Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 2264187, 10 pages
https://doi.org/10.1155/2021/2264187

Research Article

Extracting Low-Rate DDoS Attack Characteristics: The Case of Multipath TCP-Based Communication Networks

Gang Lei,[1] **Lejun Ji**,[1] **Ruiwen Ji**,[1] **Yuanlong Cao**,[1] **Xun Shao**,[2] **and Xin Huang**[1]

[1] *School of Software, Jiangxi Normal University, Nanchang 330022, China*
[2] *School of Regional Innovation and Social Design Engineering, Kitami Institute of Technology, Japan*

Correspondence should be addressed to Yuanlong Cao; ylcao@jxnu.edu.cn

Received 25 April 2021; Accepted 26 June 2021; Published 8 July 2021

Academic Editor: Longzhe Han

The multipath TCP (MPTCP) enables multihomed mobile devices to realize multipath parallel transmission, which greatly improves the transmission performance of the mobile communication network. With the rapid development of all kinds of emerging technologies, network attacks have shown a trend of development with many types and rapid updates. Among them, low-rate distributed denial of service (LDDoS) attacks are considered to be one of the most threatening issues in the field of network security. In view of the current research status, by using the network simulation software NS2, this paper first compares and analyzes the throughput and delay performance of the MPTCP transmission system under LDDoS attacks and, further, conducts simulation experiments and analysis on the queue occupancy rate of the LDDoS attack flow to extract the basic attack characteristics of the LDDoS attacks. The experimental results show that the LDDoS attacks will have a major destructive effect on the throughput performance and delay performance of the MPTCP transmission system, resulting in a decrease in the robustness of the transmission system. By analyzing and comparing the occupancy rate of the LDDoS attack flow in the MPTCP transmission system, it can be concluded that (1) the occupancy rate of the LDDoS scattered pulse traffic sent by each puppet machine changes slightly, and (2) the occupancy rate of LDDoS attack data flow is much greater than that of ordinary TCP data flow.

1. Introduction

With the continuous innovation and development of the new generation of Internet technology, a variety of wireless network technologies have been deployed and applied on a large scale. In order to improve the transmission performance of the mobile communication network and provide better network services, more and more mobile devices have a variety of different standards of the network interface. Multihomed mobile devices can use multipath transmission technology in the transmission system to realize multipath parallel transmission, so as to achieve effective use of bandwidth resources, increase transmission rate, and balance network load [1]. In recent years, the Internet Engineering Task Force (IETF) has proposed several transmission protocols to support multihomed connections. Among them, the multipath TCP (MPTCP) is one of the most representative achievements in the research of current multipath transmission technology [2]. As a transport layer protocol supporting multipath data transmission, MPTCP retains the stability and reliability of the traditional TCP. It can maintain backward compatibility with existing Internet devices and greatly improve the transmission quality of the transmission system [3, 4]. Therefore, MPTCP has become a hot issue studied by many academic workers and has broad application prospects in the development of the Internet in the future.

Although the MPTCP transmission system can improve system performance by implementing multipath data parallel transmission, with the increasing number of network attacks, the MPTCP transmission system will reduce the robustness of the system and the quality of user experience due to deliberate network attacks. For the MPTCP transmission system, it can distribute data through multiple paths in a single connection [5]. This transmission mechanism also brings certain security issues while alleviating the problem of bandwidth resource tension. When one of the transmission paths suffers a network attack, the degradation of the path's transmission performance will have a negative impact on the robustness and antidestroying ability of the entire transmission system [6]. Therefore, it is extremely important to study the security of the multipath transmission system based on MPTCP.

With the rapid development of the Internet, various types of network attacks are increasing day by day, and network security issues have penetrated into all aspects of our social life. A large number of experimental studies have shown that among the numerous network attacks, low-rate distributed denial of service (LDDoS) has become one of the most threatening problems in the field of network security [7]. The LDDoS attack uses the timeout retransmission mechanism of the TCP to periodically send short pulse attacks to the attack target through multiple puppet machines, causing the transmission system to continue to be in a timeout retransmission state [8]. So the transmission system cannot respond to normal requests from legitimate users, thus achieving the purpose of the attack [9]. One of the biggest characteristics of LDDoS attacks is that the attacker only needs to use fewer attack data packets to cause large-scale and long-term network paralysis, which greatly reduces the throughput of the attacked object. In the MPTCP multipath transmission system, LDDoS attacks are easier to evade detections because of their low transmission rate and strong concealment [10, 11]. Thus, the robustness of the system reduces and the transmission performance of the transmission system is seriously affected. Therefore, studying the attack characteristics and detection methods of LDDoS attacks in the MPTCP transmission system will become a hot topic in the future.

The current academic research is mainly aimed at the transmission system based on the TCP to extract the attack flow characteristics, thereby improving the ability to detect and defend against LDDoS attacks. In view of the current research status, the paper mainly studies the attack characteristics of LDDoS attack flow in the transmission system based on MPTCP and improves the detection and defense capabilities of the transmission system based on MPTCP to LDDoS attack. Through the NS2 (Network Simulator version 2) network simulation software [12], in the transmission network based on MPTCP, we study the changes in the throughput and delay performance of the transmission system under LDDoS attacks, compare the share of normal data flow or attack data flow sent by different edge nodes in the transmission link under LDDoS attacks, and observe and analyze the basic characteristics of LDDoS attack flow in the MPTCP transmission network. The research results of this paper are at the basic stage of feature mining of LDDos attacks, enriching the related research on MPTCP robustness and LDDoS attacks, and providing ideas for the research of LDDoS detection and defense methods.

The rest of this paper is organized as follows. The second part introduces the research results in related fields of LDDoS detection and defense. The third part mainly introduces the simulation experiment design and the analysis of the experimental results and draws the experimental conclusions. The last part is the summary and outlook.

2. Related Work

In recent years, various network attacks have shown a significant growth trend due to the development of emerging information technologies such as the Internet of Things, especially LDDoS attacks [13]. The average rate of LDDoS attack data flow is low and very similar to normal traffic, which can be completely hidden in normal background traffic and is not easily noticed. Because LDDoS attacks are more efficient and more harmful, it is difficult to be discovered by traditional DDoS/LDDoS attack defense systems, resulting in a rapid decline in network quality [14]. Currently, many networks do not have effective mechanisms to deal with threats from LDDoS attacks. LDDoS presents a typical and extremely destructive threat to the network environment. How to accurately detect LDDoS attack flow has become a research hotspot in the field of network security at home and abroad.

Due to the distributed nature of LDDoS and the methods used by attackers to forge, randomly change the source IP address of the message, and randomly change the content of the attack message, it is difficult to extract the attack characteristics and the location of the attack source. The existing detection and defense methods use abnormal characteristics of the network and traffic to perform detection and defense indirectly. In the existing research literature, there are many filtering methods and metrics for LDDoS attacks. Simsek et al. [15] proposed an ipdv-based LDDoS filtering method using average Internet protocol packet delay variation (mipdv). Cheng et al. [16] proposed an abnormal network traffic feature sequence prediction method to detect DDoS attacks in a big data environment. Sahoo et al. [17] proposed a general entropy- (GE-) based metric to detect low-rate DDoS attacks on the control layer. Behal and Kumar [18] are based on information theory's general entropy (GE) and general information distance (GID) indicators to detect DDoS attacks. Yue et al. [19] proposed a feedback control model to describe the process of congestion control and combined the congestion window and queue behavior for analysis. They designed a two-dimensional queue distribution model consisting of an instantaneous queue and an average queue to extract attack characteristics.

Recently, in order to improve detection accuracy, many scholars merge multiple characteristics of network traffic to perform detection. Liu et al. [20] used the features extracted from the network traffic and proposed a new detection method based on multifeature fusion to solve this problem. The attack feature set containing the acknowledgment character (ACK) sequence number, packet size, and queue length can be used to detect LDDoS attack flow. Experiments have proved that the detection rate of the multifeature fusion algorithm is higher than that of the single-feature detection method and other algorithms. In addition, more and more researchers apply machine learning methods to detect complex LDDoS attacks and improve the efficiency and robustness of intrusion detection systems. Wu et al. [21]

proposed a multifeature DDoS attack detection method based on a factorization machine (FM) machine learning algorithm to improve the detection accuracy of low-rate DDoS attacks on the SDN data layer. Tang et al. [22] proposed an LDDoS attack detection method based on multiple characteristics of network traffic. This method uses the Adaboost classification algorithm in the machine learning field to effectively identify LDDoS attack flow. Tang et al. [23] proposed an LDDoS attack detection method based on multifeature fusion and Convolutional Neural Network (CNN) by calculating various network features and fusing them into feature maps. Siracusano et al. [24] proposed an LDDoS attack detection method based on malicious TCP flow characteristics. The authors conducted experiments using six supervised AI algorithms to classify attacks from legitimate streams, proving the potential of AI in LDDoS detection. Liu et al. [25] researched and developed a new semisupervised locally sensitive incremental conduction support vector machine (LS-ITSVM) method, which can identify abnormal network traffic such as LDDoS, and has high detection accuracy. Zhang et al. [26] proposed a detection algorithm combining power spectral density (PSD) entropy function and support vector machine, which can detect LDDoS traffic from normal traffic. In order to minimize the computational cost and find only the most relevant patterns for detection, machine learning models based on support vector machines are used to learn traffic patterns and select appropriate features for detection algorithms.

By tracking the detection and defense research of LDDoS in recent years, we find that in the network based on the TCP protocol, the detection and defense methods of LDDoS have achieved some results. However, more and more networks now use advanced MPTCP technology, and multihomed mobile devices can increase their throughput by distributing application data on multiple paths at the same time. At the same time, attacks on MPTCP networks have also increased. When a MPTCP connection is attacked by a network and becomes a poorly performing path or a broken path, it may seriously affect other stable paths, and without a relevant solution, MPTCP will undoubtedly suffer severe performance degradation. Cao et al. [27] proposed an LDDoS attack energy-saving MPTCP solution called MPTCP-La/E-2, aiming to avoid cloud multipath performance degradation transmission caused by LDDoS, which is rarely considered in existing MPTCP solutions. Therefore, in MPTCP-based network, the related researches of LDDoS attack are still in the primary stage, and the basic work of its feature mining still needs to be explored in depth.

Based on the current research results obtained by academic workers, in this paper, we analyze and compare the MPTCP transmission system's throughput performance and delay performance when subjected to LDDoS attacks. At the same time, through simulation experiments and analysis of the queue occupancy rate of the LDDoS attack flow, we extract attack characteristics of LDDoS attacks. This paper enriches the related research on MPTCP robustness and LDDoS attacks and provides research methods for the detection and defense of LDDoS attacks in multipath transmission systems.

3. Experimental Design and Analysis

3.1. Experimental Design. In order to study the performance of MPTCP under LDDoS attack, and to extract the attack characteristics of LDDoS attack in the multipath transmission system based on MPTCP, this experimental study uses a network simulation software NS2 which is widely used in the academic circles to carry out network simulation experiment. We design a "symmetric" network simulation topology on the network simulation platform, which is also widely used in real life [28], as shown in Figure 1. For example, two MPTCP-based mobile devices in the same area use the same router to communicate with the corresponding server at the same time. When the router is subjected to certain types of attacks, both communication paths will be affected to varying degrees.

In this information transmission network, two senders (Sender 1, Sender 2) adopt the MPTCP protocol and send TCP data streams. The two data streams converge on the bottleneck router R_0 through link A and link B. After being forwarded, they are received by the data receivers (Receiver 1, Receiver 2) accordingly. The bandwidth between the two senders and the router R_0 and the two receivers and the router R_1 is set to 2 Mb, and the transmission delay time is set to 25 ms. The bottleneck bandwidth of the link between R_0 and R_1 is set to 4 Mb, and the transmission delay time is set to 25 ms. All links use the Drop-Tail algorithm [29]. In addition, in order to simulate the LDDoS attack effect, R_0 is connected to four edge nodes that send UDP attack flow, and R_1 is connected to four edge nodes that receive UDP attack flow. The bandwidth between each edge node and its connected router is set to 1 Mb, and the transmission delay time is set to 25 ms.

In order to achieve the better attack effect, LDDoS attacks use the more commonly used CBR/UDP data stream with a fixed transmission rate, that is, all attackers will send CBR/UDP data packets [27]. We set the size of the data packet to 1444 and the transmission rate to 1 Mbps. In addition, LDDoS attacks have three basic attack characteristics, which can be expressed by the following expressions,

$$\mathrm{LDDoS}(P, D, R) = \mathrm{LDDoS}(100\mathrm{ms}, 100\mathrm{ms}, 1\mathrm{Mbps}). \tag{1}$$

The specific description is that the attack period of the LDDoS attack is set to 100 ms, the attack duration is 100 ms, and the attack rate is 1 Mbps. The attack flow starts to be sent at 1.0 s, and the total simulation time is 60 s.

We can achieve effective attacks by reasonably setting and adjusting the parameter values of P, D, and R. An effective and successful LDDoS attack can force the normal data flow to enter the slow start phase. At this time, the value of the congestion window (cwnd) is reduced to the size of 1 data packet. As the sent message segments are continuously confirmed, cwnd becomes exponential grade growth [13]. When cwnd exceeds the value of the slow start threshold (ssthresh) state variable, the slow start phase ends and the congestion avoidance phase is entered. In the congestion avoidance phase, the value of the cwnd slowly increases according to a linear law, and the value of cwnd increases by 1 every time

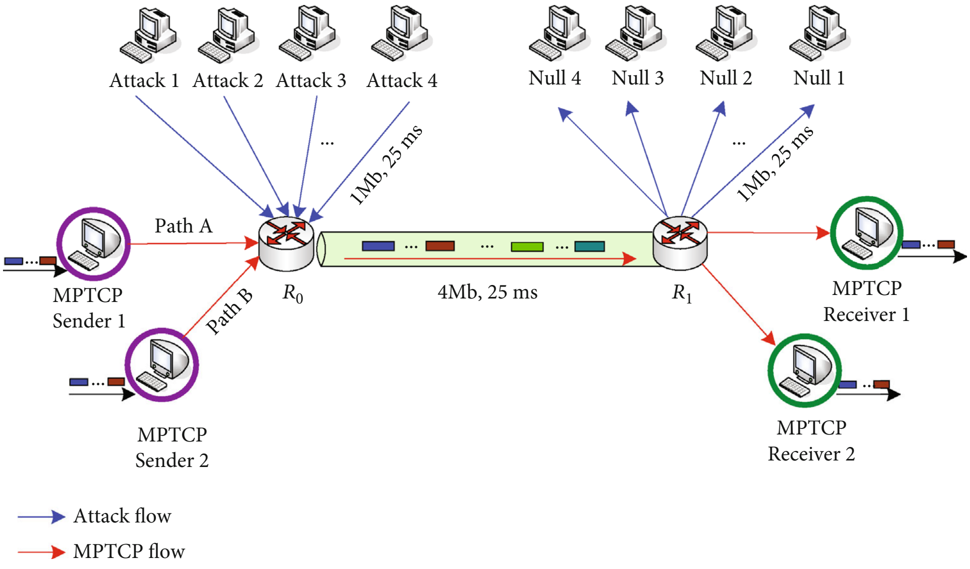

Figure 1: A basic "symmetric" simulation topology with LDDoS attacks.

a round-trip time RTT passes. When the data packet is lost due to network congestion timeout, the transmission system enters the fast retransmission phase, then enters the fast recovery phase, updates the value of ssthresh to half of cwnd, and updates the value of the cwnd to 1, which is the initial congestion window size, and then start to execute the congestion avoidance algorithm [30].

After the above parameter settings, we can get the best LDDoS attack flow in this experiment. Figure 2 shows the changes in the cwnd of the network transmission system after being attacked by LDDoS. After suffering the LDDoS attack, the network begins to appear congested, and the value of the cwnd dropped sharply. With the enhancement of the attack effect, after 20 s, the size of the cwnd remains at about 1, causing the MPTCP sender to be in a timeout retransmission state and unable to exit, resulting in the best attack effect.

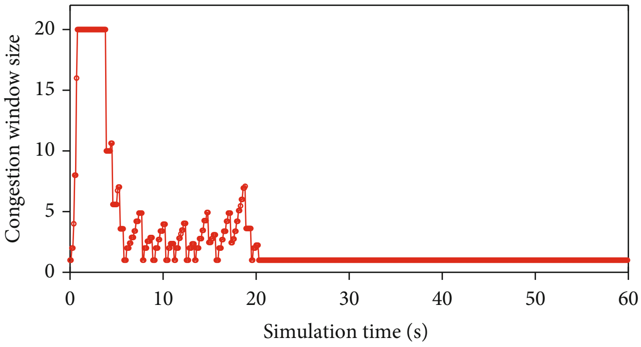

Figure 2: The congestion window size of the transmission system with the LDDoS attack.

3.2. Experimental Analysis

3.2.1. Performance Analysis. The experiment part mainly compares the transmission ability of the transmission system based on MPTCP to transmit packets under normal conditions and LDDoS attack. The experiment mainly analyzes and compares two performance evaluation indicators, throughput performance and end-to-end delay time performance.

The throughput is the amount of data successfully transmitted in a network unit time, which can be calculated by the following equation:

$$\text{throughput} = \frac{\text{packet\_sum} \times 8/10^6}{\text{interval}}. \tag{2}$$

Here, the *interval* is set to 0.1 s, which means that we calculate the throughput of the transmission system every 0.1 s. The *packet_sum* is the size of the data packet successfully received within the interval. The throughput unit is set to Mbps. The end-to-end delay time refers to the time required for a message or packet to be transmitted from one end of the network to the other end [31]. In the entire transmission system, each data packet has a unique packet id. We need to identify the *send time* and *receive time* of the data packet with the same packet id. The calculation equation is

$$\text{delay} = \text{receive\_time} - \text{send\_ time}. \tag{3}$$

(1) Throughput Performance Comparison. In order to observe the impact of the LDDoS attack on the MPTCP transmission system more intuitively, we evaluated the throughput performance of the transmission system, respectively, from the sender to the receiver of the entire transmission system throughput performance, Sender 1 for sending the path A throughput performance and Sender 2 for sending the path B throughput performance.

Figure 3 shows the throughput of the transmission system when it has not suffered the LDDoS attack. It can be seen from the figure that when the transmission system is

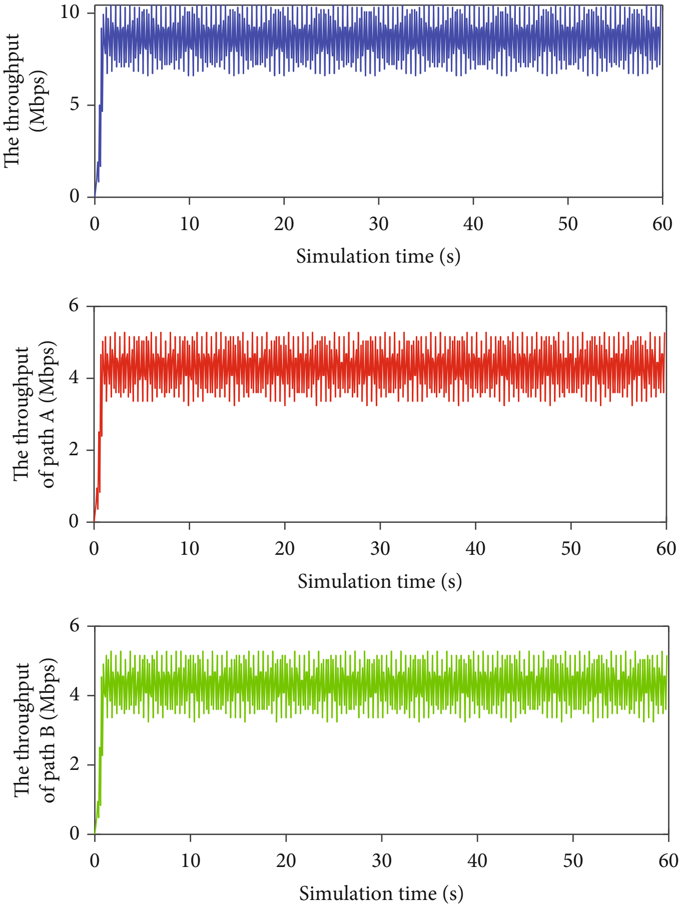

FIGURE 3: The throughput performance of the transmission system without LDDoS attacks.

not attacked by LDDoS, the TCP data flow sent by the sender can be transmitted normally. The throughput gradually increases from 0. This is because every time a TCP data packet is successfully sent, the cwnd value will continue to increase, and the throughput will increase until the maximum bandwidth capacity is reached. The throughput change trends of path A and path B are roughly the same. The throughput of the entire transmission system is the sum of the throughput of path A and path B. The simulation result is also consistent with the actual situation.

Figures 4–6, respectively, show the throughput of the entire transmission system, path A, and path B when subjected to the LDDoS attack. It can be seen from the figures that the throughput of the entire transmission system, path A, and path B has significantly decreased compared with not suffering from the LDDoS attack, especially after about 5 s, the throughput gradually approaches 0 until equal to 0. In addition, the throughput change trends of path A and path B are inconsistent. The throughput of path B becomes 0 after about 5 s, indicating that path B has been completely occupied by the attack flow packets, resulting in the failure to send TCP data packets. Although the throughput of path A gradually becomes 0 after about 5 s, it will fluctuate to a certain extent within about 20 s to 25 s. This shows that the transmission performance of path A is better than that of path B after being attacked by the LDDoS. The change in throughput of the entire transmission system is basically the same as that of path A after about 5 s, which confirms the operating mechanism of the MPTCP protocol. When the network's own link fails randomly or is attacked by external network attacks, the MPTCP protocol stipulates that the path with better transmission performance should be selected for transmission when sending data packets, which can effectively avoid causing the network congestion and affect the transmission performance of the transmission system [32]. At the same time, this also reflects the design principle of the MPTCP protocol congestion avoidance algorithm, whose throughput must reach the throughput of the best-performing path among all the paths of the transmission system [33].

Through the comparison of the above simulation experiment results, we can clearly see that the LDDoS attack will have a great impact on the throughput performance of the MPTCP transmission system. With the extension of the attack time, the throughput of the normal data flow will gradually drop to 0 and will be maintained. That is to say, the transmission path is completely occupied by the attack flow data packets, resulting in the

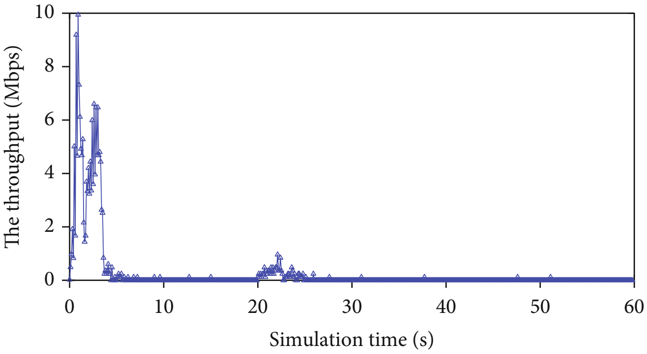

Figure 4: The throughput performance of the transmission system with LDDoS attacks.

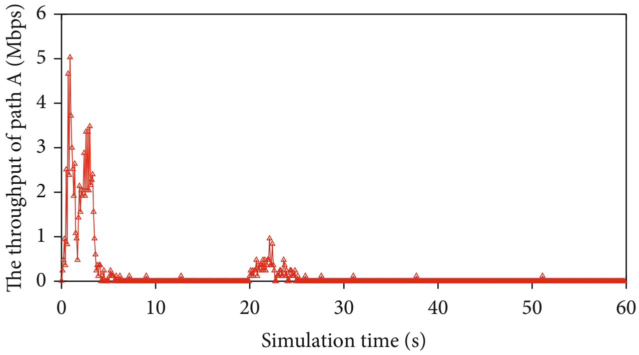

Figure 5: The throughput performance of Path A with LDDoS attacks.

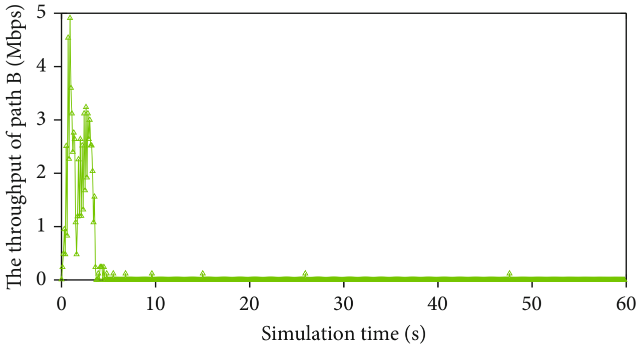

Figure 6: The throughput performance of Path B with LDDoS attacks.

failure to send TCP data packets normally, which seriously affects the robustness of the transmission system.

(2) End-to-End Delay Performance Comparison. In order to further study the impact of LDDoS attacks on the MPTCP-based transmission system, based on the above comparison and analysis of the throughput performance, we analyze the delay performance of the transmission system, including the delay performance of the entire transmission system from the sender to the receiver, the delay performance of path A, and the delay performance of path B.

Figure 7 shows the change trend of the delay performance of the transmission system when it is not attacked by LDDoS. We can see from the figure that the delay performance change of the entire transmission system is basically the same as the delay performance change of path A and path B. The range of change and the trend of change basically coincide, except for the initial small fluctuations. In addition, after about 1 s, the delay will remain stable at about 0.09 s.

Figure 8 shows the change trend graph of the delay performance of the transmission system when it is subjected to the LDDoS attack. We can see from the figure that both the path A and path B have a large delay variation. It is worth noting that the delay variation curve of path A disappears after about 24.6 s, and the delay variation curve of path B disappears after about 4.2 s, which indicates that there is no normal TCP data flow on path A after about 24.6 s, and there is no normal TCP data flow on path B after about 4.2 s, indicating that the two paths have been completely occupied by the LDDoS attack flow, which is consistent with the throughput performance of the transmission system. In addition, we can also see from the figure that the delay curve of the entire transmission system is roughly the same as the delay curve of the path A. This feature is in line with the MPTCP protocol congestion control design principle. When the transmission system is congested, the path with the best transmission performance should be selected for data flow transmission to ensure the transmission performance of the transmission system as much as possible.

Through the analysis of the above simulation experiment results, we can conclude that the average delay of the entire transmission system when subjected to the LDDoS attack is approximately 0.15 s, which is about 0.06 s higher than the average delay when not subjected to the LDDoS attack. In addition, when subjected to LDDoS attacks, the transmission time of the TCP data flow is greatly shortened, which seriously affects the normal transmission of data and the normal use of the transmission system.

This part of the experiment mainly compares the throughput performance and delay performance of the MPTCP-based multipath transmission system under the two conditions of LDDoS attacks and no LDDoS attacks. From it, we can clearly see that the LDDoS attack has

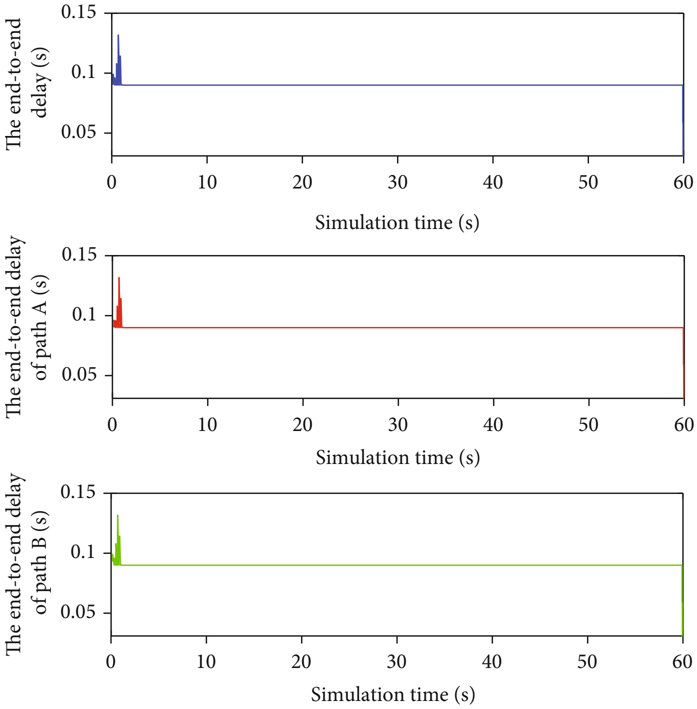

Figure 7: The end-to-end delay performance of the transmission system without LDDoS attacks.

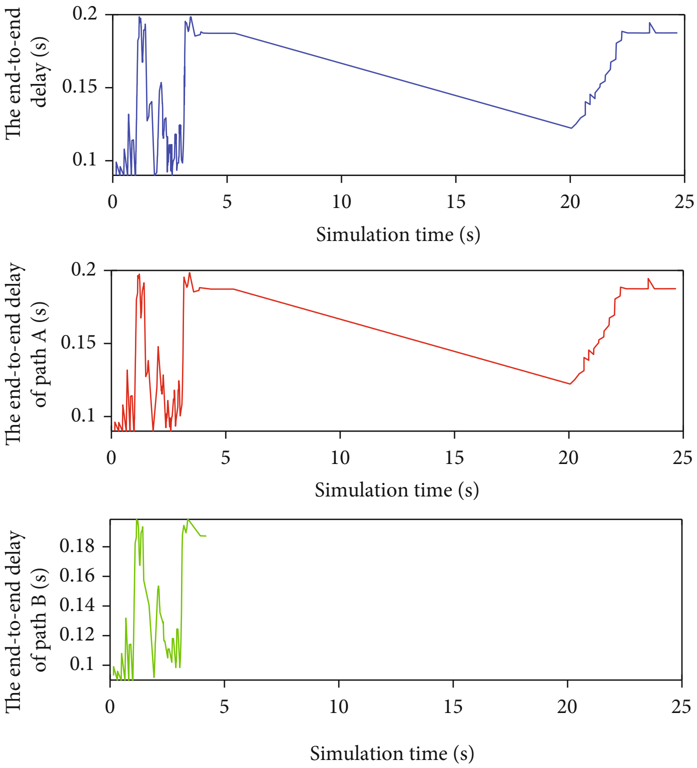

Figure 8: The end-to-end delay performance of the transmission system with LDDoS attacks.

an extremely serious destructive impact on the multipath transmission system. In the transmission network based on MPTCP, LDDoS attacks make the transmission system lose its ability to respond to normal user requests, and the TCP data flow cannot be transmitted normally, and the throughput approaches 0 or even disappears, which leads to the decline of the robustness of the multipath transmission system and fails to meet the user's demands for data transmission performance and quality of service [34]. Therefore, studying and realizing the feature extraction of the LDDoS attack flow in multipath transmission systems has become particularly urgent and important. At the same time, it also provides necessary prerequisites for the detection and defense of LDDoS attacks.

3.2.2. Feature Extraction Analysis. In order to study the behavioral characteristics of LDDoS attacks in the multipath transmission system based on the MPTCP protocol, we conduct a further specific analysis on this multipath transmission system. In this experimental part, we attack the multipath transmission system according to the optimal attack parameters set in the previous experiment design, that is, the attack period of the LDDoS attack is 100 ms, the attack duration is 100 ms, and the attack rate is 1 Mbps. We study the changes in the queue occupancy of the normal data flow and the attack flow during the attack process. So the feature extraction of LDDoS attack flow in a multipath transmission system is realized, which lays an important foundation for the detection and defense of the LDDoS attack.

In order to facilitate the understanding of the experimental data, we simplified the network topology, as shown in Figure 9. As set up in the previous experimental design part, the network topology includes two MPTCP source ends (nodes 1, 3) sending FTP/TCP data streams and four LDDoS source ends (nodes 10, 11, 12, 13) sending CBR/UDP data streams. A total of six data streams are converged to the bottleneck route R_0 (node 8), and data is forwarded via this. During the simulation running time of this transmission system, we record the queue occupancy rate of the data flow every 5 s from 0 s, that is, the proportion of the data flow successfully sent by this node in the total data flow successfully sent by the six source nodes in this period [35], the calculation equation is

$$\text{occupancy rate} = \frac{\text{throughput\_node}[k]}{\sum_i \text{throughput\_node}[i]} \times 100\%, \qquad (4)$$

where *throughput_node*$[k]$ is the throughput of the sender labeled k, and the value of i is the node label of all senders. Then, we draw the simulation results of the operation into a data flow statistical table and, then, carry out a comparative analysis of the occupancy rate changes.

Table 1 is a data flow statistics table drawn from the simulation results. The statistics table shows the statistics of the queue occupancy rates of two normal data streams and four attack data streams. As shown in the following table, the row headings in the table indicate the data flow of the corresponding node number in the network topology; the column headings indicate the change of the data flow queue occupancy rate recorded every 5 s statistical time window; each value represents the specific value of the queue occupancy rate recorded by the data flow in a time interval of 5 s.

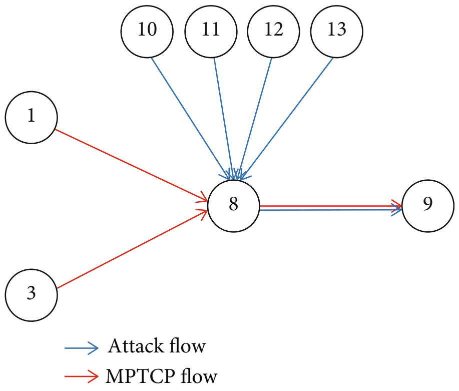

Figure 9: A simplified version of the network topology.

By carefully observing the data flow statistics table, we can summarize the following three points from it. First, the occupancy rate between the two normal TCP data streams is not much different. When the LDDoS attack occurs, the occupancy rate drops significantly. In the first two statistical time windows, the occupancy rate of data flow No. 1 is reduced from 11.03% to 0.24%, and the share of data flow No. 3 is reduced from 10.94% to 0.12%, a decrease of 10.79% and 10.82%, respectively. At the same time, these data also show that the transmission performance of data flow No. 1 is slightly better than that of data flow No. 3, which confirms the experimental conclusions drawn in the previous comparison experimental part in the delay performance comparison. When the transmission system suffers the LDDoS attack, although the occupancy rate of data flow No. 1 increases slightly within the operating time interval of 20 s to 25 s, the overall occupancy rate of TCP data flow is still close to 0. Eventually, it becomes 0 directly. Second, the occupancy rates of the four UDP attack data streams are not much different, and most of the time, they will even be completely equal. In the first two time intervals, as the share of the TCP data flow decreases, the share of the UDP data flow increases to a certain extent, but compared with the decline of normal data streams, the share of attack data streams increases. The magnitude is relatively small, about a 5% increase. On the whole, the share of attack data streams is basically stable. Third, by simply summing the occupancy rates of the normal data flow and the attack data flow, we can find that the occupancy rate of the attack flow is much larger than that of the normal data flow, and the difference between the two gradually increases until the percentage difference is 1.

Through the above specific analysis of the data flow statistics table, we can get two attack characteristics of the LDDoS attack in the multipath transmission system based on the MPTCP protocol. First, the occupancy rate of the LDDoS scattered pulse traffic sent by each puppet machine changes slightly. Second, the occupancy rate of the LDDoS attack data flow in the multipath transmission system based on the MPTCP protocol is far greater than the occupancy rate of the normal TCP data flow.

Table 1: The occupancy rate of the MPTCP flow and the attack flow.

Flow number	0-5 s	5-10 s	10-15 s	15-20 s	20-25 s	25-30 s	30-35 s	35-40 s	40-45 s	45-50 s	50-55 s	55-60 s
1	11.03%	0.24%	0.04%	0.00%	1.57%	0.12%	0.04%	0.04%	0.00%	0.00%	0.04%	0.00%
3	10.94%	0.12%	0.00%	0.04%	0.00%	0.04%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
10	19.57%	24.91%	24.99%	24.79%	24.61%	24.96%	24.99%	24.99%	25.00%	25.00%	24.99%	25.00%
11	19.52%	24.91%	24.99%	25.11%	24.61%	24.96%	24.99%	24.99%	25.00%	25.00%	24.99%	25.00%
12	19.52%	24.91%	24.99%	25.03%	24.61%	24.96%	24.99%	24.99%	25.00%	25.00%	24.99%	25.00%
13	19.42%	24.91%	24.99%	25.03%	24.61%	24.96%	24.99%	24.99%	25.00%	25.00%	24.99%	25.00%
Total	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

4. Conclusion and Outlook

This paper uses network simulation software NS2 to compare and analyze the throughput performance and delay performance of MPTCP mobile communication networks under LDDoS attack and introduces the impact of the LDDoS attack on MPTCP mobile communication networks. At the same time, through the simulation experiment and analysis of the queue occupancy rate of the LDDoS attack flow, the attack characteristics of the LDDoS attack are extracted. The experimental results show that in the transmission system based on the MPTCP protocol, the best LDDoS attack will have a significant impact on the throughput performance and delay performance of the transmission system. Compared with the non-LDDoS attack, the throughput drops sharply or even becomes 0, and the delay increases and is unstable, resulting in the decline of the robustness of the transmission system. By analyzing and comparing the occupancy rate of the LDDoS attack flow in the MPTCP transmission system, we can conclude that in the multipath transmission system based on the MPTCP, (1) the occupancy rate of the LDDoS scattered pulse traffic sent by each puppet machine changes slightly; (2) the occupancy rate of LDDoS attack data flow is much greater than that of TCP normal data flow.

By analyzing the queue occupancy rate of the attack data flow, this paper summarizes the two basic characteristics of LDDoS attacks in MPTCP transmission systems, provides research methods for the detection and defense of LDDoS attacks in multipath transmission systems, and enriches the research on the robustness of MPTCP and LDDoS attacks. However, the research results of this paper are in the initial stage of LDDoS attack feature extraction, and the accuracy rate analysis of the experimental results has not been carried out. In the future research work, we will further improve the feature extraction method, combining machine learning [36] and Convolutional Neural Networks and other related methods to extract the features of LDDoS attacks more accurately, and then use these attack features to detect and defend against LDDoS attacks, and improve the transmission performance and service quality of the MPTCP transmission system.

Data Availability

No data were used to support this article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (NSFC) under Grant No. 61962026, by the Natural Science Foundation of Jiangxi Province under Grant No. 20192ACBL21031, by the ROIS NII Open Collaborative Research 2021 under Grant no. 21AF03, and by the Cooperative Research Project Program of the Research Institute of Electrical Communication, Tohoku University.

References

[1] J. Wu, R. Tan, and M. Wang, "Energy-Efficient multipath TCP for quality-guaranteed video over heterogeneous wireless networks," *IEEE Transactions on Multimedia*, vol. 21, no. 6, pp. 1593–1608, 2019.

[2] 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, 2017.

[3] C. Raiciu, S. Barre, C. Pluntke, A. Greenhalgh, D. Wischik, and M. Handley, "Improving datacenter performance and robustness with multipath TCP," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, pp. 266–277, 2011.

[4] P. Dong, W. Yang, W. Tang et al., "Reducing transport latency for short flows with multipath TCP," *Journal of Network and Computer Applications*, vol. 108, pp. 20–36, 2018.

[5] W. Li, H. Zhang, S. Gao, C. Xue, X. Wang, and S. Lu, "SmartCC: a reinforcement learning approach for multipath TCP congestion control in heterogeneous networks," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 11, pp. 2621–2633, 2019.

[6] Z. Xu, J. Tang, C. Yin, Y. Wang, and G. Xue, "Experience-driven congestion control: when multi-path TCP meets deep reinforcement learning," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 6, pp. 1325–1336, 2019.

[7] H.-H. Chen and S.-K. Huang, "LDDoS attack detection by using ant colony optimization algorithms," *Journal of Information Science and Engineering*, vol. 32, no. 4, pp. 995–1020, 2016.

[8] Z. Liu and X. Yin, "LSTM-CGAN: towards generating low-rate DDoS adversarial samples for blockchain-based wireless network detection models," *IEEE Access*, vol. 9, pp. 22616–22625, 2021.

[9] Z. Wu, L. Ma, M. Wang, M. Yue, and L. Wang, “Research on time synchronization and flow aggregation in LDDoS attack based on crosscorrelation,” in *Proceedings of 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 25–32, Liverpool, UK, June 2012.

[10] Z. Wu, C. Wang, and H. Zeng, “Research on the comparison of flood DDoS and low-rate DDoS,” in *Proceedings of 2011 International Conference on Multimedia Technology*, pp. 5503–5506, Hangzhou, China, July 2011.

[11] X. Liu, J. Ren, H. He, Q. Wang, and C. Song, “Low-rate DDoS attacks detection method using data compression and behavior divergence measurement,” *Computers & Security*, vol. 100, article 102107, 2021.

[12] S. Toklu and M. Simsek, “Two-layer approach for mixed high-rate and low-rate distributed denial of service (DDoS) attack detection and filtering,” *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 7923–7931, 2018.

[13] M. V. Kieu, D. T. Nguyen, and T. T. Nguyen, “A way to estimate TCP throughput under low-rate DDoS attacks: one TCP flow,” in *Proceedings of 2020 RIVF International Conference on Computing and Communication Technologies (RIVF)*, pp. 1–8, Ho Chi Minh City, Vietnam, October 2020.

[14] Z. Li, H. Jin, D. Zou, and B. Yuan, “Exploring new opportunities to defeat low-rate DDoS attack in container-based cloud environment,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 31, no. 3, pp. 695–706, 2020.

[15] M. Simsek, “A new metric for flow-level filtering of low-rate DDoS attacks,” *Security and Communication Networks*, vol. 8, no. 18, p. 3825, 2015.

[16] J. Cheng, R. Xu, X. Tang, V. S. Sheng, and C. Cai, “An abnormal network flow feature sequence prediction approach for DDoS attacks detection in big data environment,” *Cmc-Computers Materials & Continua*, vol. 55, no. 1, pp. 95–119, 2018.

[17] K. S. Sahoo, D. Puthal, M. Tiwary, J. J. P. C. Rodrigues, B. Sahoo, and R. Dash, “An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics,” *Future Generation Computer Systems*, vol. 89, pp. 685–697, 2018.

[18] S. Behal and K. Kumar, “Detection of DDoS attacks and flash events using information theory metrics-an empirical investigation,” *Computer Communications*, vol. 103, pp. 18–28, 2017.

[19] M. Yue, Z. Wu, and J. Wang, “Detecting LDoS attack bursts based on queue distribution,” *IET Information Security*, vol. 13, no. 3, pp. 285–292, 2019.

[20] L. Liu, H. Wang, Z. Wu, and M. Yue, “The detection method of low-rate DoS attack based on multi-feature fusion,” *Digital Communications and Networks*, vol. 6, no. 4, pp. 504–513, 2020.

[21] Z. Wu, Q. Xu, J. Wang, M. Yue, and L. Liu, “Low-rate DDoS attack detection based on factorization machine in software defined network,” *IEEE Access*, vol. 8, pp. 17404–17418, 2020.

[22] D. Tang, L. Tang, R. Dai, J. Chen, X. Li, and J. J. P. C. Rodrigues, “MF-Adaboost: LDoS attack detection based on multi-features and improved Adaboost,” *Future Generation Computer Systems*, vol. 106, pp. 347–359, 2020.

[23] D. Tang, L. Tang, W. Shi, S. Zhan, and Q. Yang, “MF-CNN: a new approach for LDoS attack detection based on multi-feature fusion and CNN,” *Mobile Networks and Applications*, vol. 25, 2020.

[24] M. Siracusano, S. Shiaeles, and B. Ghita, “Detection of LDDoS attacks based on TCP connection parameters,” in *2018 Global Information Infrastructure and Networking Symposium (GIIS)*, pp. 1–6, Thessaloniki, Greece, October 2018.

[25] Z. Liu, X. Yin, R. Yang, and A. Dong, “Early detection of LDDoS attacks in IOT utilizing locality sensitive incremental TSVM method,” in *2021 23rd International Conference on Advanced Communication Technology (ICACT)*, pp. 194–199, PyeongChang, Korea, February 2021.

[26] N. Zhang, F. Jaafar, and Y. Malik, “Low-rate DoS attack detection using PSD based entropy and machine learning,” in *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, pp. 59–62, Paris, France, June 2019.

[27] Y. Cao, F. Song, Q. Liu, M. Huang, H. Wang, and I. You, “A LDDoS-aware energy-efficient multipathing scheme for mobile cloud computing systems,” *IEEE Access*, vol. 5, pp. 21862–21872, 2017.

[28] J. Wu, C. Yuen, B. Cheng, M. Wang, and J. Chen, “Streaming high-quality mobile video with multipath TCP in heterogeneous wireless networks,” *IEEE Transactions on Mobile Computing*, vol. 15, no. 9, pp. 2345–2361, 2016.

[29] W. Wei, H. Song, H. Wang, and X. Fan, “Research and simulation of queue management algorithms in ad hoc networks under DDoS attack,” *IEEE Access*, vol. 5, pp. 27810–27817, 2017.

[30] J. Xu, B. Ai, L. Chen, L. Pei, Y. Li, and Y. Y. Nazaruddin, “When high-speed railway networks meet multipath TCP: supporting dependable communications,” *IEEE Wireless Communications Letters*, vol. 9, no. 2, pp. 202–205, 2020.

[31] Y. Cui, L. Wang, X. Wang, H. Wang, and Y. Wang, “FMTCP: a fountain code-based multipath transmission control protocol,” *IEEE/ACM Transactions on Networking*, vol. 23, no. 2, pp. 465–478, 2015.

[32] W. Wei, K. Xue, J. Han, D. S. L. Wei, and P. Hong, “Shared bottleneck-based congestion control and packet scheduling for multipath TCP,” *IEEE/ACM Transactions on Networking*, vol. 28, no. 2, pp. 653–666, 2020.

[33] C. Xu, P. Wang, C. Xiong, X. Wei, and G.-M. Muntean, “Pipeline network coding-based multipath data transfer in heterogeneous wireless networks,” *IEEE Transactions on Broadcasting*, vol. 63, no. 2, pp. 376–390, 2017.

[34] P. Hurtig, K.-J. Grinnemo, A. Brunstrom, S. Ferlin, O. Alay, and N. Kuhn, “Low-latency scheduling in MPTCP,” *IEEE/ACM Transactions on Networking*, vol. 27, no. 1, pp. 302–315, 2019.

[35] Z. Wu and D. Zhang, “Attack simulation and signature extraction of low-rate DDoS,” *Journal on Communications*, vol. 29, no. 1, pp. 71–76, 2008, (in Chinese).

[36] R. Ji, Y. Cao, X. Fan, Y. Jiang, G. Lei, and Y. Ma, “Multipath TCP-based IoT communication evaluation: from the perspective of multipath management with machine learning,” *Sensors*, vol. 20, no. 22, p. 6573, 2020.