

ROSE⁺: A Robustness-Optimized Security Scheme Against Cascading Failures in Multipath TCP under LDDoS Attack Streams

Jinquan Nie[†] Lejun Ji[†] Yirui Jiang[§] Young Ma[‡] Yuanlong Cao^{†,‡}

[†]School of Software, Jiangxi Normal University, Nanchang 330022, China

[‡]School of Computer and Information Engineering, Jiangxi Normal University, Nanchang 330022, China

[§]School of Water, Energy, and Environment Cranfield University Bedfordshire MK43 0AL, UK
{jqnie, ji_lejun, may, ylcao}@jxnu.edu.cn yirui.jiang@cranfield.ac.uk

Abstract—Multipath TCP leverages parallel data transmission across multiple paths to improve transmission rates, reliability, and resource utilization. However, Multipath TCP faces severe network security and communication reliability challenges when exposed to low-rate distributed denial-of-service (LDDoS) attacks. In this paper, we propose a robustness optimization security scheme against cascading failures in Multipath TCP (ROSE⁺) to tackle the challenges posed by Low-rate Distributed Denial of Service (LDDoS) attacks on network security and communication reliability. The scheme integrates the intricate network load-capacity cascading failures model and leverages the unique characteristics of multipath TCP to facilitate the redistribution of load traffic at ineffectiveness nodes, thereby alleviating the cascading failures induced by LDDoS attack streams. Additionally, we optimize the robustness of communication transmission systems by devising a load-capacity cascading failures model. The experimental results demonstrate that the scheme reduces the probability of cascading failures by 20.07%. This research provides new ideas and methods to improve the robustness and destruction resistance of multipath TCP transmission.

I. INTRODUCTION

Over recent decades, the Transmission Control Protocol (TCP) [1] has demonstrated robust efficacy in facilitating network communications. Nonetheless, the evolving landscape of cyber threats has introduced complexities and heightened challenges to network security and reliability [2]. The TCP protocol relies on a single-path transmission in each connection, which makes it an easy target for Denial of Service (DoS) [3] attacks, leading to single points of failure and connection interruptions, further affecting service availability.

Current defense strategies predominantly focus on anomaly detection and blocking of obvious high-speed pulse attacks. Methods such as rate-limiting, traffic analysis, and black-hole filtering are effective in mitigating DoS attacks. However, the Low-rate Distributed Denial of Service (LDDoS) [4] attack is known for its stealthiness as an evolved version of DoS attacks. LDDoS attacks deplete vital network resources, including bandwidth, computational capacity, and memory, culminating in service quality degradation or total system incapacitation. It is characterized by transferring traffic to the

target in a low-rate, decentralized manner to elude conventional detection mechanisms.

Although the TCP protocol exhibits adaptive capabilities, allowing it to manage a certain level of attacks and path ineffectiveness through congestion control and traffic shaping, its effectiveness diminishes in a multipath environment. Since Multipath TCP [5] allows the use of multipath for data transfer, when one path is ineffective due to LDDoS attacks, Multipath TCP tries to transfer the data to other available paths. As depicted in Fig. 1, the LDDoS attacks seize network resources through dispersed low-rate traffic, incapacitating the targeted node's ability to process legitimate requests.

This can precipitate node overloads and result in cascading failures [6]. Subsequently, load redistribution ensues, with the compromised node offloading its traffic to adjacent network nodes in accordance with established protocols. However, this adaptive mechanism does not completely solve the problem because when multiple paths are attacked at the same time or the load is suddenly increased, the load of the remaining paths may quickly reach its capacity limit, leading to overloading and failure of more nodes.

At present, the collective research efforts of experts and scholars both domestically and internationally have predominantly focused on various facets of the multipath TCP, encompassing protocol specification [7], data scheduling [8], congestion control [9], and fairness concerns [10]. However, there has been insufficient focus on the robustness aspects of multipath TCP. Notably, there is a lack of academic research dedicated to optimizing robustness and resilience analysis within multipath TCP transmission [11].

Inspired by the preceding discourse, we propose a robustness-optimized security scheme against cascading failures in multipath TCP (ROSE⁺). This scheme integrates a complex network load-capacity model against cascading failure with the inherent characteristics of the multipath TCP. ROSE⁺ facilitates cross-path redistribution of load traffic at ineffectiveness nodes, thereby mitigating the cascading failures induced by LDDoS attack streams. The primary contributions of this paper are outlined as follows:

- We analyze for the first time the robustness of cascading

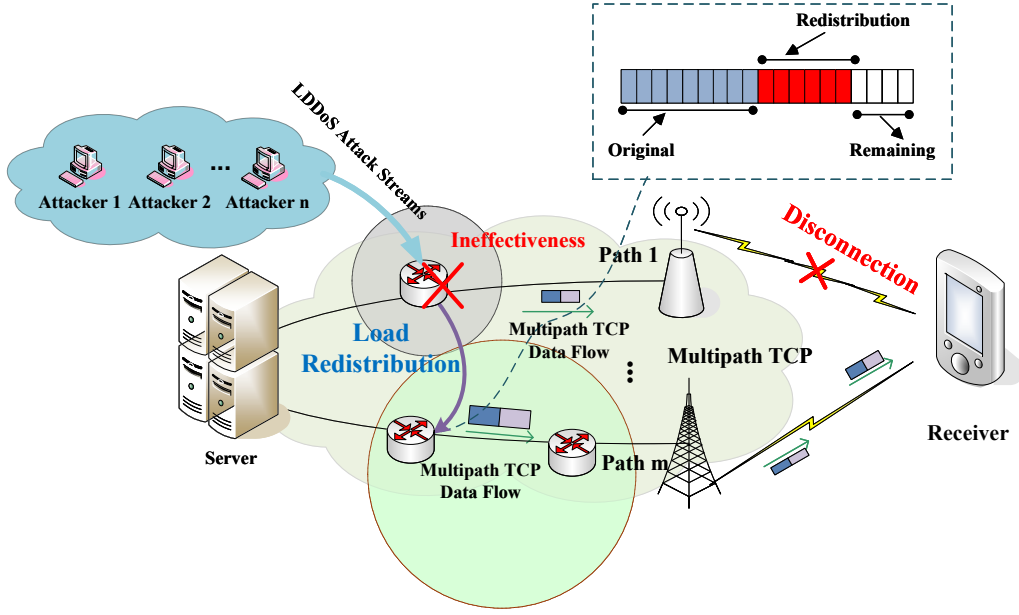


Fig. 1. Diagram of Cascading Failures in the multipath transmission.

failures occurring under LDDoS attacks in the multipath TCP. We construct a load-capacity cascading failures model to visualize the cascading failures behavior from the perspective of attack strategies and optimize the robustness model of the communication transmission, to avoid the large-scale spread of cascading failures in the network.

- Based on the above constructed model, we further optimize by the load redistribution method based on the ratio of node-free capacity. Finally, the effectiveness and robustness of the algorithm are verified through simulation experiments and performance evaluation, and the performance is evaluated in terms of the probability of cascading failures, average throughput, packet disorder, and jitter rate, respectively.

The remainder of this paper is structured as follows. Section II provides a comprehensive overview of the ROSE⁺ scheme design. In Section III, the results obtained from simulation experiments are presented. Finally, conclusions and future work are given.

II. OVERVIEW OF ROSE⁺

To facilitate understanding and readability of the scheme of ROSE⁺, we have compiled important symbols in Table I.

We can construct an abstract model of the multipath TCP transmission topology using an unweighted network graph denoted as G . This graph consists of n nodes and m edges, where the sender, receiver, and each communication node have bidirectional communication capabilities. The concrete representation of this unweighted network graph is defined as follows,

$$G = (V, E), \quad (1)$$

TABLE I
NOTATIONS USING ROSE⁺

Notations	Descriptions
α, β	Tolerance factor
f_{ij}	The carrying of traffic function with the node pairs $\langle v_i, v_j \rangle$
$C_i(t)$	Communication capacity at moment t of the i -th node
$L_i(t)$	The Communication load at moment t of the i -th node
$Q_i(t)$	The proportion of free capacity at moment t of the i -th node
Ψ	The node collection of lose effectiveness nodes
Ω	The node collection of neighbors of the lose effectiveness nodes
RTT_{sk}	The Round-Trip Time between v_s and v_k .

where $V = \{v_1, v_2, v_3, \dots, v_n\}$ denotes the multipath transmission system contains n transmission nodes ($n = |V|$), $E = \{\langle v_i, v_j \rangle\}$ denotes the multipath transmission system contains m edges ($m = |E|$).

Secondly, the construction of a robustness analysis model for multipath TCP transmission, rooted in the load-capacity cascading failures model, necessitates the determination of the initial communication load and the definition of communication capacity on the node.

Taking the k -th transmission node as an example, i.e., $v_k \in V$, assume that its initial communication load as the packets sent between all node pairs $\langle v_i, v_j \rangle$, then it can be specifically expressed as,

$$L_k(0) = \left(\sum_{(i,j) \in V} f_{ij}(k) + \sum_{(j,i) \in V} f_{ji}(k) \right) \cdot T_{interval}, \quad (2)$$

where f_{ij} represents the carrying of traffic function at the node pairs $\langle v_i, v_j \rangle$, denotes the feasible flow sent by the v_i to the v_j . Let $L_k(0)$ represent the initial communication load experienced by the entity v_k over a predefined time interval

$T_{interval}$, which is by default set to 100ms.

Assuming that the transmission nodes in a multipath TCP transmission network possess data carrying and data transmission capabilities, the communication capacity of the transmission nodes can be expressed using the Motter-Lai model [12] as follows,

$$C_k(t) = L_k(0) + \alpha \cdot L_k(t)^\beta, \quad (3)$$

where $C_k(t)$ denotes the communication capacity of the transmission node v_k , the tolerance coefficient $\alpha \geq 0, \beta > 0$, with specific values determined based on the network's actual conditions. For simplification purposes, we adopt a linear load-capacity model, where β defaults 1. The communication capacity of each transmission node is directly influenced by its initial load and is further modulated by the tolerance factor.

To enhance real-time feedback on the transmission capacity of each communication node, specific communication statuses are assigned based on their communication load. These statuses include "normal", "weak communication", and "ineffectiveness". This relationship can be expressed as follows,

$$S_k(t) \doteq \begin{cases} normal, & L_k(t) \leq L_k(0) \\ weak\ communication, & L_k(0) < L_k(t) < C_k \\ ineffectiveness, & L_k(t) \geq C_k \end{cases}, \quad (4)$$

where $S_k(t)$ denotes the communication state value of the node at the t moment. If the $S_k(t)$ is in "ineffectiveness" status, the current v_k enters the set Ψ , the set of failed nodes.

When a transmission node is identified as failing, the process of redistributing the load from that node to its neighboring nodes is referred to as "load redistribution". An effective and judicious load redistribution scheme serves as a pivotal measure in averting cascading failures within multipath TCP transmission. The load capacity of the transmission node itself is considered in the load redistribution policy, thus defining the following the ratio of idle capacity,

$$Q_s(t) = 1 - \frac{L_s(t)}{\max(L_s(0), C_s(t))}, \quad (5)$$

where $Q_s(t)$ denotes the proportion of free capacity of the $v_s \in \Omega$ at the t moment, Ω is the set of neighbors of the failed nodes. At this point, the load increment assigned by the lose effectiveness node $v_k \in \Psi$ to the neighboring node $v_s \in \Omega$ is,

$$\Delta L_s(t) = Q_s(t) \cdot \sum_{k \in \Psi}^N L_k(t) \cdot \frac{C_s / RTT_{sk}}{\sum_{s,j \in \Omega} C_j / RTT_{jk}}, \quad (6)$$

where N is the number of failed redistribution, and RTT_{sk} represents the Round-Trip Time (RTT) between v_s and v_k . At this juncture, the load redistribution strategy within the robustness model of multipath TCP is influenced by various factors, including the node's load capacity (expressed as the node-free capacity ratio) and the status of communication links. This strategy is dynamically computed and updated in real time.

Upon determining the load redistribution strategy, the redistribution process is sequentially executed on neighboring

nodes of the failed transmission node, while simultaneously calculating the real-time load of transmission nodes adjacent to the failed node. Taking v_s as an example, its communication load is updated after the load redistribution process as follows,

$$L_s(t+1) = L_s(t) + \Delta L_s(t). \quad (7)$$

Given that the load redistribution process alters the load distribution among neighboring nodes of the failed transmission node, it becomes imperative to re-evaluate the communication state of except for lost effectiveness nodes after each round of load redistribution.

As load redistribution occurs, the communication status of non-failed nodes needs to be re-evaluated after each round of redistribution. If the $L_s(t+1) \leq C_s$, it does not fail in that round. However, if the $L_s(t+1) > C_s$, the node fails in that round and triggers the next round of load redistribution. The cascading failures process continues until the communication load of all nodes remains below their respective communication capacities, indicating that no more nodes transition to the "ineffectiveness" state.

The main pseudo-code of the ROSE⁺ is provided in Algorithm 1. We briefly analyze the steps of the algorithm as well as the time complexity.

Algorithm 1: Robustness Optimization Security Scheme Against Cascading Failures Algorithm

```

1 for ( $i = 0; i < count(V); i++$ ) do
2   Calculate the initial communication load  $L_i(0)$  of
   the transmission nodes and define their
   communication capacity  $C_i(0)$  by Eq. (2) and (3);
3 end
4 Selection attack model based on LDDoS attack and
  get the selected node collection  $v_{selected}$ ;
5 for ( $i = 0; i < count(V); i++$ ) do
6   if ( $v_i == v_{selected} \&\& S_{v_{selected}}(t) ==$ 
    $ineffectiveness$ ) then
7     Mark the node as a failed node and add the
     node to the  $\Psi$ ;
8   end
9 end
10 for ( $i = 0; i < count(\Psi); i++$ ) do
11   for ( $j = 0; j < count(\Omega); j++$ ) do
12     Calculate the proportion of free capacity of the
     node  $Q_j(t)$ ;
13     Calculate the  $RTT_{ij}$  between the failed node
      $v_i$  and the neighbor's node  $v_j$ ;
14     Obtained  $\Delta L_j(t)$  according to Eq. (7);
15      $L_j(t+1) \leftarrow L_j(t) + \Delta L_j(t)$ ;
16     if ( $S_i(t)$  not  $ineffectiveness$ ) then
17       break;
18     end
19   end
20 end

```

Step 1: Initialize the communication load and capacity of each transmission node in the network. Based on the Motter-Lai model, define the $L_i(0)$ and $C_i(0)$ of each transmission node (line 2). The loop traverses all nodes V , executing $|V|$ times, and each execution computes $L_i(0)$ and $C_i(0)$ with time complexity $O(|V|)$.

Step 2: Identify the attack strategy and mark ineffectiveness nodes. The selection of the node subset v_{selected} is predicated on the LDDoS attack paradigm, encompassing both stochastic and targeted assault vectors. The complexity of this model is hypothesized to be $O(f(V))$ (line 4). Subsequently, an exhaustive traversal of the entire node ensemble V is conducted, ascertaining for each node v_i its inclusion in v_{selected} and its “ineffectiveness” status; affirmative findings result in the node’s inclusion in the set Ψ . Consequently, the temporal complexity for this procedure is expressed as $O(f(V)) + O(|V|)$.

Step 3: Update the communication load distributions for nodes that have lost effectiveness and their immediate neighbors. The outer loop iterates over the set of ineffectiveness nodes Ψ , executing $|\Psi|$ times (line 10). For each node exhibiting ineffectiveness, a reallocation of load is necessitated, directing the node’s load to its adjacent transmission nodes. This is achieved through the inner loop, which navigates the set of neighboring nodes Ω of the failed node, executing $|\Omega|$ times. The real-time update of the network’s communication state is facilitated by calculating $Q_j(t)$ and RTT_{ij} , thereby ensuring the integrity of network communication (lines 12-15). The computational operations for these updates are constant in time $O(1)$, rendering the overall time complexity of the process to be $O(|\Psi| \cdot |\Omega|)$.

To summarize, the cardinalities $|\Psi|$ and $|\Omega|$ are both functions of $|V|$. In the extreme scenario, where all nodes’ neighbors are traversed, then $|\Psi| \approx |V|$ and $|\Omega| \approx |V|$. Consequently, the aggregate complexity is approximated by $O(f(V)) + O(|V|^2)$, with $|V|^2$ typically being the predominant term. Hence, the algorithm’s overall complexity is $O(|V|^2)$ in the worst-case scenario.

III. SIMULATION RESULTS AND DISCUSSION

A. Simulation Setup

To validate the rationale and efficacy of the multipath TCP robustness analysis model against cascading failures, a cascading failures scenario under LDDoS attack in multipath TCP transmission is constructed within the NS-2 simulation platform [13], depicted in Fig. 2. In this scenario, the multipath TCP receiver is positioned adjacent to the “last-hop” wireless link, while the multipath TCP transmitter is tethered to the backbone network.

To simulate the multipath TCP paths under the LDDoS attack, a constant bit rate (CBR) traffic generator is affixed to a randomly selected path, facilitating the transmission of UDP traffic to its corresponding node (the respective sink). Additionally, to emulate high-frequency burst frame loss at the data link layer, both the Uniform Path Loss (UPL) model and the Markov Loss (ML) model are incorporated into each

wireless access link of the multipath TCP system. The UPL and ML models serve to encapsulate the distributed loss attributed to wireless noise interference and the sporadic, persistent loss stemming from wireless signal fading, respectively. The experimental simulation spans 100 seconds, with detailed configuration parameters outlined in Table II.

TABLE II
EXPERIMENTAL SETTINGS

Parameter	Value	Parameter	Value
Package Size	1500Bytes	LDDoS Rate	2.5Mbps
Markov Loss Rate	1%	Uniform Loss Rate	1%
CBR generator Numbers	10	Queue Type	DropTail
center bandwidth	100Mbps	center delay	30ms
edge bandwidth	5/10Mbps	edge delay	10-60ms
α	0.2	β	1

B. Simulation Results and Analysis

1) *Throughput and Robustness:* As depicted in Fig. 3, we compare the throughput data under normal conditions (non-cascading failures) with those under selective attacks (cascading failures). Under normal circumstances, the average throughput reaches 98.09 Mbps. However, following the LDDoS selective attack, the multipath TCP throughput experiences a significant decline, with the average throughput plummeting to 79.27 Mbps, adversely impacting the normal communication of the transmission system. After conducting 50 rounds of random sampling and averaging the experimental results, the probability of cascading failure in the multipath TCP transmission system was determined to be 53.17%.

Fig. 4 illustrates a comparison of throughput trends before and after the optimization of the robust model in the case of cascading failures (selective attacks). It is evident from the figure that, compared to the selective attack scenario, the overall throughput has been somewhat improved, with the average throughput reaching 80.60 Mbps. However, due to the influence of the attack, the overall variance of the throughput remains relatively high, underscoring the potential for further enhancement through the load redistribution optimization method. Based on the multipath TCP robustness analysis model, the load redistribution method within the aforementioned load-capacity cascading failures model is refined to enhance the robustness and resilience of the multipath transmission system. After 50 rounds of random sampling and averaging the experimental results, the multipath TCP cascading failure probability was reduced to 33.10%. The inclusion of the node idle capacity ratio in the design of the load redistribution scheme leads to a decrease in node load compared to the selective attack scenario. Experimental findings demonstrate a reduction in the probability of cascading failures by 20.07%, affirming the correctness and robustness of our approach.

2) *Out-of-Order Data Sequence Number:* Out-of-Order Data Sequence Number (DSN) is a valuable metric that effectively assesses and elucidates the performance of multipath

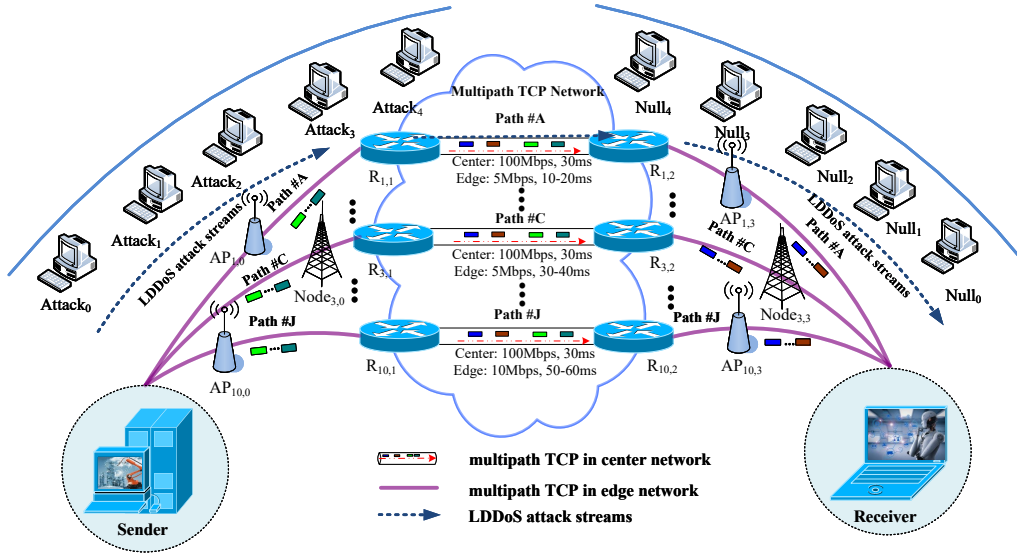


Fig. 2. Diagram of Topology.

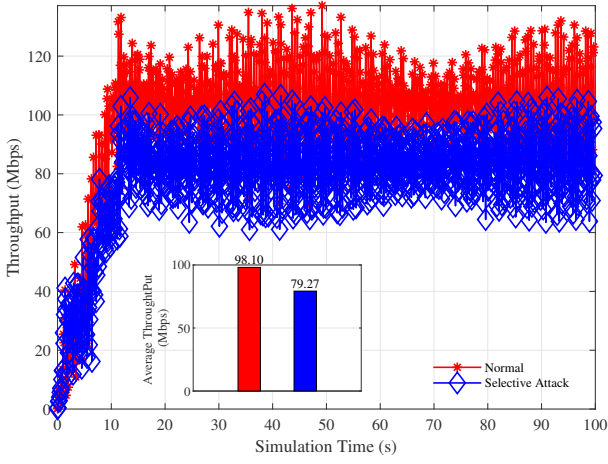


Fig. 3. Diagram of multipath TCP throughput comparison before and after attack.

protocols. Out-of-Order DSN can be obtained by an offset between DSNs of two continuously received multipath TCP data.

Fig. 5 illustrates a comparison of the trends in Out-of-Order DSN before and after implementing the optimized robustness model, particularly in cases of cascading failures resulting from selective attacks. The optimized ROSE⁺ exhibits a decreased occurrence of Out-of-Order DSN when compared to the robustness analysis model. This improvement indicates that the load redistribution scheme has been optimized to minimize the average delay during multipath transmission, thereby enhancing the overall performance of the transmission system.

The reduction in DSN indicates a more orderly and reliable packet delivery process. It suggests that the ROSE⁺ effectively maintains the integrity and order of transmitted data, miti-

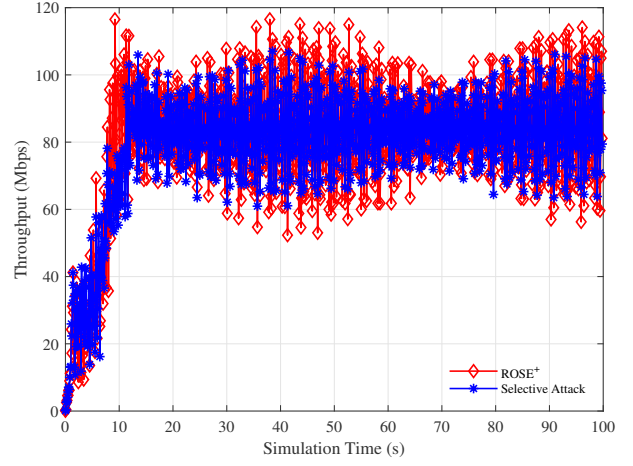


Fig. 4. Diagram of multipath TCP throughput comparison selective attack and after optimization.

gating issues such as lost, duplicated, or corrupted packets. The improved reliability in packet delivery contributes to enhanced transmission efficiency and dependability, resulting in an overall boost to the performance of the multipath TCP transmission system.

3) *Jitter*: Fig. 6 illustrates the comparison of jitter trends before and after optimizing the robustness model in the scenario of cascading failures resulting from selective attacks. The observations reveal that the ROSE⁺ demonstrates higher jitter values during 30s periods when compared to the selective attack. However, it is known through the calculation that the standard deviation of the selective attack is 2.8898e-04 and the standard deviation of the ROSE⁺ is 2.8663e-04, which has a smaller standard deviation.

This phenomenon may arise due to the frequent occurrence of jitter when selecting a new transmission path based on

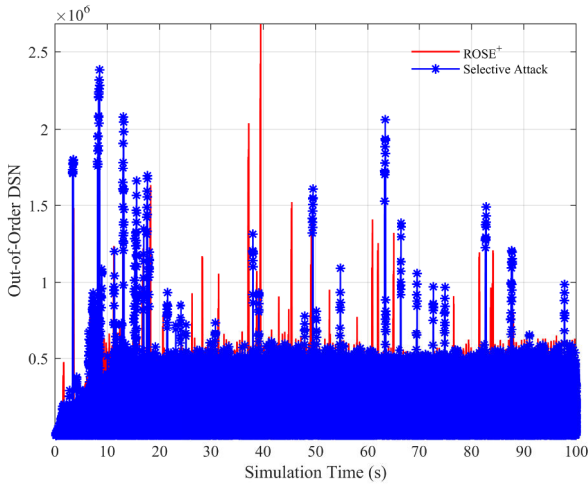


Fig. 5. Diagram of the multipath TCP Out-of-Order DSN comparison selective attack and after optimization.

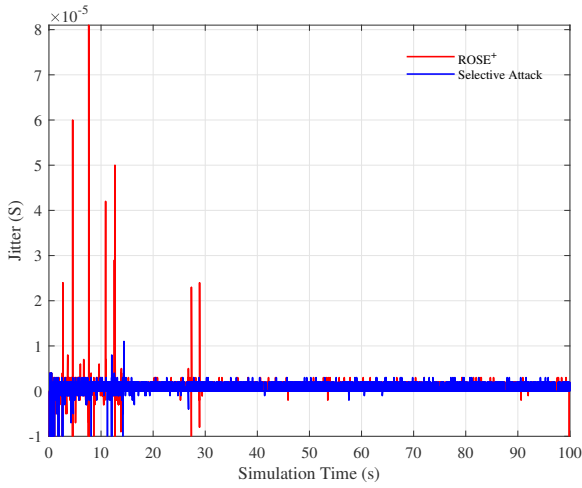


Fig. 6. Diagram of the multipath TCP jitter comparison before and after optimization.

the “load redistribution” of the ratio of idle capacity, thereby increasing the jitter rate. However, as time advances, ROSE⁺ showcases its adaptability and responsiveness by promptly adjusting to the evolving network conditions. It successfully overcomes the initial instability and gradually achieves stabilization. It is important to note that while the ROSE⁺ may exhibit higher jitter values, it is within tolerable limits. It is essential to carefully weigh the trade-off between increased jitter and the benefits of enhanced load balancing and robustness to ensure the desired transmission performance.

IV. CONCLUSION AND FUTURE WORK

The cascading failures phenomenon has a significant impact on multipath TCP transmission. To address this issue, the ROSE⁺ scheme is developed, aiming to enhance the robustness and stability of the multipath TCP transmission in

the presence of cascading failures. The experimental results demonstrate that the ROSE⁺ scheme, based on the load-capacity cascading failures model, effectively measures the robustness and stability of the multipath TCP. Moreover, it reduces the probability of cascading failures by 20.07%, thus enhancing the reliability and robustness of multipath TCP transmission to a certain extent.

In future research, the ROSE⁺ solution should be developed with an “intelligent” approach by incorporating emerging technologies like machine learning and deep learning [14]. Also, realize real-time dynamic monitoring and defense of abnormal traffic, reduce the occurrence of anomalous traffic leakage and false positives of network attacks, etc.

ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China under Grant No. 61962026 and in part by the Natural Science Foundation of Jiangxi Province under Grant No. 20224ACB202007.

REFERENCES

- [1] J. Postel. Transmission Control Protocol. Technical report, sep. 1981.
- [2] J. Su, X. Bai, and K. Zhou, “Analysis and Comparison of Delay Tolerant Network Security Issues and Solutions,” in Proc. of 2023 IEEE 22nd International Conference on Trust, Security, and Privacy in Computing and Communications (TrustCom), Exeter, United Kingdom, pp. 1512-1517, 2023.
- [3] T. Sommestad, H. Holm and M. Ekstedt, “Estimates of Success Rates of Denial-of-Service Attacks,” in Proc. of 2011 IEEE 10th International Conference on Trust, Security, and Privacy in Computing and Communications (TrustCom), Changsha, China, pp. 21-28, 2011.
- [4] K. Chen, H. Wang, and P. Hong, “A Defense Strategy Against LDDoS Attack Aggregation in DCN,” in Proc. of IEEE International Conference on Communications (ICC), Rome, Italy, pp. 797-802, 2023.
- [5] A. Ford, C. Raiciu, M. Handley, O. Bonaventure, “TCP Extensions for Multipath Operation with Multiple Addresses,” RFC 6824, IETF, Jan. 2013.
- [6] K. Wong, C. Wong, and H. Lao, “Mitigation and recovery of cascading failures in scale-free networks,” in Proc. of IET International Conference on Information and Communications Technologies (IETICT), Beijing, China, 2013.
- [7] J. Han et al., “Leveraging Coupled BBR and Adaptive Packet Scheduling to Boost MPTCP,” IEEE Transactions on Wireless Communications, vol. 20, no. 11, pp. 7555-7567, Nov. 2021.
- [8] Y. Xing et al., “A Low-Latency MPTCP Scheduler for Live Video Streaming in Mobile Networks,” IEEE Transactions on Wireless Communications, vol. 20, no. 11, pp. 7230-7242, Nov. 2021.
- [9] J. Wu, B. Cheng, M. Wang and J. Chen, “Quality-Aware Energy Optimization in Wireless Video Communication With Multipath TCP,” IEEE/ACM Transactions on Networking, vol. 25, no. 5, pp. 2701-2718, Oct. 2017.
- [10] Y. Thomas, M. Karaliopoulos, G. Xylomenos and G. C. Polyzos, “Low Latency Friendliness for Multipath TCP,” IEEE/ACM Transactions on Networking, vol. 28, no. 1, pp. 248-261, Feb. 2020.
- [11] Y. Cao, R. Ji, L. Ji, X. Shao, G. Lei, and H. Wang, “MPTCP-meLearning: A Multi-Expert Learning-based MPTCP Extension to Enhance Multipathing Robustness Against Network Attacks,” IEICE Transactions on Information and Systems, vol.E104-D, no.11, 2021.
- [12] S. Kai, H. Yunhe, S. Wei, et al. Modeling of Cascading Failures. Power System Control Under Cascading Failures: Understanding, Mitigation, and System Restoration. IEEE, 2019.
- [13] UC Berkeley. LBL, USC/ISI, and Xerox Parc, NS-2 documentation and software, version 2.35.
- [14] B. He et al., “Learning-Based Real-Time Transmission Control for Multi-Path TCP Networks,” IEEE Transactions on Cognitive Communications and Networking, vol. 9, no. 5, pp. 1353-1369, Oct. 2023.



DSPACE

<https://dspace.org/>

ROSE+ : A robustness-optimized security scheme against cascading failures in multipath TCP under LDDoS attack streams

Nie, Jinqun; Ji, Lejun; Jiang, Yirui; Ma, Young; Cao, Yuanlong

2024-12-17

IEEE

<https://doi.org/10.1109/trustcom63139.2024.00254>

Nie J, Ji L, Jiang Y, et al., (2024) ROSE+ : A robustness-optimized security scheme against cascading failures in multipath TCP under LDDoS attack streams. In: 2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 17-21 December 2024, Sanya, China