER	An attacker delays/ deletes/ injects/ modifies/ re-directs/ re-orders /replays or otherwise alters messages on a communications segment of the system to attack integrity
T. ENTRY. EAVESDROP	An attacker eavesdrops on messages on a communications segment of the network in order to reduce confidentiality.
T. ENTRY. IMPERSONATE	An attacker impersonates a user of services to reduce the confidentiality or integrity of the network, or simply to gain free use of the system.

The deployment of 5G systems within the aviation ecosystem, coupled with the development of the connected aircraft and digital cockpit has expanded the threat landscape beyond these traditional attack vectors.

Figure 5 shows the burgeoning threat taxonomy for smart airports, including human error, system failures and malicious actions. Despite the awareness of the increasing number of cyber threats against it, both literature and events show that cyber security within aviation has not yet reached maturity:



FIGURE 5. Threat taxonomy for smart airports.

- 2019: The US Department of Homeland Security (DHS) successfully managed to hack a parked Boeing 757 without physical access to the network or having placed a saboteur on the aircraft [45].
- 2018: Malicious code was uploaded to British Airways in order to steal personal data relating to 429,612 customers and members of staff from its servers.
- 2015: Polish airline providers at Warsaw Chopin airport were hit with a DoS attack on a critical network resulting in 22 flights being cancelled or delayed.
- 2015: Elements of Sweden's ATC operational capacity were blocked for up-to five days following a successful attack by the cyber espionage group ''Fancy Bear''.

The most commonly occurring cyber attack nowadays is the Distributed Denial of Service(DDoS). A DDoS attack is a distributed yet coordinated attack on service availability predominantly deployed against host servers (application, storage, database or Domain Name Servers (DNS)) or network resources. To ensure anonymity of the actor they are mostly deployed using compromised 3rd party systems (botnets) [46], [47], and [48]. The system of systems topology favoured by aviation introduces a host of new vulnerabilities in to the system, these vulnerabilities are further exacerbated by the proposed implementation of 5G technology.

C. SECURITY ISSUES IN 5G NETWORKS

Due to the dynamic nature of 5G wireless networks, communication is susceptible to a variety of attacks with targets ranging from data privacy to network integrity. Finding an widely acceptable security solution to protect 5G networks is particularly difficult due to the aviation requirement for scalable networks; derived from instant arrival or departure of users from the Area Of Operation (AOO). Unlike traditional wired network topologies that operate dedicated routers and switches, 5G increased service coverage derives from massive IoT and Peer-to-Peer side linking. These techniques, coupled with the requirement for dynamic network adjustment open the wireless channel to both legitimate network users and malicious actors. Furthermore, the dynamic and distributed topology of SDN-Edge-IoT Ecosystem Architecture results in a reduced centralised authority for cyber security analysis and decision making. Network nodes are able to access or leave the network as required. The roaming nature of these nodes makes them vulnerable to network capture. This is particularly prevalent in Common-Off-The-Shelf (COTS) devices that lack dedicated inbuilt detection and mitigation protocol thereby posing the weakest link and focal point for a cascading cyber attack through the network. Derived from literature evaluation, Figure 6 shows the primary attack vectors deployed against IoT and cyber physical systems to block, steal, manipulate or delete data.

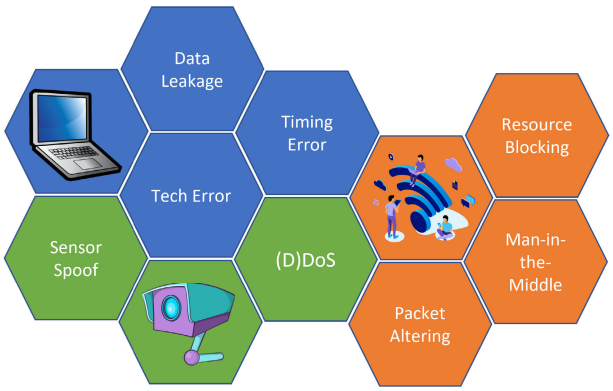


FIGURE 6. Potential IoT cyber physical system attack vectors.

The reliance on distributed mobile nodes to form the core network infrastructure exposes IoT communications topologies to a variety of attacks - specifically regarding network availability. Attacks against system availability primarily consist of Denial of Service (DoS) attacks. A DoS Attack generates a network state wherein it cannot accomplish its expected functions due to disrupted network services such as routing, for its authentic users.

D(D)oS attacks primarily occur at the Transport Layer of the TCP/IP Stack [49]. The transport layer is responsible for controlling the flow of data within the communication stack [50]. The main vulnerabilities found within the transport layer are related to intentional corruption or degradation of traffic packets; or exploiting protocol flaw to generate D(D)oS attacks against the network.

There are three commonly occurring protocol driven attack vectors used against the transport layer [51] and [52]:

- **Transmission Control Protocol Synchronisation (TCP SYN) Flood Attacks:** A SYN attack occurs when an attacker - operating through a spoofed IP address - transmits multiples of Synchronisation (SYN) packets to a server. The SYN and ACK from the server are sent to the fake IP address and the link remains in a semi open state until ACK packets are received from the target IP address. The target device, is unable respond

as its address has been hijacked by the malicious actors. This process enables malicious parties to bombard the server with a constant stream of SYN packets resulting the system backlog queue containing the one way open connection entries to exceed its finite size - dropping new connections.

- **User Datagram Protocol (UDP) Flood Attacks:** In this instance the attacker overwhelms random ports on the targeted host with IP packets containing UDP datagrams. Utilising UDP characteristics such as the lack of a three-way handshake structure, as with TCP, a high volume of ''best effort'' traffic can be sent over the network. This coupled with the lack of built-in data surge protection makes UDP attacks both highly effective and able to be enacted with limited resources.
- **ICMP Flood Attack:** This attack type occurs when an attacker attempts to overwhelm a targeted device with ICMP echo-request packets. The high rate of traffic results in a block causing the target IP to become inaccessible to normal traffic.

It is common for a DrDoS attack to be used as part of a wider stratagem. In addition to attacking system availability these methods can be used to subvert systems and deploy malware to generate a botnet. In turn these botnets can be used to launch DDoS attacks of a much higher magnitude, coalescing vast reserves of distributed compute power to be deployed as required- as in the case of the storm worm botnet [53]. The placement of the Intrusion Detection system is an important consideration. In most instances they are deployed behind the firewall at the edge network to facilitate high levels of visibility. However, this heightened awareness comes at the expense of host – to – host traffic analysis. Reference [54] highlights the four main deployment options for DrDoS detection systems are given in Figure 7. However, D(D)oS attacks have become more difficult to detect due to the fusion of multiple attack vectors. The utilisation of multiple protocols to ensure attack success is now commonplace. In order to combat this diverse attack methodology, more robust, wide-net defence techniques are required. Traditional signature driven Intrusion Detection Systems (IDS) are not able to detect the novel zero-day nature of modern attack strategies while existing statistically driven systems are limited by the requirement to define operational limits. Lately, Machine Learning structures are being explored in order to compensate for limitations of existing solutions in order to ensure both, the integrity of services rendered by the airport and the safety of personnel within the aviation environment.

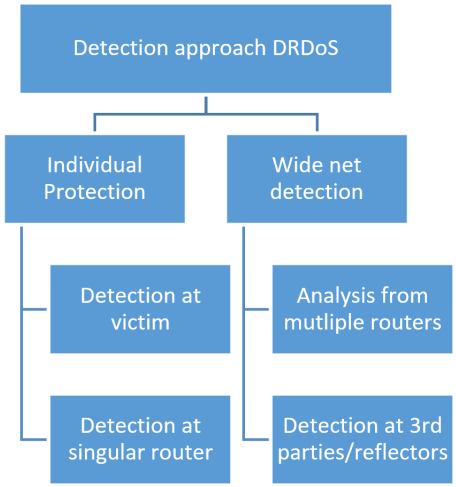


FIGURE 7. DrDoS detection techniques based on deployment area.

IV. PROPOSED METHOD

In this paper we propose a novel lightweight Multi-Channel CNN-GRU approach to DrDoS detection by evaluating the spacio-temporal domains. An initial parallel architecture has been deployed to enable the analysis of N time series image features in tandem. As prior work has focused on either purely in the spatial or temporal domains to the best of our knowledge no previous work has been done wherein the detection method operates within the combined domain using time series imaging. The proposed method for lightweight detection and classification of D(D)oS events within 5G heterogeneous networks comprises a four stage process: Data Collection, Feature Extraction, Gramian Angular Field (GAF) Conversion and CNN Analysis. Utilising GAFs provides a method to preserve temporal dependency within the model. As time increases the position moves from top-left to bottom-right. The GAFs comprise temporal correlations generated by representing the relative correlation by difference of directions with respect a given time interval. Convolutional Neural Networks are then used to extract and analyse spatial features and the pooling layers are used for dimensionality reduction. Finally a Gated Recurrent Unit (GRU) is used to classify the output feature vector which is then evaluated using a ensemble based late fusion method to determine the final output.

A. EXPERIMENTAL ENVIRONMENT

A deployed 5G IoT based system within the aviation domain will comprise multiple key technologies and components to interface together as to enable connectivity and data exchanges. The aviation environment operates as a heterogeneous ecosystem and as such, a multitude of applications can be migrated over from legacy systems to an homogenous 5G architecture; including but not limited to: Asset Tracking, Energy management, Passenger Services and Maintenance. Our simulation is designed to evaluate and test a novel cyber security method using GAF-CNN-GRU methods for intruder detection. There are multiple potential deployment scenarios for such a system as:

- The IoT Device Layer: Here the IDS method is deployed within the IoT devices themselves. This level of granularity allows for the detection of anomalous behaviour

at the device level in real time. However, the detriment of this deployment structure is it results in a limited visibility of the wider network and as such lacks system context. Furthermore, resource limitations of many IoT style devices results in a limited deployment pool.

- The IoT Gateway Layer: This would allow a more centralised monitoring structure based on the aggregated data from multiple IoT devices with minimal latency and bandwidth constraints based on local data processing. Despite these benefits however the processing and memory capacity of gateways may become a limiting factor combined with the generation of a single point of failure as a gateway malfunction may result in compromising the entire IDS structure.
- The Edge Layer: This method provides low latency as with the IoT device layer allowing processing of data closer to the source, thereby enabling real time analysis and response. Furthermore, operation at the edge layer allows a greater degree of discrimination on traffic forwarding as only relevant information will be transmitted to the core network reducing the overall system bandwidth requirement. However, as with the IoT device layer, the edge layer boasts limited resources and a narrow view of the broader network.
- Core Network Layer: Deployment of IDS inside the core network would facilitate network wide network wide visibility allowing analysis of devices, gateways and network functions all combined within an integrated security infrastructure; however, this is done at the cost of increased latency reducing the effectiveness of real time analytics.

Our method is based on the Edge Computing Layer of the 5G architecture as we believe it will interface best with a Moving Target Defence (MTD) proactive security mechanism that we shall explore in a future paper. The Edge Computing Layer is beneficial due to the proximity to data sources and the real-time response rate. To avoid the issues of resource constriction to methods have been applied; Lightweight Anomaly Detection Algorithm, based on the MobileNet architecture and a GRU designed for lightweight application combined with a extensive pre-processing and feature analysis which has resulted in a reduced computational load whilst not effecting detection accuracy. The simulation has been developed using MATLAB combined with the Canadian Institute for Cyber Security 2019 DDoS dataset [23]. Figure 8 shows attacks contained within the dataset demonstrates a range of protocols used and subsequent attack vectors. Attacks based off TCP protocols include MSSQL, SSDP. Whereas UDP attack vectors include CharGen, NTP and TFTP. In addition, there are certain attacks that can be carried out using either TCP or UDP like DNS, LDAP, NETBIOS and SNMP as would be expected within a heterogeneous aviation environment. Subsequent subsections this paper explores the feature selection and elimination process. Retained features are converted in to Gramian Angular Field Representations and stored in a MATLAB image data-store as this

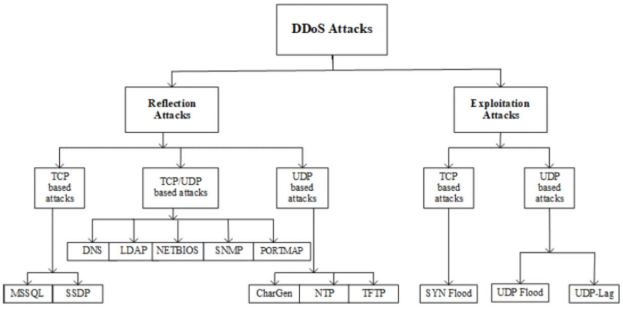


FIGURE 8. CIC 2019 Dataset Taxonomy [23].

allows for ease of integration with machine learning workflows in MATLAB. The Gramian fields contained within the data-store were then split into train, test, validate sets with a ratio of 0.7:0.2:0.1 respectively. The Machine learning model was the generated using the machine learning toolbox in MATLAB where the data-store inputs were then used as inputs into the parallel CNN-GRU architecture, looking at edge deployment structures allows us to circumvent the additional data aggregation steps that would be needed for gateway deployment.

B. DATASETS

There are several established datasets that specialize in D(D)oS attacks such as 'DDoS Attack 2007', 'Anonymized Internet Traces' produced by CAIDA, 'Smart-Defender' from CCA and CIC-DDoS2009 from Canadian Institute for Cyber Security (CIC). For this we have both the data-set developed by [55] and the CIC 2019 D(D)oS dataset.

The dataset generated in [55] is a combination of both hardware and software elements representing the performance of a real cyber physical system rather than simply evaluating the virtual components. Features collected in the dataset encompass the full CPS domain evaluating the central processing unit (CPU), volatile memory (RAM), non-volatile memory (ROM), as well as the system bus, communication subsystems, battery utilisation, and input/output units - specific descriptions have been taken from [55] and presented below:

- CPU utilisation: The CPU utilisation percentage parameter represents the percentage of the total available CPU computing power available at a given instance.
- Memory load: Usage percentage parameter indicates the amount of active system virtual memory used.
- Task Count: The total number of current CPU software processes.
- Thread count: Records all active threads at a given time instance.
- CPU temperature
- Power consumption
- Received (RX) and Transmitted (TX)

The unique quality of this dataset is that the parameters comprise both hardware and software elements of the Cyber Physical System (CPS) which adjust instantly with variable

operational circumstances; resulting in a dynamic visualisation of the system's health which can be analysed via analysis of these parametric changes. In addition to this, in order to provide an accurate and reliable comparison to current state of the art literature this method has also been evaluated using the Canadian Institute for Cyber Security (CIC) 2019 D(D)oS dataset which utilises network flow statistics primarily from the transport and application layers. The dataset generated in [55] has 8 constituent features, all of which have been used as inputs for the GAF-mfCNN architecture. Compared to this the CIC dataset comprises 79 usable features. In order to reduce this number and thereby the computational load; the CIC dataset features have been ranked and evaluated using the principles of Information Entropy with three middle ranking features being selected as the input feature vectors.

C. FEATURE SELECTION

At the highest level of abstraction a machine learning classifier maps a series of input data points - features - against a target variable. This process is used so that the model learns a mapping between the input and target variables to facilitate the accurate prediction of the target variable. The goals of feature refinement are:

- Improve models predictive accuracy
- Reduce the computational requirements of prediction
- Increase the interpretability of our model

In many instances the raw data may not provide optimal information to train an ideal model, therefore it may be necessary to remove features that:

- Are highly correlated with extant features within the dataset thereby providing the same information to the model.
- Highly uncorrelated with the output such that they provide little or no information regarding predictive output.
- Provide no variable information into the predictive model IE. sequence that comprises fully the same value.

Before we evaluated our model on the CIC 2019 dataset, we had to determine which features to use as inputs for the multi-channel CNN. When dealing with anomaly detection and classification, information entropy is a metric we use for determining high value input features. For a given feature, X, that can exist in M discrete states information entropy is given in Equation 1:

$$H(X) = -\sum_{i=1}^{M} p_i \log_2 \frac{1}{p(i)} \tag{1}$$

The 78 features of the CIC 2019 dataset were evaluated and their information entropy scores calculated and ranked in ascending order. A random variable with high entropy is assumed to be a uniform random variable across the classes. Contrary to this, a variable with low entropy is considered to be less uniform implying it is associated with only a reduced set of possible outcomes. For evaluating the CIC dataset three medium entropy variables have been selected as inputs to the classification structure: *'Idle Min'*, *'Active Mean'* and *Packet Length Std*. The outputs for this method of feature selection are given in Figures 29 and 30. These initial results have been developed using a random subset of features based off the Information Entropy scores. However, in order to refine our model we shall evaluate the CIC dataset features to determine which contribute most to the predictive model.

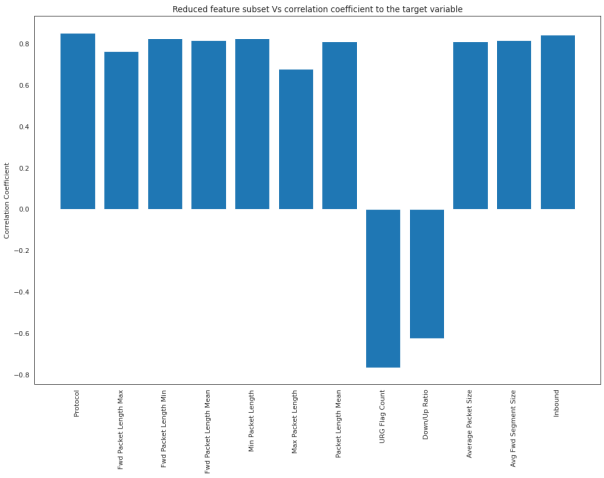


FIGURE 9. CIC 2019 reduced feature subset selected by evaluating correlation to the target variable.

Following this we refine our feature selection using various feature selection mechanisms. Figures 15 and 16 are representations of the correlation matrix between dataset variables indicating the depth of association. The value of the correlation coefficient varies between $+1$ and -1. A value of $\pm$ 1 indicates a perfect positive/negative association between variables. However as the correlation coefficient tends towards 0, the relationship between the two variables is weaker. Figure 15 shows the averaged correlation coefficients derived from Figure 16. To reduce the pool of potential features we remove any feature with a correlation coefficient in the range of $\pm$ 0.5. Figure 9 shows the reduced feature subset.

Figure 10 shows the intra-feature correlations of the reduced feature subset.

It is desirable to maximise the information being input into the classifier, as such it is important to select features which maximises the correlation to the output variable as shown in Figure 9 whist also minimising the intra-feature correlation.

Figures 11 and 12 show the depth of correlation between features for positive and negative correlations respectively. Features that are linked by vectors with a high intensity of colour correspond to a high correlation, conversely loosely correlated features are shown by a low colour intensity. In order to maximise information input we remove features that have a correlation outside the range of $\pm$0.5.

Evaluating Figures 13 and 14 reduces our final input features by 50% to:

- Max Packet Length
- Protocol
- Inbound
- URG Flag Count

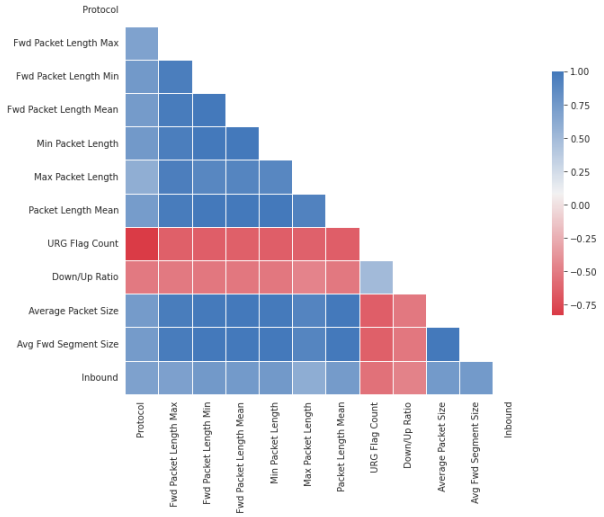


FIGURE 10. Intra-dataset correlation of the features held in the subset.

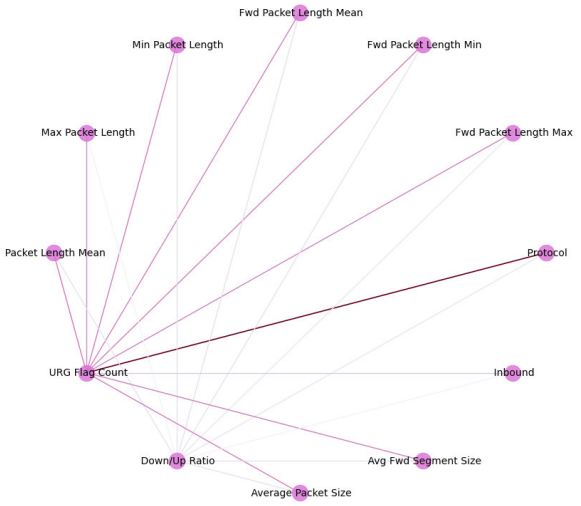


FIGURE 12. Graphical representation of weighted negative feature correlations.

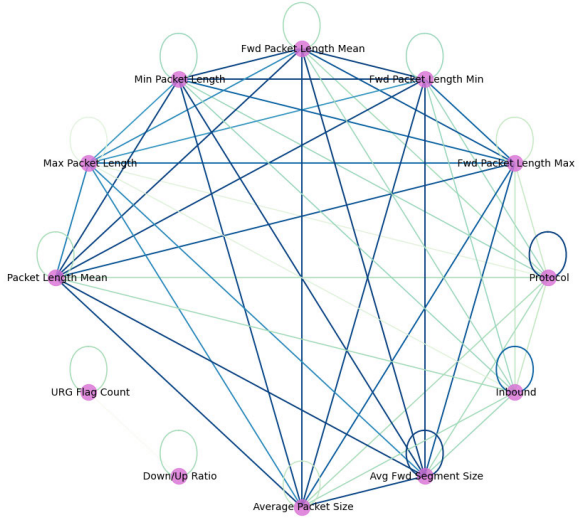


FIGURE 11. Graphical representation of weighted positive feature correlations.

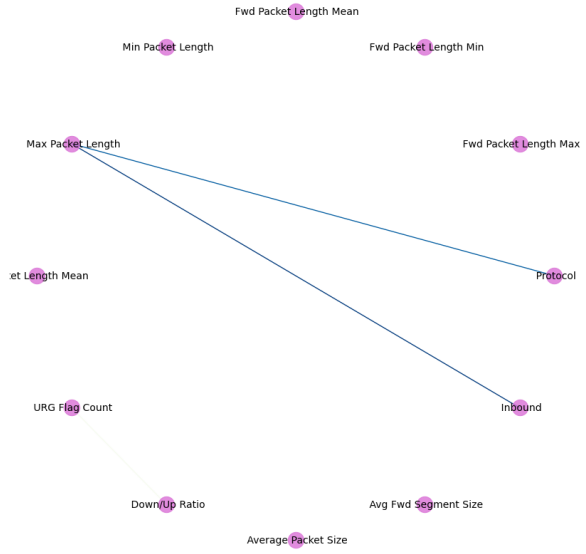


FIGURE 13. Positive intra-feature correlation set with 0.5 cut off.

- Down/Up Ratio
- Fwd Packet Length Max

However, Figures 13 and 14 indicate a relatively high intra-feature correlation between several remaining attributes. Recursive Feature Elimination (RFE) is used to reduce our subset to the final three features for network input. RFE involves an iterative procedure where the goal is to identify the most relevant features. In this particular case, it was decided to retain only three features. By employing Cross Validation with RFE, various combinations of features were assessed, ultimately determining the ideal set of three features for input into the classifier [56], [57], [58].

D. FEATURE REPRESENTATION

In this work we are not only interested in determining when an attack is currently in progress but also identifying the trigger point of the attack, where the network state transitions from benign to the attack class. Figure 17 is a graphical representation of the binary state change over time as our network moves from benign status to attack classification.

This has been achieved by splicing together benign traffic packets and Attack traffic patterns at random intervals. Figure 18 provides a scaled down representation of the LDAP class pre-spliced GAF input sequence for a given variable.

For each input sequence a random number between 0 - $\frac{SequenceLength}{2}$ is selected. The randomly selected number of STI is then cut out and benign network traffic spliced in. A high level overview of the process is given in Figure 19

The objective of this is to simulate and thereby train the model to identify the network state change from benign to attack.

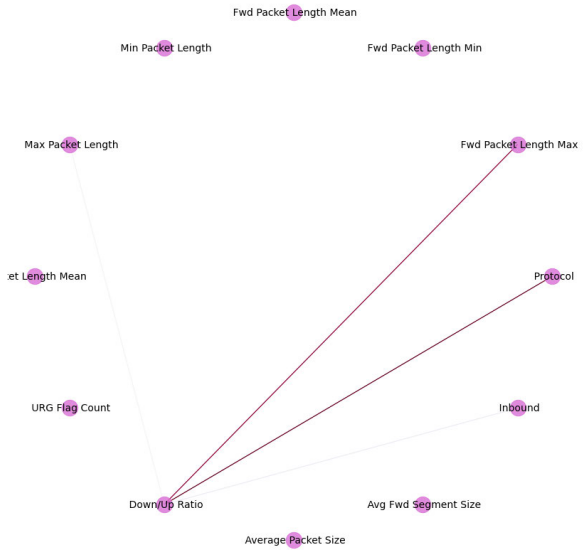


FIGURE 14. Negative intra-feature correlation set with 0.5 cut off.

The data collected is a continuous time series and as such has been segmented by a sliding window representing the Area of Interest (AOI) at a given instant in time. Visual representations of the time series data are given in Figures 20 and 22; for both figures the X-axis is the sequence index ranging from 1 - 30, and the Y-axis is the normalised feature value.

Figures 20 and 22 show the original data obtained by the time window is collected as a series of unique uni-variate sequences over time. As such it must be converted to a format equivalent to a two-dimensional image for CNN evaluation.

To accomplish this a Gramian Angular Field for the time series has been generated.

1) GRAMIAN ANGULAR FIELD

A Gramian angular field is an image representation of a time series, derived from the temporal correlation between each pair of values that comprised an arbitrary time sequence 'X' of length N. The first step in the process is to normalise the data to the range of $[-1, 1]$ as given in Equations 2 and 3.

$$\tilde{x}^i_{-1} = \frac{(x_i - \max(X)) + (x_i - \min(X))}{\max(X) - \min(X)} \tag{2}$$

$$\tilde{x}^i_0 = \frac{x_i - \min(X)}{\max(X) - \min(X)} \tag{3}$$

Following data normalisation each of the uni-variate time sequences are transformed from Cartesian coordinates to Polar coordinates by the process shown in Equation 4

$$\begin{cases} \phi_i = \arccos(\tilde{x}_i), & -1 \le \tilde{x}_i \le 1, \tilde{x}_i \in \tilde{X} \\ r_i = \dfrac{i}{N}, & i \in N \end{cases} \tag{4}$$

Equation 4 introduces the re-scaled time series, achieved by taking the inverse cosine of the normalised observation $\tilde{x}$ and assigns it as the Polar coordinate angle ϕ_i; time instance $\frac{i}{N}$ is assigned as the radius. The conversion from Cartesian to polar coordinates is used as unlike Cartesian coordinates, Polar coordinates preserve temporal relations. The angular variation of the cosine function corresponding to the normalised data greater than zero is assigned a value in the range of $[0,\pi/2]$, whereas the angle corresponding to normalised values greater than -1 is assigned the range of $[0,\pi]$. A full description of the GADF conversion can be found in [59] with the key elements described below.

$$GADF = \cos(\phi_i - \phi_j) \tag{5}$$

$$GADF = \sqrt{I - \tilde{X}^2}' \cdot \tilde{X} - \tilde{X}' \cdot \sqrt{I - \tilde{X}^2} \tag{6}$$

In Equation 6 'I' corresponds to a unit row vector. After the polar transformation given in Equation 4 by calculating the difference between sampling points as the sequence progresses as a function of sine, the time correlation and dependencies between indices are identified as a function of angular change [60]. Gramian Angular Difference Fields (GADF) matrices are then defined in Equation 7:

$$\mathbf{GADF} = \begin{bmatrix} \sin(\phi_1 - \phi_1) \cdots \sin(\phi_1 - \phi_n) \\ \sin(\phi_2 - \phi_1) \cdots \sin(\phi_2 - \phi_n) \\ \cdots \ddots \cdots \\ \sin(\phi_n - \phi_1) \cdots \sin(\phi_n - \phi_n) \end{bmatrix} \tag{7}$$

The application of Gramian Angular Fields (GAF) Converts uni-variate time series into a two-dimensional image. The Mapping form 1-D to 2-D is in Figure 21. Figure 23 shows the output of GAF being applied to the uni-variate time series given in Figure 22. The success of Deep Neural Networks (DNNs) such as CNNs is largely attributed to classification and data generation on homogeneous data such as image, audio, and text. However it still struggles on tabular data [61]. This work proposes to utilise the GAF implementation algorithm [62] to transform the network packet data into images by assigning the angular difference in the time series to a given pixel position. The core advantages of the GAF methodology are:

- Gramian Fields are a technique to maintain temporal dependency, as while time increments over the sequence the position within the Gramian Matrix moves from top-left to bottom-right.
- GAFs contain frame localised temporal correlations as the matrices represent the relative correction by difference of angular direction over a given time interval.
- No prior knowledge is required about the features
- Each pixel represents a unique feature requiring less memory and results in reduced training time.
- Constant neighbourhood structure.
- Thee original time series is reconstructable from the central diagonal that contains the original angular data.

The output of the GAF generation is an N channel image where N is the number of distinct time series. A representation of the GAF output structure is shown in Figure 24 Due to the varying statistical properties of the input time series multi-channel feature extraction is required to achieve useful and reliable feature extraction.

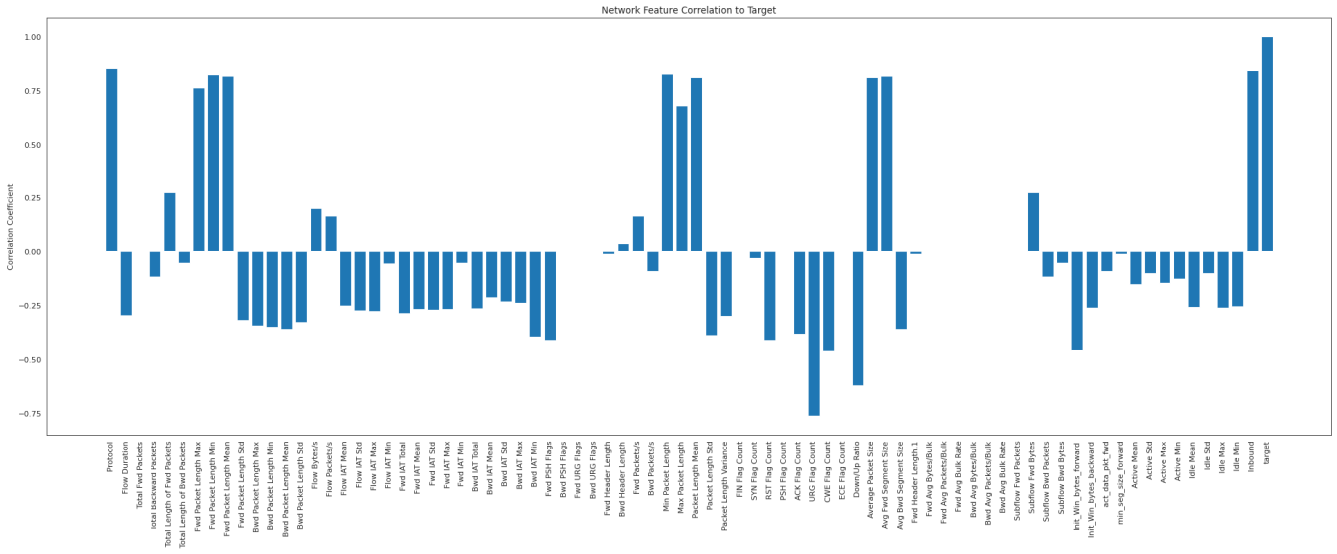


FIGURE 15. Network feature correlation with target variable.

E. MULTI-CHANNEL FEATURE EXTRACTION

In the previous section it is described how we generate time series mappings for each input sequence. Each of these maps corresponds to a respective input channel in order to learn the high level visual features that correlate to temporal dependencies. Due to the different statistical properties of the various feature input vectors it is difficult for a 1-channel model to directly encode the multi-channel features via simple late fusion based on the modal class. As such we propose a fusion based multi-channel convolutional neural network (mfCNN) as shown in Figure 25. An ensemble late fusion method has been adopted to combine the output feature maps from all CNNs.

F. CNN-GRU HYBRID MODEL

Deep Neural Networks are capable of extracting features automatically. utilising this feature extractor methodology is critical in building an end-to-end model. The following section explores the integration of the GRU and MobileNet architectures. MobileNet is used in extraction and classification network features. GRU is used to enhance the performance of the model by maintaining the state information of the features that it comes across in the previous generation of the image classification. The full classifier architecture is given in Figure 25.

1) CONVOLUTIONAL NEURAL NETWORK MODEL

The Convolutional Neural Network (CNN) is now commonplace, having become an efficient and effective method for pattern recognition and image analysis [63]. The generic CNN architecture comprises a convolutional layer and pooling layer for feature extraction a fully connected layer and a softmax activation function. The convolution process that enables feature extraction is characterised by sparse interaction and parameter sharing. Sparse interactions reduce the size of the convolution kernel compared to the initial input size. Furthermore, sharing of parameters makes sure that only one parameter set needs to be learned, thereby reducing the storage requirements of the model significantly and generates a translational equivalent feature [64]. Similarly, Pooling is used to ensure that when translation varies due to changing input, the overall input representation remains predominantly unchanged. The deep convolutional neural network (DCNN) model is primarily used as a pattern classifier, which at the user level avoids the need for both artificial feature engineering and the non-optimal utilisation of features. Optimal feature selection results in improvements across both accuracy and generality of a classifier.

A key layer to ensuring a successful classification is the feature extraction functions which is found within the convolutional layer. The process performs the convolution operation on the current set of data via multiple convolutional kernels. The outputs of this are then passed to the next layer via the bias calculation, activation function and finally pooling operations. The whole process is condensed in to in Equation 8.

$$x_j^l = f(\Sigma_{i \in M_j} x_i^{l-1} \times k_{ij}^l + b_j^l) \tag{8}$$

In Equation 8 '$\times$' is the symbol representation of the convolutional operation. x_i^{l-1} is the input to the current layer and x_j^l the output for the current l-th layer. The other parameters in the function are f,M_j, k_{ij}^l and b_j^l which correspond to the kernel element, current feature map element, weight value and bias accordingly.

2) LIGHT-WEIGHT CONVOLUTIONAL MODEL

For this we have used a modified structure based on the MobileNet [65] architecture. MobileNet utilises the

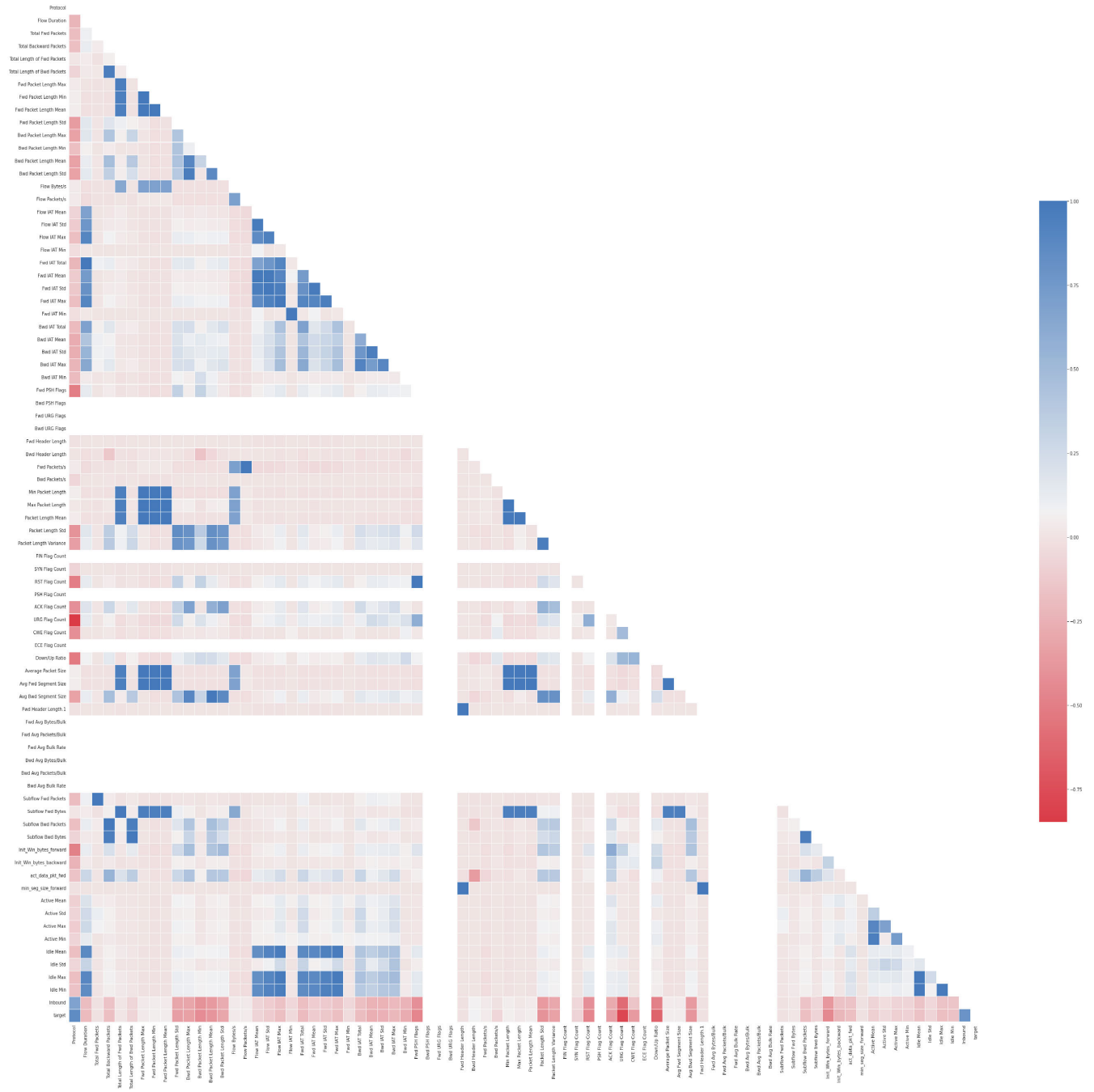


FIGURE 16. Correlation plot between features and target variable for '*Benign*' and *MSSQL* attack classes in the CIC 2019 DDoS dataset.

principles of Depthwise Separable Convolutions, Batch Normalization (BN) and Rectified Linear Unit (ReLU) thereby significantly reducing the number of parameters when compared to other commonplace CNN architectures. Table 2 provides comparison of MobileNet with two other commonplace CNN architectures. During the exploratory phase of this work it became apparent that the original MobileNet has a tendency to over-fit. As such we have applied slight modifications to the architecture to reduce the over-fitting and increase the generality of the model by removing several layers to reduce model complexity and the addition of several dropout layers. Generally, The largest aspect of a trained machine learning algorithm is the model parameters. Parameters represent the weights and biases that once learnt, define the model's behaviour. The size of the parameters is dependant on the number of layers, units, and connections in the model. As stated we removed repeated layers 10-13 as each layer has the same output shape. The removal of

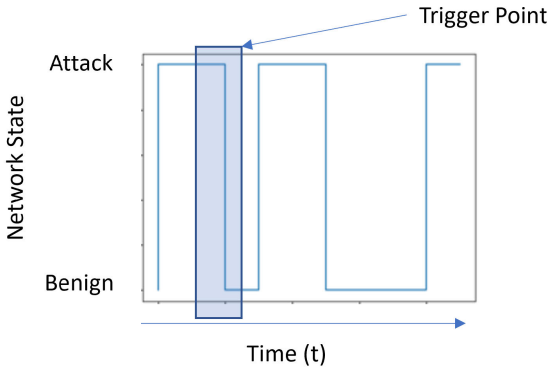


FIGURE 17. Network state moving between benign and attack class.

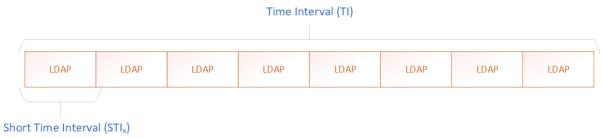


FIGURE 18. Sequence traffic pre-spliced.

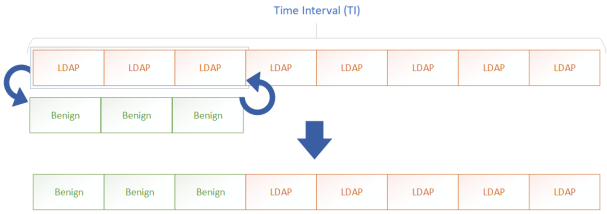


FIGURE 19. Sequence traffic adjustment during and after splice.

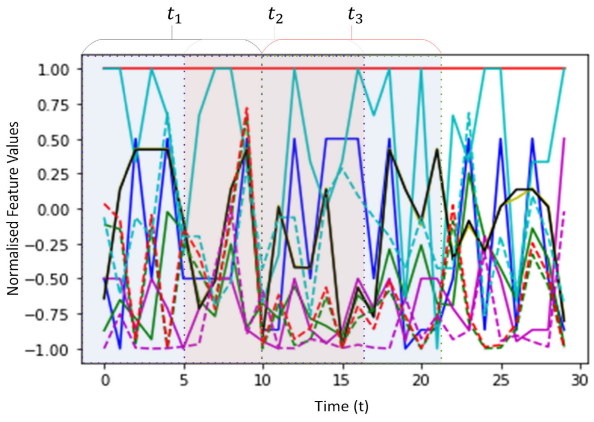


FIGURE 20. Combined Feature Variation over windowed time.

layers in a DNN structure promotes 2 core advantages to this work:

- Model Efficiency: Removing redundant layers reduces the complexity and computational requirements of the network. It can lead to faster training and inference times since there are fewer operations to perform.
- Parameter Reduction: Each layer in a DNN adds parameters to the model. By removing redundant layers, you reduce the number of parameters, which can help mitigate over-fitting, reduce memory requirements, and make the model more manageable.

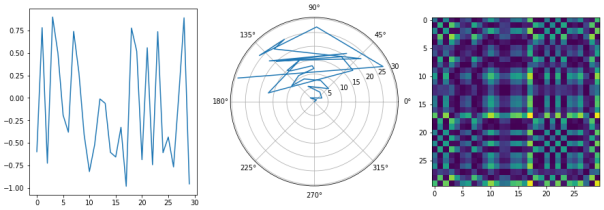


FIGURE 21. One-dimensional time series converted to two-dimensional images in polar coordinate system.

TABLE 2. Comparison of MobileNet to other common CNN architectures.

Model	ImageNet Accuracy	Million Mult-Adds	Million Parameters
MobileNet	70.6%	4866	29.3
GoogleNet	69.8%	1550	6.8
VGG 16	71.5%	15300	138

However, layer removal can also result in the reduction in a networks capacity to generalise. In order to mitigate the possible drop-off in generalization owing to the removal of layers we deploy a set of dropout layers distributed though-out the topology; as dropout layers act as a regularization technique to prevent over-fitting and improve the generalization ability of neural networks.

Overall, we have retained the same initial structure for convolution and feature extraction we have simplified the end result by replacing the standard layers with a standard fully connected layer which employs a softmax activation function; and a dropout layer set to 0.6. This modification has a further effect of reducing the model parameters thereby reducing both the size and computational requirements of the model.

3) COMPUTATIONAL COMPLEXITY

Separable Convolution is divisible in to two components:

- Depth-wise Convolution.
- Point-wise Convolution.

When applying depth-wise convolution each channel is utilised by one convolutional kernel; resulting in the output feature map having the same number of input channels as the original input layer. Following the implementation of depth-wise convolution the resultant output has the same feature map dimensions as the input. The resultant feature maps are combined with using point-wise convolution.

Point-wise convolution operates much the same way as the traditional CNN convolution except it uses a 1×1 kernel to iterate over every instance within the feature map. The depth of the kernel directly corresponds to the number of channels in the previous layer (M) resulting in a kernel size of $1 \times 1XM$.

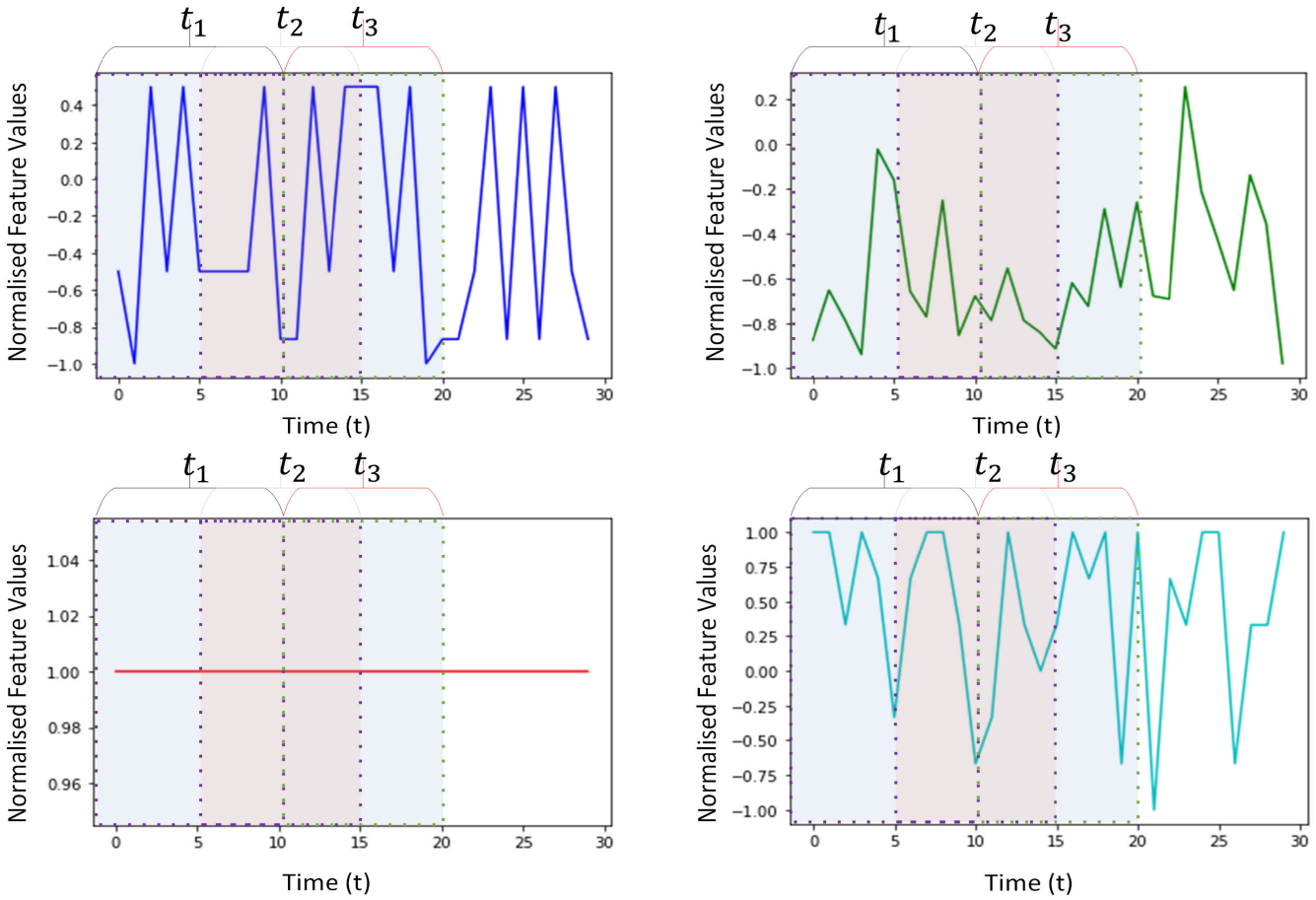


FIGURE 22. Individual feature variation over windowed time.

4) GATED RECURRENT UNIT (GRU)

Convolutional Networks are widely used for extracting the local features of input matrices and therefore are able to isolate and analyse temporal dependencies within the instantaneous subset of a data stream. However, convolutional layers do not account for the dependencies that evolve over a multi-frame sequence. The time series variation of network traffic data has temporal dependencies that extend beyond the borders of a single frame. In order to segregate and evaluate this temporal evolution we intend to combine convolutional analysis with the use of Recurrent Neural Network (RNN) architecture; as its ability to capture temporal context makes it suitable for sequence data. Unfortunately, traditional tanh RNN cells are prone to the vanishing gradient issue and therefore lack the ability to evaluate long-term dependencies which is required for reliable long-term traffic analysis. Long Short Term Memory (LSTM) and Gated Recurrent Units (GRU) networks are two variants based on the recurrent structure able to capture long-term dependencies. The basic RNN captures temporal relationships by evaluating the hidden states - the equation for which is given in Equation 9.

$$h_t = g(W_{x_t} + Uh_{t-1} + b) \tag{9}$$

where x_t is a multi-dimensional (N-Dimensional) input sequence for time 't'. h_t is the m-dimensional hidden state and 'g' the activation function. 'W' and 'U' are m x n and m x m matrices respectively. Finally, b is a bias given as an n x 1 vector. The GRU architecture reduces the gating signal from the LSTM model, operating only two gates; update (z_t) and reset (r_t). The mathematical model breakdown is given in Equations 10 and 11:

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot \tilde{h}_t \tag{10}$$

$$\tilde{h}_t = g(W_h x_t + U_h(r_t \odot h_{t-1}) + b_h) \tag{11}$$

where the two gates are defined as:

$$z_t = \sigma(W_z x_t + U_z h_{t-1} + b_z) \tag{12}$$

$$r_t = \sigma(W_r x_t + U_r h_{t-1} + b_r) \tag{13}$$

Figure 26 provides the GRU architecture comprising the update and reset gate. The function of the update gate is to decide how much the activation function or cell content is adjusted. As with the LSTM, the reset gate facilitates the removal of previous states from the cell memory. Finally, the hidden layer is calculated via 'H_t'. The proposed model, combines both CNN and GRU architectures exploiting the

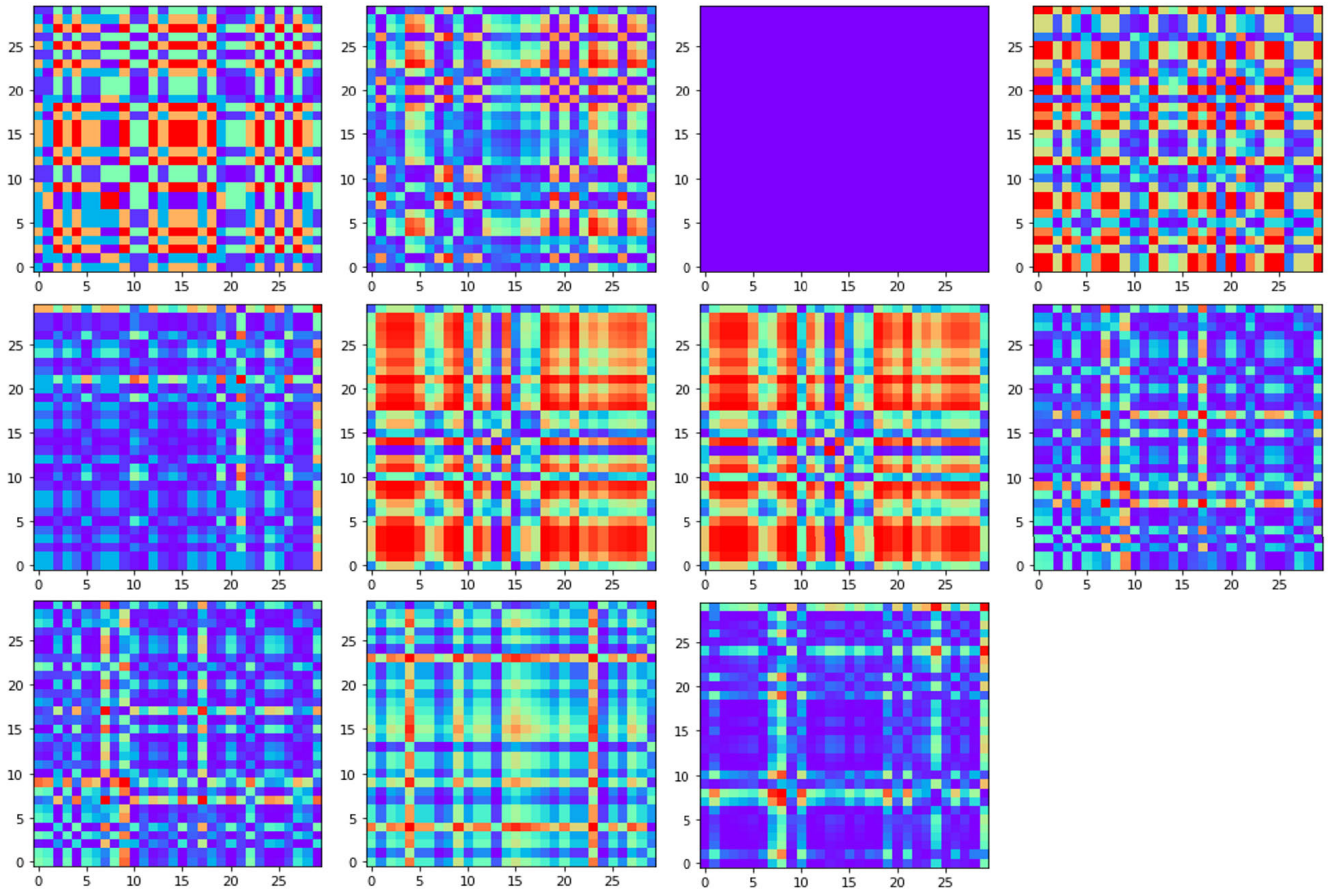


FIGURE 23. One-dimensional time series converted to two-dimensional images through application of GADF.

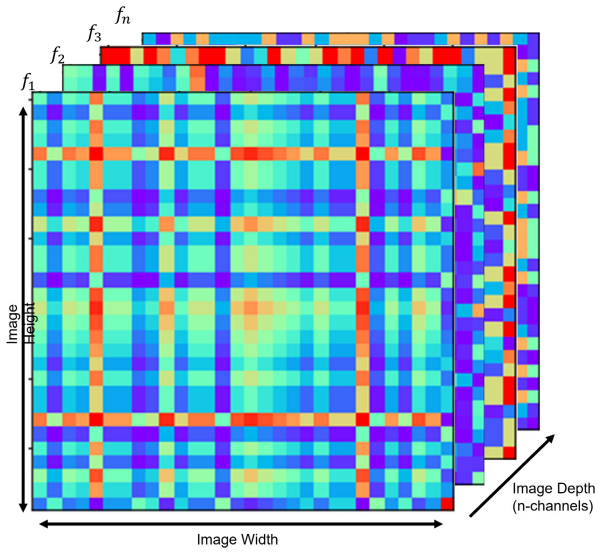


FIGURE 24. GAF output represented in 3-dimensional state space.

strengths of both. Convolutional methods are used for the extraction of local features while GRU captures the long-term dependencies in the time-series data. This combined hybrid topology, enables the capture of diverse information across a range of network features.

5) LATE FUSION

Multi-modal fusion is the process by which information from multiple sources is joined in order to generate a classification. For this work we have focused on late level feature fusion. Compared to feature level fusion which integrates low level features decision level fusion utilises the decision output from each CNN and combines them to obtain the final event classification.

Despite omitting the low level feature interactions which are key to early fusion, late fusion has an added level of flexibility and simplicity in the decision making process.

V. RESULTS AND DISCUSSION

The objective of this work has been to develop a method of prediction and classification for DDoS threats to aviation operational networks. A multi-Channel CNN for feature extraction coupled with a GRU for classification offer a powerful solution to detect and classify cyber-threats within these networks. We introduce four metrics, which will be used

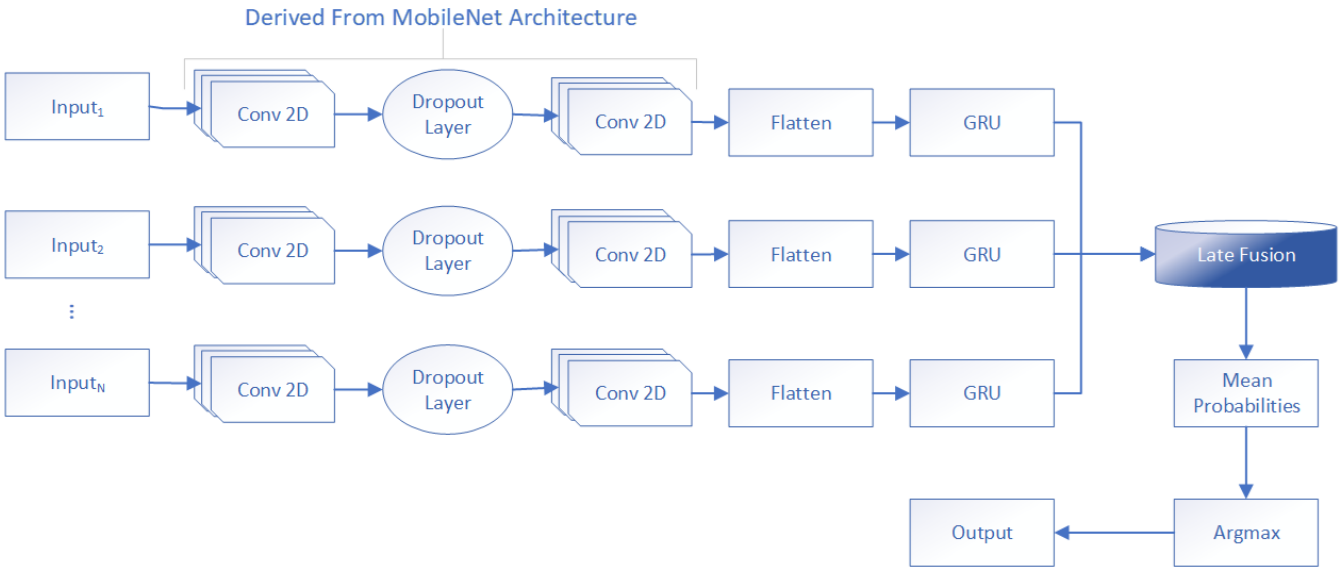


FIGURE 25. CNN-GRU Architecture.

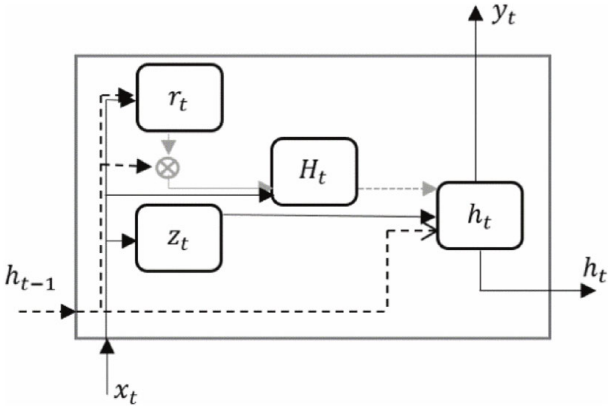


FIGURE 26. GRU architecture.

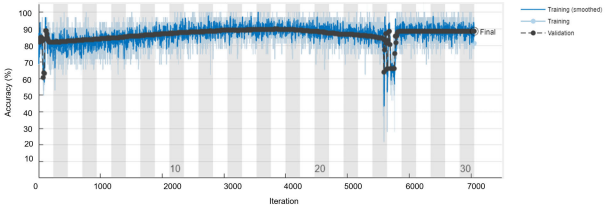


FIGURE 27. Test and validation accuracy variation vs iterations.

to assess the per-class classification performance: Accuracy, Precision, Recall, and F1-score. Initial prototyping of this work was done using MATLAB 2021B combining the Datastore functionality with the Deep Learning Toolbox. Subsequently, simulation and analysis was migrated to Python due to ease of ML implementation and optimisation. Within Python, the 'ptys' package was used for its time series analysis functionality and the TensorFlow software library for CNN and GRU generation, deployment and optimisation. All evaluation was carried out on a PC with an Intel(R) Core(TM) i7-10750H CPU with up to 16GB RAM available. No GPU acceleration as used in this work.

- Precision: The fraction of correctly predicted positives among the total predicted positive observations

$$Precision(P) = \frac{T_p}{T_p + F_p} \tag{14}$$

- Recall: The fraction of correctly predicted positives among all events in the class

$$Recall(R) = \frac{T_p}{T_p + F_n} \tag{15}$$

- F-Score: Weighted average of precision and recall

$$F - Score(F1) = \frac{2 \times P \times R}{P + R} \tag{16}$$

A. EXPERIMENTAL RESULTS

The Accuracy and Loss graphs given in Figures 27 and 28. Initial Evaluation with a learning rate of 0.001 attained a validation accuracy of 89.08%.

The training accuracy and loss of the GAF-CNN-GRU model on a random subset of features contained within the CIC-2019 dataset is shown in Figures 27 and 28. It can be seen that the loss value rapidly decreases over the first epoch then remains predominantly consistent with a few spikes of increasing loss around iteration 5750, after which the losses converge close to -15.

When training on the random CIC subset, the model achieved a training accuracy of 75% and a validation accuracy of 89.08%. On the validation set Precision, Recall and F1 scores were 89.4%, 91.76% and 90.56% respectively.

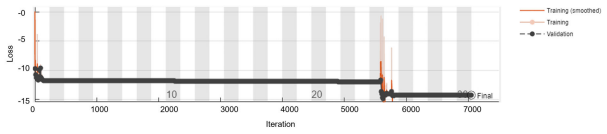


FIGURE 28. Test and validation loss variation vs iteration.

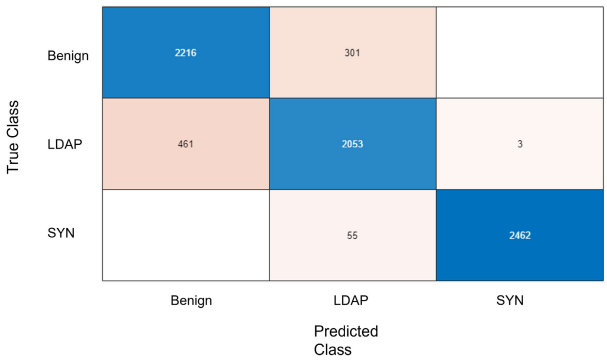


FIGURE 29. Confusion matrix for CIC 2019 training set utilising a randomised subset.

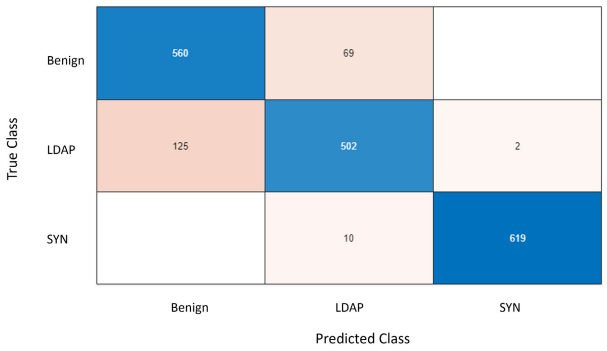


FIGURE 30. Confusion matrix for CIC 2019 validation set using a randomised subset.

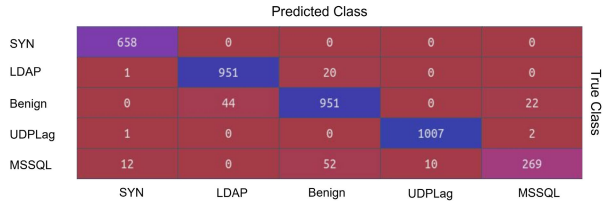


FIGURE 31. Confusion matrix for CIC 2019 validation set using the optimised feature subset.

When evaluating the training confusion matrix given in Figure 29 we see the highest proportion of mis-classifications occurred between the Benign and LDAP classes; with 12% of benign traffic sequences being mis-classified as LDAP and 18.1% of LDAP traffic being wrongly classified as Benign.

This mis-classification carries over to the validation dataset. In Figure 30 we see miss-classification rates of 11.0% and 20.2% for Benign and LDAP traffic sequences respectively.

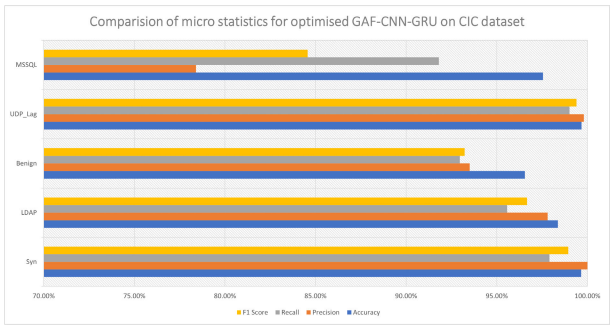


FIGURE 32. Micro statistics of accuracy, precision, recall and f1 Score across CIC Dataset Classes.

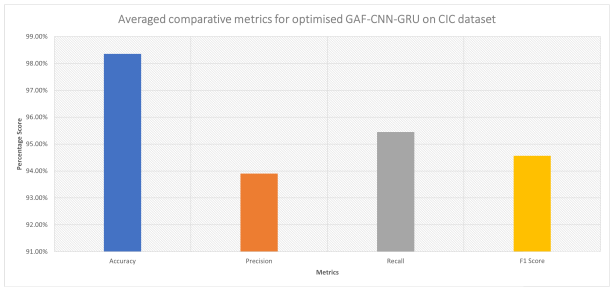


FIGURE 33. Averaged statistics of accuracy, precision, recall and f1 Score across optimised CIC Dataset Classes.

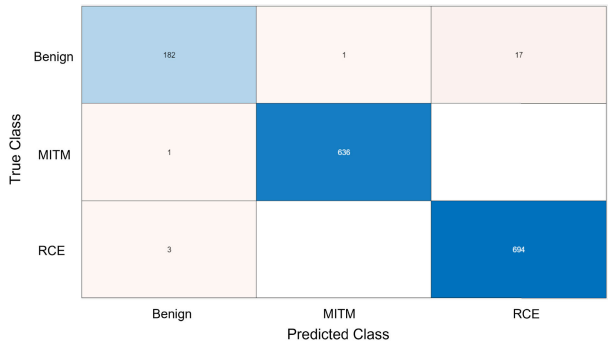


FIGURE 34. Validation confusion matrix when applied to Cranfield Cyber Security Dataset.

Using the random subset of CIC data as a baseline the GAF-CNN-GRU model was re-run using an optimised feature subset. The model achieved an accuracy of 98.36%, the confusion matrix for which is given in Figure 31.

Figure 31 shows the model is able to easily distinguish between SYN, LDAP and UDP Lag. However, there are minor errors in classification of the Benign and MSSQL traffic classes.

The micro-data for each of the target classes is given in Figure 32

Figures 32 and 33 show the Accuracy, Precision and F1 Scores for both individual classes and the average output of the whole model. The method achieved 93.90%, 95.45% and 94.56% for Precision, Recall and F1-score respectively.

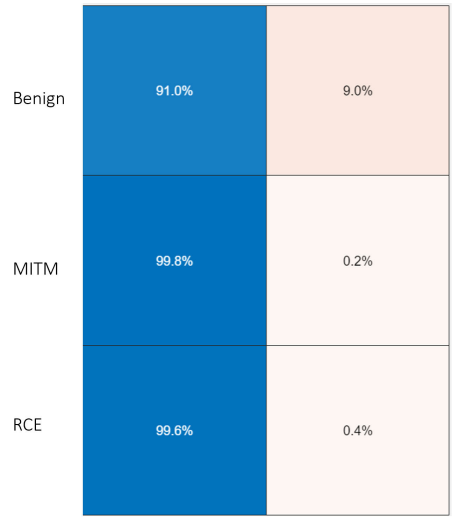


FIGURE 35. Breakdown of true/false positives across classes.

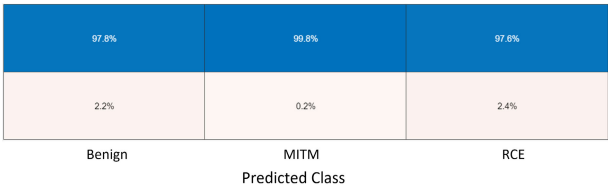


FIGURE 36. Breakdown of percentage accuracy for predicted classes.

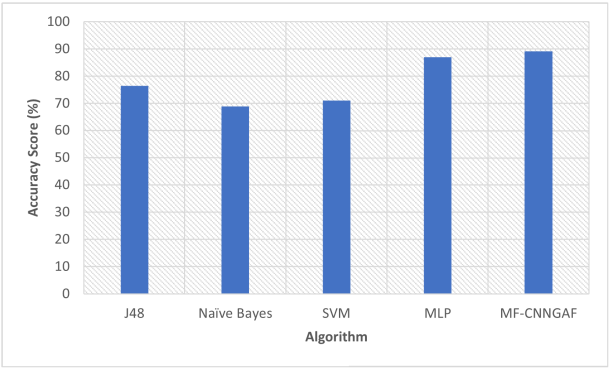


FIGURE 37. Performance of mf-CNNGAF and other models in multi-class classification on the CIC dataset.

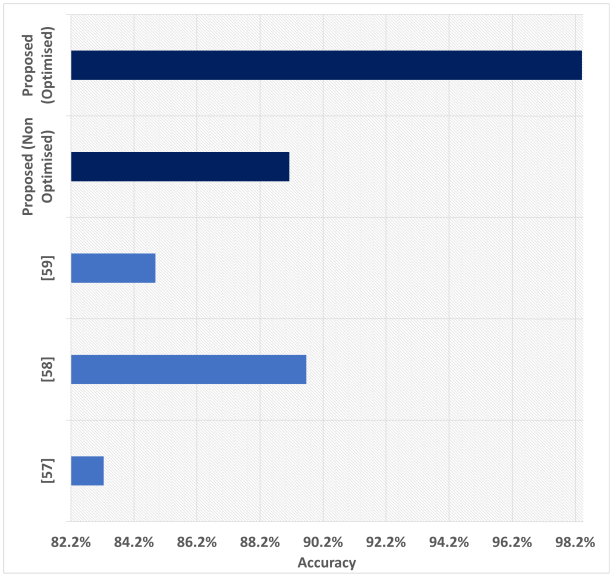


FIGURE 38. Accuracy comparison of mf-CNNGAF and other models in multi-class classification on the CIC dataset.

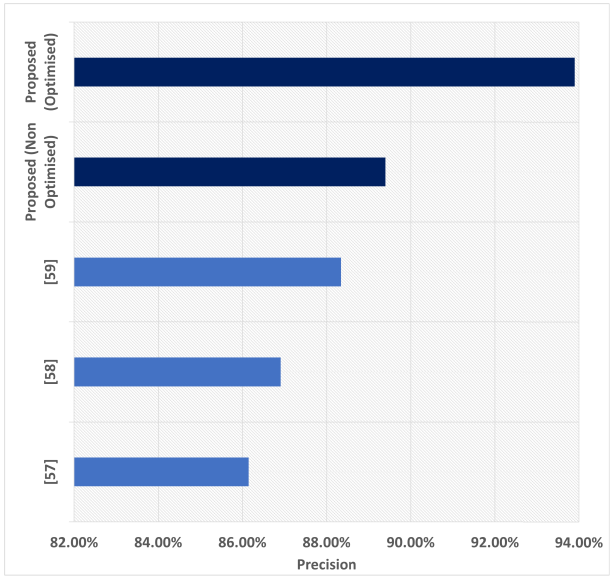


FIGURE 39. Precision comparison of mf-CNNGAF and other models in multi-class classification on the CIC dataset.

Finally, we evaluated the performance of the GAF-mfCNN algorithm on the Cranfield CPS Dataset classification performance in terms of TPR, Accuracy, FPR, Recall, Precision and F-score. The total number of event sequences considered is 1,534 of which our solution correctly classified 1,512 achieving an accuracy of 98.56%. The confusion matrix in Figure 34 provides a class breakdown of predictions vs actual.

Further breakdowns given in Figures 35 and 36.

Precision, Recall and F1-scores of 97.84%, 91% and 94.3% have been achieved respectively on the Cranfield Dataset. To compare this method to existing Machine Learning techniques explored in literature we compared the proposed method to the J48 Decision Tree, Naive Bayes, Support Vector Machine Recurrent Neural Network and Multi-Layer Perception.

Figure 37 shows the results when various Machine Learning algorithms are applied to the testing set. Finally we compare our methodology to three similar time series driven approaches in literature.

- The 1D CNN LSTM proposed in [66] uses the 1D-CNN for supervised learning on time-series data. This method serialises Transmission Control Protocol/Internet Protocol (TCP/IP) packets in a predetermined time range as an invasion Internet traffic model for the IDS.

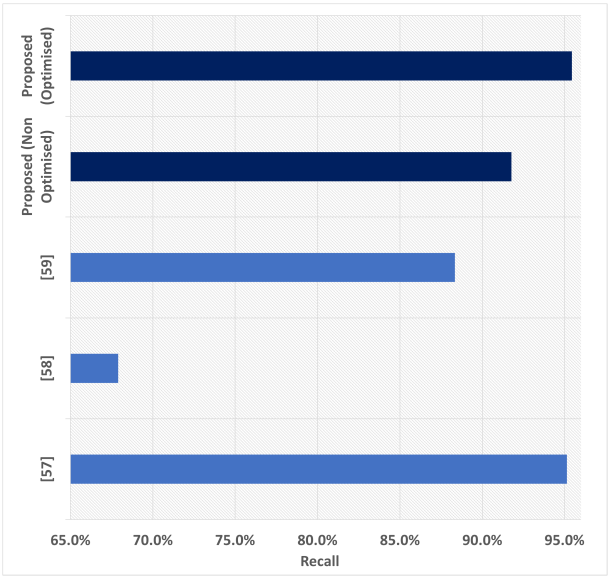


FIGURE 40. Recall of mf-CNNGAF compared to other models in multi-class classification on the CIC dataset.

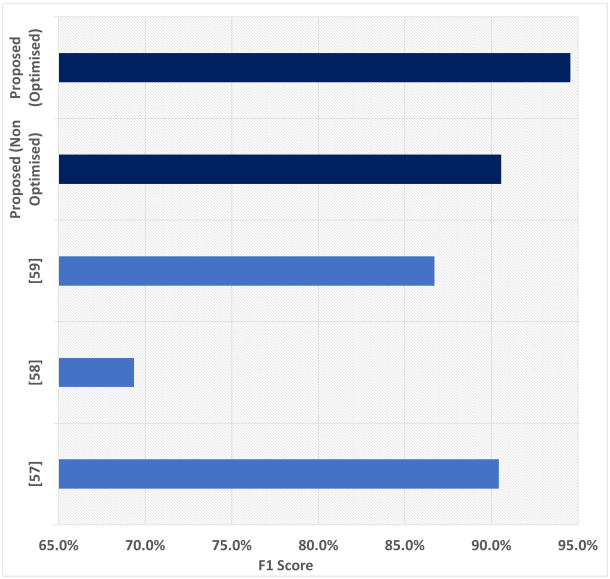


FIGURE 41. F1-Score of mf-CNNGAF compared to other models in multi-class classification on the CIC dataset.

- Reference [67] created a network intrusion detector capable of distinguishing between "bad" connections, which are further categorised into the classifications DoS, Probe, and R2L, and Benign connections by combining LSTM and GRU for dimensionality reduction and time series analysis.
- Reference [68] utilises a pure LSTM to evaluate long term temporal dependencies that connects consecutive tasks to detect anomalous behaviour.

In addition we also compare our approach to CNN driven methodologies evaluated on the CIC 2019 DDoS dataset.

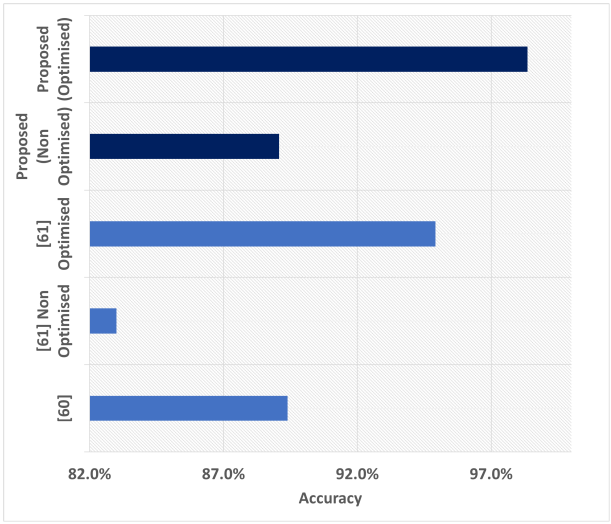


FIGURE 42. Accuracy of mf-CNNGAF compared to other CNN driven models in multi-class classification on the CIC dataset.

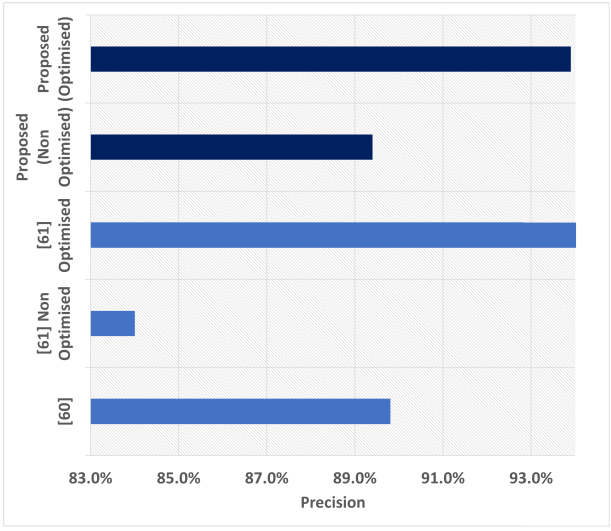


FIGURE 43. Precision of mf-CNNGAF compared to other CNN driven models in multi-class classification on the CIC dataset.

- Reference [69] uses a stacked ensemble of deep learning approaches comprising; Convolutional Neural Network (CNN), Long Short Term Memory (LSTM) network and a Gated Recurrent Unit.
- The methodology identifies high quality features and then uses a CNN to extract the features which are fed in to a BiLSTM to detect DDoS attack events and predict outcomes [70].

Figures 38 - 45 provide a comparison of our approach to current state of the art methodologies. From the Figures we see our approach either matches or exceeds the current state of the art in terms of Accuracy, Recall, F1-Score and precision while operating on a severely reduced feature selection.

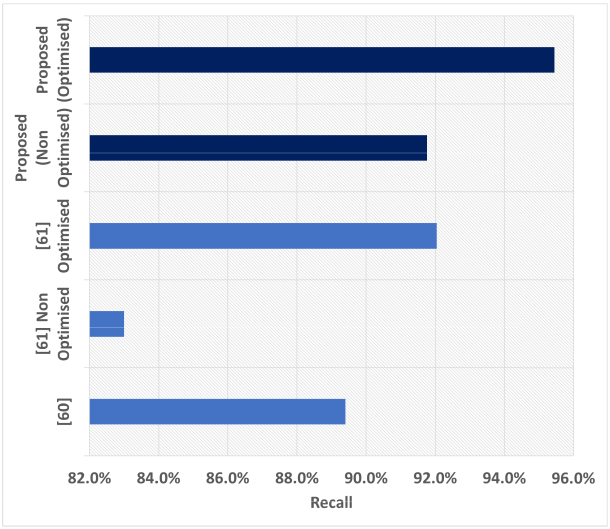


FIGURE 44. Recall of mf-CNNGAF compared to other CNN driven models in multi-class classification on the CIC dataset.

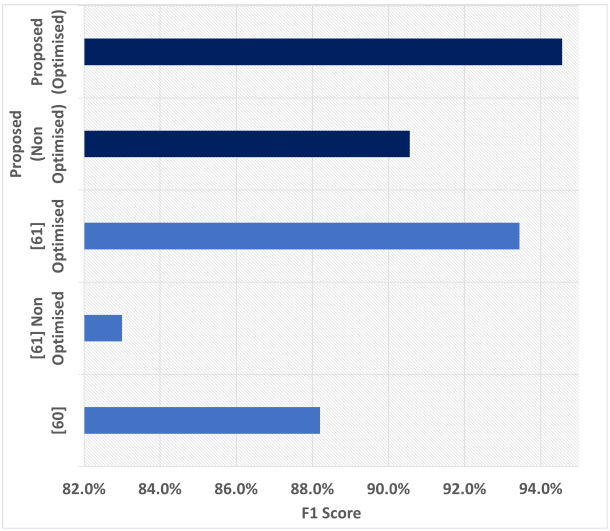


FIGURE 45. F1-Score of mf-CNNGAF compared to other CNN driven models in multi-class classification on the CIC dataset.

VI. CONCLUSION

Cyber Network Traffic can be categorised as a dynamic non linear system within which the recurrence of states can be assumed to hold true due to the inherent periodicities of cyber operation. We breakdown the full time series in to a series of time series features comprising representations of given time series characteristics. We use Gramian Angular Fields to encode time series data in to images representing the signal variation through phase space. Using this phase space time series image representation a multi-channel Convolutional Neural Network-based Gated Recurrent Unit algorithm has been proposed for detection of cyber-attacks, including D(D)oS, RCE and MITM attacks, in air-side aviation edge networks. Conventional detection methods primarily utilise either entropy analysis or apply Machine Learning techniques to network tabular data. This work combines a lightweight CNN based on the MobileNet architecture to work a feature extractor for a GRU combining the spatial analysis generated from the convolutions architecture with the spacio-analytical properties inherent to the GRU to attain a greater level of accuracy with a reduced feature set. The objective of this methodology was achieved via the mf-CNNGRU to evaluate the dynamic shift in network feature states which occurs when a system transitions from benign to attack traffic. This accurate modelling of dynamic state transitions allows the model to detect cyber-attacks in real time with a high degree of accuracy. The input to the proposed algorithm is generated by deploying a sliding window over a series of time series values for a given continuous system variable - this sliding window is utilised to accurately capture the dynamic state evolution of the edge network in real time. Simulation results demonstrated that the GAF multi-channel CNN GRU hybrid detection algorithm can achieve performance gains over the existing time series based anomaly detection methodologies. Furthermore, when comparing to existing purely CNN driven approaches we see our method has a negligible reduction in performance metrics while using a feature set that has been decreased by 96.59% reducing the computational overhead for edge deployment. Generally, feature reduction facilitates a reduced need for resources in order to complete computations in conjunction with less storage capacity.

ACKNOWLEDGMENT

This project is supported by the grant received from Department for Transport (DfT), U.K. Government under the Future Aviation Security Solutions Industrial Ph.D. Partnerships (FASS IPPs)). The research is carried out with the collaboration of Cranfield University, U.K. and Thales, U.K. The authors of this publication are thankful to Thales, U.K. for providing funding and supporting this study.

REFERENCES

[1] R. AlMashari, G. AlJurbua, L. AlHoshan, N. S. Al Saud, O. BinSaeed, and N. Nasser, "IoT-based smart airport solution," in *Proc. Int. Conf. Smart Commun. Netw. (SmartNets)*, Nov. 2018, pp. 1–6.

[2] H. Whitworth, S. Al-Rubaye, A. Tsourdos, J. Jiggins, N. Silverthorn, and K. Thomas, "Aircraft to operations communication analysis and architecture for the future aviation environment," in *Proc. IEEE/AIAA 40th Digit. Avionics Syst. Conf. (DASC)*, Oct. 2021, pp. 1–8.

[3] S. Al-Rubaye and A. Tsourdos, "Airport connectivity optimization for 5G ultra-dense networks," *IEEE Trans. Cognit. Commun. Netw.*, vol. 6, no. 3, pp. 980–989, Sep. 2020.

[4] N. Abosata, S. Al-Rubaye, G. Inalhan, and C. Emmanouilidis, "Internet of Things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications," *Sensors*, vol. 21, no. 11, p. 3654, May 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/11/3654

[5] Y. Tang, Q. Chen, M. Li, Q. Wang, M. Ni, and X. Fu, "Challenge and evolution of cyber attacks in cyber physical power system," in *Proc. IEEE PES Asia–Pacific Power Energy Eng. Conf. (APPEEC)*, Oct. 2016, pp. 857–862.

[6] Y. Zhauniarovich and P. Dodia, "Sorting the garbage: Filtering out DRDoS amplification traffic in ISP networks," in *Proc. IEEE Conf. Netw. Softwarization (NetSoft)*, Jun. 2019, pp. 142–150.

[7] L. Tan, Y. Pan, J. Wu, J. Zhou, H. Jiang, and Y. Deng, "A new framework for DDoS attack detection and defense in SDN environment," *IEEE Access*, vol. 8, pp. 161908–161919, 2020.

[8] A. Warrier, S. Al-Rubaye, D. Panagiotakopoulos, G. Inalhan, and A. Tsourdos, "Interference mitigation for 5G-connected UAV using deep Q-learning framework," in *Proc. IEEE/AIAA 41st Digit. Avionics Syst. Conf. (DASC)*, Sep. 2022, pp. 1–8.

[9] H. Moayyed, M. Mohammadpourfard, C. Konstantinou, A. Moradzadeh, B. Mohammadi-Ivatloo, and A. P. Aguiar, "Image processing based approach for false data injection attacks detection in power systems," *IEEE Access*, vol. 10, pp. 12412–12420, 2022.

[10] Z. Zhou, Z. Chen, T. Zhou, and X. Guan, "The study on network intrusion detection system of snort," in *Proc. Int. Conf. Netw. Digit. Soc.*, vol. 2, May 2010, pp. 194–196.

[11] M. H. Nguyen, Y.-K. Lai, and K.-P. Chang, "An entropy-based DDoS attack detection and classification with hierarchical temporal memory," in *Proc. Asia–Pacific Signal Inf. Process. Assoc. Annu. Summit Conf. (APSIPA ASC)*, Dec. 2021, pp. 1942–1948.

[12] K. Bavani, M. P. Ramkumar, and E. Selvan G. S. R., "Statistical approach based detection of distributed denial of service attack in a software defined network," in *Proc. 6th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Mar. 2020, pp. 380–385.

[13] S. Oshima, A. Hirakawa, T. Nakashima, and T. Sueyoshi, "DoS/DDoS detection scheme using statistical method based on the destination port number," in *Proc. 5th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Sep. 2009, pp. 206–209.

[14] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2015, pp. 77–81.

[15] N. I. G. Dharma, M. F. Muthohar, J. D. A. Prayuda, K. Priagung, and D. Choi, "Time-based DDoS detection and mitigation for SDN controller," in *Proc. 17th Asia–Pacific Netw. Operations Manage. Symp. (APNOMS)*, Aug. 2015, pp. 550–553.

[16] R. Wang, Z. Jia, and L. Ju, "An entropy-based distributed DDoS detection mechanism in software-defined networking," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug. 2015, pp. 310–317.

[17] A. H. Hamamoto, L. F. Carvalho, L. D. H. Sampaio, T. Abrão, and M. L. Proença, "Network anomaly detection system using genetic algorithm and fuzzy logic," *Exp. Syst. Appl.*, vol. 92, pp. 390–402, Feb. 2018, doi: 10.1016/j.eswa.2017.09.013.

[18] P. S. Saini, S. Behal, and S. Bhatia, "Detection of DDoS attacks using machine learning algorithms," in *Proc. 7th Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, Mar. 2020, pp. 16–21.

[19] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer Internet of Things devices," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2018, pp. 29–35.

[20] P. Verma, S. Anwar, S. Khan, and S. B. Mane, "Network intrusion detection using clustering and gradient boosting," in *Proc. 9th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2018, pp. 1–7.

[21] T. T. Khoei, G. Aissou, W. C. Hu, and N. Kaabouch, "Ensemble learning methods for anomaly intrusion detection system in smart grid," in *Proc. IEEE Int. Conf. Electro Inf. Technol. (EIT)*, May 2021, pp. 129–135.

[22] D. Perez, M. A. Astor, D. P. Abreu, and E. Scalise, "Intrusion detection in computer networks using hybrid machine learning techniques," in *Proc. 43rd Latin Amer. Comput. Conf. (CLEI)*, Sep. 2017, pp. 1–10.

[23] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2019, pp. 1–8.

[24] M. V. O. de Assis, L. F. Carvalho, J. J. P. C. Rodrigues, J. Lloret, and M. L. Proença Jr., "Near real-time security system applied to SDN environments in IoT networks using convolutional neural network," *Comput. Electr. Eng.*, vol. 86, Sep. 2020, Art. no. 106738. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790620305930

[25] K. Alrawashdeh and C. Purdy, "Toward an online anomaly intrusion detection system based on deep learning," in *Proc. 15th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2016, pp. 195–200.

[26] J. Kim, N. Shin, S. Y. Jo, and S. Hyun Kim, "Method of intrusion detection using deep neural network," in *Proc. IEEE Int. Conf. Big Data Smart Comput. (BigComp)*, Feb. 2017, pp. 313–316.

[27] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," in *Proc. IEEE Local Comput. Netw. Conf.*, Oct. 2010, pp. 408–415.

[28] X. Yuan, C. Li, and X. Li, "DeepDefense: Identifying DDoS attack via deep learning," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, May 2017, pp. 1–8.

[29] A. Koay, A. Chen, I. Welch, and W. K. G. Seah, "A new multi classifier system using entropy-based features in DDoS attack detection," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2018, pp. 162–167.

[30] D. Kaur, A. Anwar, I. Kamwa, S. Islam, S. M. Muyeen, and N. Hosseinzadeh, "A Bayesian deep learning approach with convolutional feature engineering to discriminate cyber-physical intrusions in smart grid systems," *IEEE Access*, vol. 11, pp. 18910–18920, 2023.

[31] B. I. Hairab, M. S. Elsayed, A. D. Jurcut, and M. A. Azer, "Anomaly detection based on CNN and regularization techniques against zero-day attacks in IoT networks," *IEEE Access*, vol. 10, pp. 98427–98440, 2022.

[32] Z. Wu, H. Zhang, P. Wang, and Z. Sun, "RTIDS: A robust transformer-based approach for intrusion detection system," *IEEE Access*, vol. 10, pp. 64375–64387, 2022.

[33] M. A. Naderi and H. Mahdavi-Nasab, "Analysis and classification of EEG signals using spectral analysis and recurrent neural networks," in *Proc. 17th Iranian Conf. Biomed. Eng. (ICBME)*, Nov. 2010, pp. 1–4.

[34] L. Wang, K. Keong Teo, and Z. Lin, "Predicting time series with wavelet packet neural networks," in *Proc. Int. Joint Conf. Neural Netw.*, 2001, pp. 1593–1597.

[35] M. Poulos and S. Papavlasopoulos, "Automatic stationary detection of time series using auto-correlation coefficients and LVQ—Neural network," in *Proc. IISA*, Jul. 2013, pp. 1–4.

[36] A. Botalb, M. Moinuddin, U. M. Al-Saggaf, and S. S. A. Ali, "Contrasting convolutional neural network (CNN) with multi-layer perceptron (MLP) for big data analysis," in *Proc. Int. Conf. Intell. Adv. Syst. (ICIAS)*, Aug. 2018, pp. 1–5.

[37] C. Xu, "Applying MLP and CNN on handwriting images for image classification task," in *Proc. 5th Int. Conf. Adv. Electron. Mater., Comput. Softw. Eng. (AEMCSE)*, Apr. 2022, pp. 830–835.

[38] R. D. Yogaswara and A. D. Wibawa, "Comparison of supervised learning image classification algorithms for food and non-food objects," in *Proc. Int. Conf. Comput. Eng., Netw. Intell. Multimedia (CENIM)*, Nov. 2018, pp. 317–324.

[39] *858P1 Internet Protocol Suite (IPS) for Aeronautical Safety Services, Part 1, Technical Requirements*, ARINC, Annapolis, MD, USA, 2021.

[40] EUROCONTROL and Federal Aviation Authority Future Communication Study Operational Concepts and Requirements Team, "Chapter 4.3.3.1: Threat identification," Commun. Oper. Concept Requirements Future Radio Syst. V2, 2007, p. 72.

[41] A. Prajapati, A. Sakadasariya, and J. Patel, "Software defined network: Future of networking," in *Proc. 2nd Int. Conf. Inventive Syst. Control (ICISC)*, Jan. 2018, pp. 1351–1354.

[42] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A review," in *Proc. Int. Conf. Comput. Sci. Electron. Eng.*, vol. 3, Mar. 2012, pp. 648–651.

[43] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[44] M. H. Shahriar, N. I. Haque, M. A. Rahman, and M. Alonso Jr., "G-IDS: Generative adversarial networks assisted intrusion detection system," 2020, *arXiv:2006.00676*.

[45] T. Pollard and J. Clark, "Connected aircraft: Cyber-safety risks, insider threat, and management approaches," in *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, 2019, pp. 3232–3241.

[46] D. Geer, "Malicious bots threaten network security," *Computer*, vol. 38, no. 1, pp. 18–20, 2005.

[47] P. Wang, L. Wu, B. Aslam, and C. C. Zou, "A systematic study on peer-to-peer botnets," in *Proc. 18th Int. Conf. Comput. Commun. Netw.*, Aug. 2009, pp. 1–8.

[48] T. Lange and H. Kettani, "On security threats of botnets to cyber systems," in *Proc. 6th Int. Conf. Signal Process. Integr. Netw. (SPIN)*, Mar. 2019, pp. 176–183.

[49] S. Muzafar and N. Jhanjhi, "DDoS attacks on software defined network: Challenges and issues," in *Proc. Int. Conf. Bus. Analytics Technol. Secur. (ICBATS)*, Feb. 2022, pp. 1–6.

[50] M. Polese, F. Chiariotti, E. Bonetto, F. Rigotto, A. Zanella, and M. Zorzi, "A survey on recent advances in transport layer protocols," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3584–3608, 4th Quart., 2019.

[51] Y. Wang, T. T. Gamage, and C. H. Hauser, "Security implications of transport layer protocols in power grid synchrophasor data communication," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 807–816, Mar. 2016.

[52] K. Geetha and N. Sreenath, "SYN flooding attack—Identification and analysis," in *Proc. Int. Conf. Inf. Commun. Embedded Syst.*, 2014, pp. 1–7.

[53] B. Smith, "A storm (Worm) is brewing," *Computer*, vol. 41, no. 2, pp. 20–22, Feb. 2008.

[54] C. Rossow, "Amplification hell: Revisiting network protocols for DDoS abuse," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2014, pp. 1–15.
[55] A. Aloseel, S. Al-Rubaye, A. Zolotas, H. He, and C. Shaw, "A novel approach for detecting cyberattacks in embedded systems based on anomalous patterns of resource utilization—PART I," *IEEE Access*, vol. 9, pp. 103204–103229, 2021.
[56] *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*, IEEE Standard td 610, 1991, pp. 1–217.
[57] S. G. Gollagi, P. K. Pareek, and M. Karamthoti, "Recursive feature elimination based multi-variate Naïve Bayes classification for product recommendation," in *Proc. 4th Int. Conf. Emerg. Res. Electron., Comput. Sci. Technol. (ICERECT)*, Dec. 2022, pp. 1–8.
[58] I. Guyon and A. Elisseeff, "An introduction of variable and feature selection," *J. Mach. Learn. Res.*, vol. 3, pp. 1157–1182, Jun. 2003.
[59] Z. Wang and T. Oates, "Imaging time-series to improve classification and imputation," 2015, *arXiv:1506.00327*.
[60] H. Xu, J. Li, H. Yuan, Q. Liu, S. Fan, T. Li, and X. Sun, "Human activity recognition based on Gramian angular field and deep convolutional neural network," *IEEE Access*, vol. 8, pp. 199393–199405, 2020.
[61] S. Popov, S. Morozov, and A. Babenko, "Neural oblivious decision ensembles for deep learning on tabular data," 2019, *arXiv:1909.06312*.
[62] Y. Zhu, T. Brettin, F. Xia, A. Partin, M. Shukla, H. Yoo, Y. A. Evrard, J. H. Doroshow, and R. L. Stevens, "Converting tabular data into images for deep learning with convolutional neural networks," *Sci. Rep.*, vol. 11, no. 1, p. 11325, May 2021.
[63] H.-C. Shin, H. R. Roth, M. Gao, L. Lu, Z. Xu, I. Nogues, J. Yao, D. Mollura, and R. M. Summers, "Deep convolutional neural networks for computer-aided detection: CNN architectures, dataset characteristics and transfer learning," *IEEE Trans. Med. Imag.*, vol. 35, no. 5, pp. 1285–1298, May 2016.
[64] M. E. Paoletti, J. M. Haut, S. K. Roy, and E. M. T. Hendrix, "Rotation equivariant convolutional neural networks for hyperspectral image classification," *IEEE Access*, vol. 8, pp. 179575–179591, 2020.
[65] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, and H. Adam, "MobileNets: Efficient convolutional neural networks for mobile vision applications," 2017, *arXiv:1704.04861*.
[66] M. Azizjon, A. Jumabek, and W. Kim, "1D CNN based network intrusion detection with normalization on imbalanced data," in *Proc. Int. Conf. Artif. Intell. Inf. Commun. (ICAIIC)*, Feb. 2020, pp. 218–224.
[67] R. Koniki, M. D. Ampapurapu, and P. K. Kollu, "An anomaly based network intrusion detection system using LSTM and GRU," in *Proc. Int. Conf. Electron. Syst. Intell. Comput. (ICESIC)*, Apr. 2022, pp. 79–84.
[68] S. A. Althubiti, E. M. Jones, and K. Roy, "LSTM for anomaly-based network intrusion detection," in *Proc. 28th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2018, pp. 1–3.
[69] M. I. Sayed, I. M. Sayem, S. Saha, and A. Haque, "A multi-classifier for DDoS attacks using stacking ensemble deep neural network," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, May 2022, pp. 1125–1130.
[70] D. Alghazzawi, O. Bamasag, H. Ullah, and M. Z. Asghar, "Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection," *Appl. Sci.*, vol. 11, no. 24, p. 11634, Dec. 2021. [Online]. Available: https://www.mdpi.com/2076-3417/11/24/11634



HUW WHITWORTH received the degree in electronic and communications engineering from the University of Kent, in summer 2019, with a focus on embedded systems engineering and antenna design, and the M.Sc. degree in applied artificial intelligence from Cranfield University, in September 2019. He is currently pursuing the Ph.D. degree in future communication methods and security, under the supervision of Dr. Saba Al-Rubaye. His M.Sc. thesis was on synthetic data generation for augmenting datasets. He is currently funded by Thales, U.K., and the U.K. DfT, based at Cranfield University's DARTeC facility where his research area is future communications networks. Recent work includes reviewing data exchanges between actors, analyzing security and vulnerabilities in these networks, and producing countermeasures and security methodologies to existing and zero-day cyber threats.



SABA AL-RUBAYE (Life Senior Member, IEEE) is a Reader in autonomous and connected systems with the School of Aerospace, Transport, and Manufacturing, Cranfield University, U.K. She is leading and was involved with several projects, including project Rise, UAS Authentication Service and Aviation Innovation in the South-West, H2020 SESAR AMULED, and DfT-Smart Airport to develop, design new connectivity techniques, and integrated software/hardware hub proof of concept. She is participating in developing industry standards by being an Active Research Group Member of IEEE P1932.1 standard of license/unlicensed interoperability and IEEE P1920.2, Standard for Vehicle-to-Vehicle Communications for Unmanned Aircraft Systems. She has published many papers in IEEE journals and conferences. She was a recipient of the Best Technical Paper Award twice published in IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, in 2011 and 2015, respectively. She has been the General Co-Chair and the TPC Co-Chair and has held other leading roles for many international conferences. She has delivered tutorials at IEEE ICC, IEEE WCNC, and IEEE VTC conferences, and invited talks at various venues, including the Communications Research Centre (CRC) of Canada, the IEEE Toronto Chapter, and the IEEE U.K. Chapter. She is a Chartered Engineer (C.Eng.) and a member of the Institute of Engineering and Technology (IET). She is holding a commercial certificate of Unmanned Aircraft Systems (UAS) Pilot, U.K.



ANTONIOS TSOURDOS is the Director of Research and the Head of the Autonomous and Cyber-Physical Systems Centre with the School of Aerospace, Transport and Manufacturing, Cranfield University, U.K. He has published several papers on topics related to UAS including assured autonomy, sense and avoid, connectivity, and networking UAS. He is the Chair of the International Federation of Automatic Control (IFAC) Technical Committee on Aerospace Control and a member of the American Institute of Aeronautics and Astronautics (AIAA) Unmanned Systems Integration and Outreach Committee, the IMechE Mechatronics, Informatics and Control Group Board, and the IET Aerospace Executive Team. He is an Editorial Board Member of the *Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering, the Aerospace Science and Technology*, the *International Journal of Systems Science*, and the *Journal of Intelligent and Robotic Systems*. He has been involved in a number of UKRI-funded Future Flight Challenge projects focused on advanced air mobility and drone operations as well as EPSRC-funded projects on autonomy.



JULIA JIGGINS is responsible for developing Thales UK's market opportunities for future aviation and space products and services across the whole of the aerospace and space environment. As the Head of Strategic Marketing-Aviation and Space at Thales UK, she is responsible for planning and executing the marketing strategy for the organization as well as for new and existing products and services. In addition to keeping track of the market's customers' needs, industry trends, and competitor analysis to ensure Thales is strategically placed in the highly competitive environment of aerospace and aviation.



https://dspace.org/

5G aviation networks using novel AI approach for DDoS detection

Whitworth, Huw; Al-Rubaye, Saba; Tsourdos, Antonios; Jiggins, Julia

2023-07-17
Institute of Electrical and Electronics Engineers (IEEE)
https://doi.org/10.1109/ACCESS.2023.3296311
Whitworth H, Al-Rubaye S, Tsourdos A, Jiggins J. (2023) 5G aviation networks using novel AI approach for DDoS detection. IEEE Access, Volume 11, July 2023, pp. 77518-77542

Downloaded from a DSpace repository. https://dspace.org/