Low-Rate DoS Attacks, Detection, Defense, and Challenges: A Survey

WU ZHIJUN©, LI WENJING, LIU LIANG©, AND YUE MENG©
College of Electronic Information and Automation, Civil Aviation University of China, Tianjin 300300, China

Corresponding author: Wu Zhijun (zjwu@cauc.edu.cn)

This work was supported in part by the Joint Foundation of National Natural Science Committee of China and Civil Aviation Administration of China under Grant U1933108, in part by the Key Program of Natural Science Foundation of Tianjin under Grant 17JCZDJC30900, in part by the Scientific Research Project of Tianjin Municipal Education Commission under Grant 2019KJ117, and in part by the Fundamental Research Funds for the Central Universities of China under Grant 3122018D007 and Grant 3122018C003.

ABSTRACT Low-rate Denial of service (LDoS) attacks has become one of the biggest threats to the Internet, cloud computing platforms, and big data centers. As an evolutionary species of DDoS attack, LDoS attack is essentially different from the DDoS attack. DDoS attacks are the behavior of malicious blocking legitimate network traffic by destroying the targets and the infrastructure around it with huge network traffic. While, LDoS attacks are the behavior of intentional degrading the quality of TCP links by throttling TCP flows to a small fraction of its ideal rate with periodic small pulse sequence. Hence, LDoS attack has a very small flow (around 10%-20% of the background traffic), it is easy to eluding the detection of routers and counter-DoS mechanisms. We try to reveal the mechanism of the LDoS attack and attempt to figure out the generation principle of LDoS attack in this paper. We classify the LDoS attacks and existing defense methods according to time domain and frequency domain in which detection and defense are performed. Furthermore, we highlight the filter approach to defense against LDoS attack. The initial purpose of our work is to encourage researchers to study effective ways to detect and defend against LDoS attacks with innovation and aggressiveness.

INDEX TERMS Low-rate Denial of Service attacks (LDoS), detection method, attack prevention system, defense mechanism.

I. INTRODUCTION

Distributed denial of service (DDoS) attacks have been raging for more than 20 years since it was reported on a large scale in 1998. DDoS attack has been very aggressive, extremely destructive, and has a huge impact. It is the favorite of cyber-criminals and black industry chain operators. After more than 20 years of development, DDoS attacks have changed dramatically in both attack strength and intelligence. In terms of attack intensity, DDoS attacks become more and more fierce, and the maximum attack traffic is almost 1Tbps. Moreover, in the near future, it will definitely exceed 1Tbps. In the aspect of intelligence, DDoS attacks have evolved from simple, large (high-rate) traffic to smart, small (low-rate) flows. Hence, a new type of DoS attack came into being. This is low-rate DoS attacks (LDoS), which was first discovered on the Internet2 backbone network by Asta Networks monitored in 2001.

Kuzmanovic and knightly et al. showed this new type of low-rate TCP-targeted DoS attack at SIGCOMM in 2003 [1]. It is a kind of attack method with strict organization, rude behavior, strong attack power and great influence. A DDoS attack is an intentionally malicious action to destroy legitimate traffic of a targeted network, server, and even service by striking down the targeting infrastructures with a large volume of network traffic (Flood) from wide world. DDoS attacks achieve effectiveness by organizing botnets or large quantity of zombies as sources that generate attack traffic. Exploited machines that are used as zombies include servers, computers and network devices, and even the Internet of Things (IoT) devices such as cameras. From a broad perspective, the DDoS attack seems to be flooding and madly hitting the riverbed. The overflowing floods are raging and ruining the river embankment, causing normal river water to ravage the surrounding infrastructure with the flood of the levee and unable to reach the true destination. This scenario is like a congestion on a highway, preventing normal traffic from reaching its set destination.
A. LOW-RATE DENIAL OF SERVICE (LDoS) ATTACK

LDoS attack exhibits a periodic pulse shape, in which the attack energy is concentrated, so the average attack traffic is small. The distributed LDoS attack is shown in Fig. 2.

Many single LDoS attack pulses from different attack sources with a small average flow rate are connected in a certain organization to form a pulse train of a certain period. These bursts form a stack at the target, causing the target bottleneck link to block or leading to a decline in quality of service of the target terminal. Although the average traffic of LDoS attacks is small, its attack power is not much smaller than the one of DDoS attack.

The targets of an LDoS attack can be categorized into two types. One is a bottleneck link and the other is a terminal system. LDoS attack can exploit the vulnerability of TCP/IP protocol and routing queue management mechanism to start attacks, which greatly reduces the throughput of the attacked link and can greatly degrade the quality of service of the attacked terminal.

The reason why the traffic of the LDoS attack is low can be derived from Fig. 2. The traffic of the LDoS attack is concentrated in the rectangular pulse in which many packets are sent in a short period of pulse duration and this sending process is repeated at a specified frequency, i.e. pulse period. Therefore, the energy of the attack depends on the amplitude and duration of the rectangular pulse, that is, the LDoS attack traffic is averaged over time in the rectangular pulse. Therefore, the average traffic of LDoS attacks is small. The effect of the LDoS attack is reflected in the reduced quality of service of the target being attacked. Therefore, it is also called a degradation of quality (RoQ) attack [2]. The form of an LDoS attack is a series of periodic pulses. Therefore, it is called a pulsing attack [3]. LDoS attacks appear to sneak stealing and consuming user traffic in cloud computing platform and big data center. Therefore, this thief behavior of LDoS attacks is aptly called a stealthy attack [4].

Instead of exhausting the resource of network and capacity of network source violently, the LDoS attack targets the adaptive mechanisms, which are widely adopted around internet to ensure using efficiency, fairness, and stability properties, to deteriorate the resource utilization rate of specific protocol or application. In general, LDoS attackers send periodical legitimate traffic to attack victim. Each attack pulse will cause the target adaptive mechanism to afford negative feedback information according to the attacker’s intention to victim, so that it can adaptively stop the service or reduce the service quality. After each adjustment, it will take a while to elevate...
service performance to the normal level. Hence, the service quality of victim-end will keep being low during the periodical attack.

Currently, the main target of LDoS attacks is systems with highly centralized services and devices, such as cloud computing and big data service platforms. The concealment of LDoS attacks makes it easy to hide in the huge traffic generated by cloud computing and big data service platforms without being discovered. Therefore, with the development of cloud computing and big data service platforms, they have become the objects of LDoS attacks. The main purpose of LDoS attack is to cause traffic loss in cloud computing platform and big data center, resulting in huge growth in traffic for cloud computing and big data users, leading to huge economic losses. This is the reason why the operators of network black industry chain love LDoS attacks. They can turn cloud computing and big data users’ traffic losses into their own economic income. According to the effect of the LDoS attack, the form of the LDoS attack is divided into three categories, Economic Denial of Sustainability (EDoS), Depletion of Bank (DoB) and Fraudulent Resource Consumption (FRC).

LDoS attacks have been rampant for a long time, but few have been reported. Concerning the report of the LDoS attack incidents, in addition to the first exposure on the backbone network of Internet2 in 2001, there was another one of attacking Tencent.com on October 17, 2004 in China. Instead, the DDoS attack event is more influential than once. The reasons why LDoS attacks are not as widely reported as DDoS attacks are as follows:

(i) The technical implementation of the LDoS attack is very difficult in achieving accurate attack traffic synchronization and aggregation. It must be very proficient in mastering the network transmission protocol and the router queue mechanism for an attacker to organize a destructive LDoS attack. Normal hackers, especially cybercriminals who only use attack tools to launch attacks, are hard to initiate LDoS attacks. Although the LDoS attack is difficult to implement, it cannot be said that its attack events are few or impossible.

(ii) LDoS attacks are very embarrassing and stealthy, which can make the LDoS attacks easy evade the detection of traditional DoS attack detection mechanisms. Even if an LDoS attack occurs, the network system is not flawed, but the system running quality is degraded, which is manifested in slow speed (slow data update, slow web page refresh, etc.). As a result, large-scale networks, cloud computing platforms, or big data center operators attribute such situations to system equipment failures or line failures, without considering attacks.

(iii) Even if the managers of cloud computing and big data service platforms have detected LDoS attack, they have no effective means and capabilities to stop the penetration and destruction of attacks. More difficult challenge for them is to extract and analyze the characteristics of LDoS attacks. The victim (the cloud computing platforms and the big data centers) passed the loss on to the user. In order not to cause customers to panic and scare away users, they generally do not report and publicize.

B. COMPARISON WITH EXISTING REVIEW STUDIES

In the above content, we briefly introduced the LDoS attack, in order to let more readers understand the LDoS attack and be familiar with its attack characteristics. We have produced a table that presents all reviews of LDoS attacks (see Table 1) and compares them with our research to highlight the advantages of our research.

From the Tabel 1, it is showed that detecting and defending against LDoS attacks has become a research hotspot in the field of network security. Many research institutions and scholars have proposed many innovative methods. Among them, some scholars published papers on the review of LDoS attacks. They attempted to illustrate the organizational form and attack characteristics of LDoS attacks from the technical aspects.

Mohan et al. [5] studied in detailing the RED, LDoS attacks against RED and the different methods used to defend against such attacks. His research details the principles and prevention mechanisms of LDoS attacks.

Qiao et al. [6] listed a variety of definitions and aliases of LDoS, and carried on a survey of currently related works are summarized and simulation of attacks are investigated, which will help to direct the continued work such as finding the algorithms to detect and protect from LDoS attacks.

Wen et al. [7] introduced the development history of LDoS attacks and the unique insights of different researchers. They also analyzed the security of TCP congestion control mechanism and found the root cause of its security vulnerabilities. Then, they described the basic model of LDoS attack and explained the principle of LDoS attack. With regard to various LDoS attack detection and defense schemes, they carried out classification and analysis from various aspects. At the end of this paper, some understandings of the problems existing in the current research and future research trends and suggestions are proposed.

He et al. [8] studied the principle of LDoS attack, and the various attack methods of the LDoS are classified, described, modeled and simulated. This paper analyzed the difficulties of LDoS attack defense and summarized the proposed LDoS attack defense methods.

Ficco and Rak [4] studies have shown that stealthy attacks have very low attack traffic with the goal of minimizing their visibility, while the destructive power of the stealthy attack is as much intense as the violent attack. Stealthy attacks are sophisticated attacks designed to cause the performance of the target system to reach a bad or even worst case through specific period, pulsing, and low-rate flow pattern. In their research, they proposed a strategy to coordinate stealth attack patterns, which shows a gradual increase in intensity, aiming to bring the largest financial cost to cloud customers, while respecting the work scale and the service arrival rate.
prescribed by detection mechanisms. Their research also illustrated the application of their proposed strategies and its impact on the target system installed in the cloud.

We compare a few survey papers on LDoS attack (Seen in Table 1). The latest research results on detection or mitigation of LDoS attacks is also highlighted in this paper. Although these papers primarily focus on the organization and detection of LDoS attack, and defense mechanisms, most failed to delve into the latest developments in LDoS attack design, protocol-related issues, and the utilization of mechanisms.

This paper investigates the LDoS attack in large-scale network, with a focus on the classifications and scope of this kind attack and its detection and defense. This survey paper intends to address the following primary points.

**Attack.** To the best of our knowledge, this paper presents the first comprehensive classification of LDoS attack. We classify LDoS attack into four categories: single source, distributed aggregation, synchronous and asynchronous attack. Then, this paper classifies the LDoS attack in each category based on the types of attack.

**Detection.** This survey paper first classifies LDoS attack detection methods from two perspectives: time domain and frequency domain, and the detection methods are divided into three categories: network traffic, routers and network behaviors. Moreover, summarized for each specific detection method.

**Defense.** The defense methods are divided into 3 categories, filtering of LDoS attacks, improving network parameter, reallocation of resources, and each specific method is analyzed.

We would like to share our achievements in network feature extraction and defense technology with readers and look forward to all suggestions from scholars in this field.

The contributions of the survey are as following.

We make a comprehensive analysis of the principles, models, methods, and effectiveness of LDoS attacks, and give an evaluation of LDoS attacks based on the experiment results of previous achievements. Through our analysis, we hope LDoS attacks could get more attention.

The performance of LDoS attacks under different TCP versions is studied, and the concealment and destruction characteristics of LDoS attacks are obtained through experiments by lists and curves.

We advocate the combination of digital signal theory and network theory approaches to prevent LDoS attacks and make some research progress. In addition to the signal processing ideas we advocate, we also analyze and compare the performance of other LDoS attack prevention methods through lists, mapping, and other means, the reader can understand the advantages and disadvantages of different algorithms via comparative analysis.

We summarize the current defense methods and propose corresponding improvement measures and prospects.

The rest of the paper is organized as follows. In Section 2, we conduct a deep comparison between DDoS attack and LDoS attack and summarize the attack characteristics of LDoS attack. In Section 3, the LDoS attacks are categorized in detail and their attack scopes are described separately. In section 4, we summarize and propose detection methods for LDoS attacks based on their attack scenarios and characteristics. In section 5, the defense methods for LDoS attacks are summarized based on their attack scenarios and characteristics. In section 6, challenges and recommendations in future research are given.

### II. CHARACTERISTICS OF LDoS ATTACKS: LDoS VS. DDoS

DoS (Denial of Service) attack is a collective term for cyber-attacks, which results in low network performance, such as denial of access to the web or any internet services. Generally, DoS attacks could be classified according to the feature of sending rate. Typical flooding DoS attack, such as SYN flood, attempts to overload the target servers with high-rate attack flow. Distinguish from the classical high-rate DoS attacks, a new type of DoS attack called as low-rate DoS (LDoS) attack, which exploits the adaptive mechanism of network by sending low-rate attack flows was discovered. LDoS is one of many forms of the distributed DoS (DDoS) attacks which has been proved itself great destructive power through crippling popular websites likes Yahoo!, CNN, eBay, Dell and Amazon in 2000, and IoT (Internet of Things) - powered DDoS attacks have hilted Internet on October 21, 2016. It is no doubt that DDoS attacks are wreaking havoc on cloud computing and big data service platforms, and large networks. Some scholars also distinguish between low rate and high rate DoS attacks

| Article | Network security threat analysis | Attack type classification | Model analysis | Attack effectiveness analysis | Attack target analysis | Detection category classification | Defense category | Detecting indicator analysis | Detection and defense method improvement suggestions |
|---------|----------------------------------|-----------------------------|---------------|-----------------------------|-----------------------|----------------------------------|-----------------|-----------------------------|-------------------------------------------------|
| [4]     | √                                | ×                           | √             | √                           | √                     | ×                                | ×               | ×                           | ×                                               |
| [5]     | ×                                | ×                           | ×             | ×                           | ×                     | ×                                | ×               | ×                           | ×                                               |
| [6]     | ×                                | ×                           | ×             | ×                           | ×                     | ×                                | ×               | ×                           | ×                                               |
| [7]     | ×                                | ×                           | ×             | ×                           | ×                     | ×                                | ×               | ×                           | ×                                               |
| [8]     | ×                                | ×                           | ×             | ×                           | ×                     | ×                                | ×               | ×                           | ×                                               |
| Ours    | √                                | ×                           | √             | ×                           | √                     | √                                | √               | √                           | √                                               |
TABLE 2. The comparison of DDoS and LDoS.

| Name        | Type of attack | Rate of attack | Effect of attack           |
|-------------|----------------|----------------|-----------------------------|
|             | Traditional    | New            | High | Low | Denial of service | Reduce quality | Steal traffic |
| DDoS        | SYN flood      | ✓              | ✓    | ✓   | ✓               | ✓              | ✓             |
|             | ICMP flood     | ✓              | ✓    | ✓   | ✓               | ✓              | ✓             |
|             | UDP flood      | ✓              | ✓    | ✓   | ✓               | ✓              | ✓             |
|             | DNS flood      | ✓              | ✓    | ✓   | ✓               | ✓              | ✓             |
|             | VoIP flood     | ✓              | ✓    | ✓   | ✓               | ✓              | ✓             |
|             | CDF            | ✓              | ✓    | ✓   | ✓               | ✓              | ✓             |
|             | Flow table flood | ✓        | ✓    | ✓   | ✓               | ✓              | ✓             |
| LDoS        | Shrew DoS      | ✓              | ✓    | ✓   | ✓               | ✓              | ✓             |
|             | Fake session   | ✓              | ✓    | ✓   | ✓               | ✓              | ✓             |
|             | Session attack | ✓              | ✓    | ✓   | ✓               | ✓              | ✓             |
|             | RoQ DoS        | ✓              | ✓    | ✓   | ✓               | ✓              | ✓             |
|             | HTTP Fragmentation | ✓      | ✓    | ✓   | ✓               | ✓              | ✓             |
|             | FRC            | ✓              | ✓    | ✓   | ✓               | ✓              | ✓             |
|             | Bandwidth Congestion | ✓               | ✓    | ✓   | ✓               | ✓              | ✓             |

According to the average amount of contracted amount per unit time. For example, Yang Xiang of Deakin University in Australia has 1000 packet/s as the standard to distinguish between high rate and low rate [9]. LDoS attacks are also known for the low-rate attack traffic that accounts for only 10-20% of normal traffic. LDoS attacks have so excellent avoidance detection capabilities that are the most favorite cybercriminal attacks, as well one of the major network security threats.

As it is shown in Table 2, the research results of traditional DDoS attacks like UDP flood, ICMP flood, Fragmentation, DNS flood, VoIP flood are rich enough [10], [11], so we don’t discuss much in this paper.

CDF (Cloud Droplet Freezing) [12] is a new type of DDoS attack in cloud computing platform that uses virtual machines to flood each other to consume the bandwidth resources of the internal communication link of the cluster and the computing resources of the physical server. The flow table flood attack [13] is a DDoS attack against the SDN architecture. In the scenarios of cloud computing and big data center applied with SDN, both the SDN control layer and the data layer may become attack targets. The controller floods the new flow table rules in the switch flow table, which will exhaust the flow table resources of data layer. All these attacks have the same effect that is denial of service with a high attack rate.

In addition to the above flooding DoS attacks, various low-rate DoS attacks are increasingly popular under cloud computing platforms. There are mainly fraudulent resource consumption (FRC) attacks [14], [15], RoQ DoS, and Shrew DoS attacks. For victims, systems that suffer from such attacks tend to significantly cut down the quality of service (QoS). To attackers, the use of such attacks tends to achieve the best price/performance ratio, and the attacker can get the ideal attack effect at a small cost. In addition, such attacks are so easy to evade detection due to their low attack rate.

As it is shown in the Fig. 3, the DDoS attack is just like a massive flood, it can instantly rush the river embankment and leads to overwhelming flooding. However, the LDoS attack is as a funnel that is full of sand and the sand is piled up on the riverbed, which makes the river mattress high, finally resulting in a decrease in river flow.

Compared with traditional DoS attacks, LDoS attack has three distinguish characteristics as follows in Fig. 4.

As we can see from Fig. 4, the main characteristics of LDoS attack can be summarized in three aspects:

1. The LDoS attack utilizes the adaptive mechanism of TCP/IP protocol (congestion control and queue management), which makes the control measures look like normal, thereby reducing service quality.

2. The LDoS attack traffic has the same characteristics as the legitimate network traffic, and has the behavior characteristics of the real data stream, and it is completely hidden in the background network traffic. Therefore, LDoS attack traffic is extremely concealed.

3. The LDoS attack is organized in a simple way, and the attack is launched through a single attack source by sending a pulse. The average rate of attack traffic is very low, and the number of packets sent is very small.

In summary, the LDoS attack can achieve the expected results, and can successfully evade the commonly used attack detection mechanism, which is extremely difficult to defend.

The analysis of the results of the above analysis shows that the LDoS attack is a periodic pulse attack and the duration of attack pulse is very short. It has the following characteristics.

(i) The LDoS attack only congests the link in a short time. It can use a small traffic to reach the same attack effect, which means that a hacker can launch an attack without controlling a large number of machines, so it is easier to complete the target of the attack.

(ii) The LDoS attack can be launched in various forms, including single attack host as well as multiple hosts. Moreover, attacks initiated by multiple hosts can further reduce the
attack traffic of each attacking host and make it easier to evade detection.

(iii) LDoS attacks only need to cause link congestion to achieve the attack purpose, so it can use any traffic, including TCP flows. The attack stream is more difficult to be filtered in the normal TCP stream, and the destination address of the traffic can also be changed. According to the behavioral characteristics of the LDoS attack, it can be likened to a kind of “sand” attack. Because the packets of the LDoS attack are concentrated in periodic pulses, each pulse is equivalent to a funnel and the attack packet is “sand”. When the attack is launched, the periodic pulse full of “sand” will leak “sand” after reaching the target, and accumulate in the bandwidth of the target, finally causing congestion. This process is like the accumulation of sand in a river over a period, and the riverbed is too high finally causing the river to flow slowly.

III. LDoS ATTACKS’ SCOPE AND CLASSIFICATION

LDoS attacks are generated using two mechanisms, the first is the congestion control in TCP/IP protocol, and the second is the router queue management. The LDoS attacks reduce TCP throughput through exploiting TCP’s slow-time-scale dynamics mechanism of retransmission time-out (RTO). LDoS attack packets are repeatedly sent at a very fast rate, causing repeated timeouts for normal traffic. Even though the throughput of TCP is reduced to a certain extent, it will not be aware of being attacked due to the low average rate of LDoS attacks.

At SIGCOMM in 2003, Kuzmanovic and Knightly [1] showed this new kind of low-rate TCP-targeted DoS attack called “Shrew Attack”, which maliciously exploits TCP’s retransmission time-out mechanism. Luo and Chang [3] named this kind of attacks as PDoS (Pulsing Denial of service) attack and presented two specific attack methods: timeout-based and AIMD (Additive Increase Multiplicative Decrease)-based attack. Guirguis et al. [2], [16] exposed a variant of RoQ (Reduction of Quality) attacks exploiting the transients of their adaptation mechanisms.

In this section, we will categorize and analyze LDoS attacks from many different perspectives, for instance, the vulnerabilities of different protocols, organizational forms, and different victim-end. Although LDoS attacks are diverse, they are essentially the same. The difference is that different attack parameters are set according to different goals, to cause a decrease in service quality.

As it is shown in Fig. 5 [1], the general model for LDoS attacks can be expressed as a ternary set of $< R, L, T >$, where...
where $R$ is the rate of each attack pulse, $L$ is the duration of each attack pulse, and $T$ is the duration of the attack period.

LDoS can be classified from three perspectives of security vulnerability, organization and actual scenario. The classification of LDoS attacks is shown in Fig. 6. According to the security vulnerabilities exploited, LDoS can be divided into three categories, including application layer, transport layer and network layer LDoS attack. In terms of organization, it can be divided into single source attack, distributed attack, synchronous attack, and asynchronous attack. From practical application scenarios, it can be divided into three types of Terminal system, Network node and Border router attack. For a detailed description of LDoS attacks under different divisions, see the following sections.

A. SECURITY VULNERABILITIES EXPLOITED BY LDoS ATTACKS

LDoS attack exploits security vulnerabilities in transmission layer protocol, network layer protocol and application layer protocol. The following analysis for vulnerabilities of LDoS attack in Sect. 3.1 will be expanded from the above three derivations.

1) VULNERABILITIES OF TRANSMISSION LAYER PROTOCOL

The adaptive mechanism included in the TCP protocol was the first target of LDoS attack. Time-out retransmission mechanism and congestion control mechanism are design for TCP to make sure of providing reliable streaming services that all bytes are received correctly and in the same order as they were sent. Packet loss, duplication, out-of-order and other issues that normally caused by traffic load balancing, network congestion or other unpredictable network behaviors will invoke these mechanisms. The LDoS attackers maliciously send periodical attack flows to result in the TCP packets loss that is regarded as congestion. Further, once congestion is detected, the adaptive mechanisms of TCP will choose reducing transmission rate or time-out that depends on the varying degrees of congestion. Therefore, LDoS attack can exploit vulnerabilities of different mechanisms by triggering congestion with diverse degrees and frequencies.

a: AGAINST TCP TIME-OUT RETRANSMISSION MECHANISM

Shrew attack is one of the LDoS attacks against retransmission time out mechanism. The Shrew attack triggers a large number of packet losses and forces these TCP connections to enter retransmission time out by sending short and high-rate attack pulses to the router of bottleneck link. The sender of TCP will not receive enough ACK to keep transmitting data and have to waiting for one RTO (Retransmission Time Out) to enter slow-start to retransmit the lost packets. Once the sender begins the retransmission, the attacker will send the next attack pulse to the same position. Hence, the TCP
connections will scarcely increase the sending rate under this attack and the sending rate will persist in an awful state. Considering the attack method, attackers must figure out the duration time \( T \) between each two neighboring attack pulses. For this purpose, attackers must match attack period \( T \) to the value of RTO.

RTO is the most important parameter of the retransmission time out mechanism. The retransmission time out mechanism ensures that the TCP sender can retransmit data without receiving any feedback information, such as ACK (acknowledgement), from the receiver. In the event of media damage, heavy congestion, etc., the receiver will not receive the lost packets and the ACK will be exhausted. In this case, the sender will wait for the retransmission time out (RTO) and retransmit those unacknowledged packets. Since it is impossible to confirm that, the unacknowledged packets lost or out-of-order, the RTO value, time setting of the retransmission timer, should be balanced between not too low and not too high. It is necessary to ensure enough time to continue to wait for the unacknowledged packets, but also to avoid spending too much time in unnecessary waiting. For this purpose, Paxson et al. [17] figured out a function of RTO. First, getting the initial measurement of RTT (round-trip time), which is equal to \( R \) and calculating the initial value of SRTT (smoothed round-trip time) and RTTVAR (roundtrip time variation). The initial value of SRTT is \( R \) and the RTTVAR is half of \( R \). Then, after a new measurement of RTT, which is equal to \( R' \), updating SRTT and RTTVAR. Finally, setting the value of RTO according to minRTO or SRTT, \( G \) and RTTVAR, where \( G \) represents the time granularity. If the value SRTT plus the larger of \( G \) and four times of RTTVAR is larger than minRTO, the RTO is equal to the value. Otherwise, RTO is equal to minRTO.

The substance of the Shrew attack is to provoke the TCP flows to repeatedly enter the time out state in which the sender can not send new data. Hence, the attacker sets the attack \( T \) period to RTO. Kuzmanovic et al. also designed a Minimum Rate DoS model for Shrew attack to reduce the cost of attacks. In this model, a double-rate attack pulse was used. The Minimum Rate DoS model for Shrew attack is shown in Fig. 7.

As shown in Fig. 7 [2], [3], the purpose of the first phase is to fill the queue with high-rate attack packets in a short time. There is a relationship between attack duration time \( l \) and attack rate \( R_{\text{max}} \). In the duration time \( l \) the attack rate \( R_{\text{max}} \) can make sure the free queue is filled, which means the \( R_{\text{max}} \) and \( l \) are approximate inverse relations.

The purpose of the second phase is to maintain the queue in full state so that TCP packets can not enqueuer and be dropped. The attack rate is equivalent to the bottleneck link bandwidth \( C \). The duration time \( l_2 \) is related to the number of TCP packets transmitted in the link. However, since this information can not be obtained accurately, for the attack effect, \( l_2 \) is usually set to 2-3 RTTs.

\[ b: \text{AGAINST TCP CONGESTION CONTROL MECHANISM} \]

The AIMD-based PDos attack proposed by Luo and Chang [3] is essentially the LDoS attack against TCP congestion control mechanism. This attack primarily exploits congestion control machine to reduce cwnd (congestion window). Since a small amount of TCP packets are lost that caused by each attack pulse, the TCP sender will receive the congestion feedback (three duplicate ACKs) from the receiver. Therefore, the sender decreases the congestion window according to the congestion avoidance algorithm. Periodical sending attack pulses will cause that the TCP repeatedly enter the fast recovery state and the cwnd is dynamically stable at a lower level. The AIMD-based PDOS attacks exploit vulnerabilities of congestion control algorithms that designed for increasing the cwnd modestly and preventing congestion. There are four congestion control algorithms are designed in TCP, including congestion avoidance, slow start, fast retransmit, and fast recovery.

\[ i) \text{SLOW START AND CONGESTION AVOIDANCE:} \] Two variables, the cwnd and the sssthresh (slow start threshold), are used in each TCP connection for implementing these algorithms. The cwnd is a limitation on the amount of data that a TCP sender can transmit into the network. Therefore, the amount of data which is allowed to transmit must not be higher than cwnd. During slow start, cwnd increase one for each ACK received. During congestion avoidance, the algorithm expects cwnd increase one per round-trip time (RTT).

Whether to enable congestion avoidance or slow start algorithms to control data transmission depends on the sssthresh value. If cwnd is less than sssthresh, use the slow start algorithm. Otherwise, when cwnd is greater than sssthresh, use the congestion avoidance algorithm.

During congestion avoidance, the TCP sender detects packet loss over the timeout of retransmission timer or the arrival of 3 duplicate ACKs. Once packet loss is detected, firstly update the value of sssthresh to half of the original value, and then update the value of cwnd to the value of sssthresh plus 3.

\[ ii) \text{FAST RETRANSMIT AND FAST RECOVERY:} \] The fast retransmission algorithm first uses the arrival of three repeated ACK’s as an indication of segment loss. After receiving three repeated ACK’s, the TCP sender then resends the packet.
The cwnd under AIMD-based LDoS attacks uses the fast retransmission mechanism to reduce cwnd. Since the AIMD-based LDoS attack doesn’t need to trigger the TCP connections to enter the retransmission time out state, the requirement of the quantity of lost packet will no more need to be a lot, even only one packet lost is enough. Meanwhile, the cost of each attack pulse will be, therefore, saved and difficult to be detected [3].

However, the performance of the LDoS attack against TCP congestion control mechanism is worse than the one against retransmission time out mechanism. Considering that, in TCP congestion control mechanism, three duplicate ACKs are needed for triggering fast retransmission and fast recovery mechanism. Therefore, an attacker must leave behind at least four TCP packets that can be successfully transmitted after the lost TCP packet caused by attack.

### c: AGAINST HYBRID MECHANISM

Guirguis [18] proposed the link-saturation Shrew attack and the full-buffer Shrew attack, both of which have better attack potency than the Shrew attack. Instead of immediately sending attack pulse when the TCP connections start retransmitting after a RTO, the LDoS attacks against Hybrid Mechanism will wait for the TCP connections increasing their cwnds in congestion avoidance and slow-start state. Obviously, the utilization rate of the bandwidth is awful during the congestion avoidance and slow-start state. During the full-buffer Shrew attack, upon the full buffer state, the attack traffic lasting an RTT with the rate equal to the bandwidth of bottleneck is enough to cause all the packets in the current cwnd to be lost. After the retransmission time out, TCP will enter the slow start process until the cwnd grows to the slow start threshold ssthresh. Since then, TCP enters the congestion avoidance process by linearly increasing cwnd until the next attack comes.

Each attack pulse includes B plus \( C \times RTT \) attack packages, the attack period \( T \) is the sum of the values of the three phases in the Fig. 10, which are given by:

**Phase 1**: Last for \( T_1 \), which equals minRTO.

**Phase 2**: during slow-start state, the cwnd exponentially increases to the \( ssthresh \), which equals \((C+1)/2\) and last for \( T_2 \).

**Phase 3**: during congestion avoidance, state the cwnd linearly increases to \( C + 1 \) and last for \( T_3 \).

The cwnd and queue under Full-buffer Shrew attack send each attack pulse every time TCP packets fill up the buffer. The full-buffer Shrew attack is consistent with the link-saturation Shrew attack, and both exploiting TCP congestion control mechanism after the TCP connection finishes the RTO to prolong the attack period \( T \). In addition to the same advantage of declining the cost of attack per unit time, the full-buffer Shrew attack requires a longer attack period. During the full-buffer Shrew attack, upon the full buffer caused by TCP packets, the cwnd increased to \( B + C + 1 \). In the first portion, then we need a pulse lasting for a \( RTT \) to trigger the whole window of TCP packets lost. After that, the TCP connection will enter the retransmission time out state. Moreover, the next attack will be sent until the buffer is full again. Hence, comparing with the link-saturation Shrew attack, the attack potency of the full-buffer Shrew attack is improved. However, the utilization rate of bandwidth is little worse [19].

Each attack pulse has two portions, the first portion is B attack packets with lower sending rate than the first portion of the link-saturation Shrew attack, and the duration is \( B/C \times rtt \); the second portion is an attack stream with the same speed as the bottleneck bandwidth, and the duration is \( rtt \). According to the periodically changes in the cwnd we can calculate the appropriate attack period, which is given by:

**Phase 1**: Last for \( T_1 \), which equals minRTO.

**Phase 2**: during slow-start state, the cwnd exponentially increases to the \( ssthresh \), which equals \((B+C+1)/2\) and last for \( T_2 \).

**Phase 3**: During congestion avoidance state, the cwnd linearly increases to \( B + C + 1 \) and last for \( T_3 \).

### 2) VULNERABILITIES OF NETWORK LAYER PROTOCOL

AQM (Active queue management) is a queue management method deployed on the router. By choosing to drop some packets as congestion notification before the queue overflows, AQM avoids queue overflow caused by heavy congestion and keeps queue at a low level. RED (Random Early Detection) is an AQM algorithm widely deployed on routers. The RED algorithm avoids congestion depending on average.
queue size, while the average queue size is calculated by Exponentially Weighted Moving Average (EWMA) method. When the average queue reaches a certain value, congestion is coming. At this point, the RED algorithm will drop some packets according to the probability to send a congestion notification to the sender. The average queue as a core indicator of the RED algorithm, and each packet enters the queue RED algorithm will calculate the current average queue $\bar{Q}$.

The value of average queue size $\bar{Q}$ is compared with the set threshold $Q_{\text{min}}$ and $Q_{\text{max}}$. The RED algorithm considers that congestion will occur after the average queue is greater than $Q_{\text{min}}$, and congestion has occurred when the average queue is greater than $Q_{\text{max}}$. When the next packet enters the queue, it will be dropped according to the probability of segmentation.

RoQ (Reduction of quality) attack was explored by Guirgis et al. [2] firstly. However, they did not state the specific steps for this attack clearly and in detail. RoQ attackers only need to periodically send attack pulses to the target node to destroy the node router’s service performance [18], [19] without careful analysis and research on the status of each transport stream.

The LDoS attack traffic is represented as a buffer size $B$ and bottleneck link of capacity $C$, which is shared by $m$ TCP connections and a single CBR connection. To simply, our considerations include a burst of $M$ packets in bits/bytes sent at a rate of delta $\delta$ packets per second or a few bits/bytes in a short time $\tau$, here $M$ is equal to $\delta$ multiplied by $\tau$. Repeating the process for each $T$ time unit. Hence, the $M$ denotes attack strength, the $\delta$ expresses attack-sending rate, the $\tau$ presents the attack duration, and the $T$ indicates the attack period. LDoS attacks send high-rate pulses to force the router’s average queue size increasing rapidly and cause a large number of normal TCP packets to be dropped. Then, the RED mechanism feeds back the congestion signal to the legitimate TCP sender. In this case, the TCP sender has two options. First, reduce cwnd accordingly to reduce the transmission rate. Second, a timeout retransmission state is entered during the idle time between the two attack pulses. At this moment, no matter what state the TCP sender is in, the router’s instantaneous queue size is rapidly reduced or even null, which will result in a reduction in the average queue size of the router. As a response, the RED mechanism gradually reduces the packet-dropping rate, while the TCP end gradually recovers from the timeout state to retransmit the packet. The TCP sender’s cwnd will go through a process of congestion avoidance and slow start to increase router queue. Once the router buffer is full, next attack pulse would come to induce a same congestion process as described above.

3) VULNERABILITIES OF APPLICATION LAYER PROTOCOL

LDoS attack against application layer refers to LDoS attacks that exploit some vulnerabilities of the application layer protocol. LDoS attacks against application layer are more specific to the victim of the attack than the against transmission layer, generally, they are easier to for an attacker to attack network service provider with causing a cessation of some service. Moreover, the damage caused by the attack can be further amplified in the application layer, and this makes LDoS attack against network layer an important direction for further exploration of LDoS.

a: AGAINST HTTP

HTTP (hypertext transfer protocol) is a stateless application layer protocol based on request-response patterns, and its ways of connecting are always based on the TCP. Most web exploits are web applications built on the HTTP. HTTP1.1 gives a mechanism for persistent connection, which refers to the server, and can send multiple objects to the client on the same established TCP connection, while the original non-persistent connections require to start TCP connection every time a service transmit an object to the client. There are three major benefits of persistent connection as (i) it reduces the number of conversations of connect and disconnect between the client and the server, avoids the unnecessary consumption of CPU resources of the client and server. (ii) it reduces the occupation of server cache resources each time a connection is established. (iii) it avoids the need to build TCP connection multiple times, each time cwnd grow with a form of slow start, thus increases the server’s delivery efficiency.

The LoRDAS [20] attack against HTTP exploits the KeepAlive mechanism provided by the HTTP, which enables the server to maintain the connection after sending the data that the client has requested rather than end it immediately. The attacker can masquerade as a normal client to establish a connection with the server, thus occupying the server its process resources. Once the connection is established, the server must wait for a timer timeout (KeepAliveTimeout) to disconnect if the server does not receive any requests. The LDoS attack against the HTTP sends a connection request to the server with an attack cycle of KeepAliveTimeout. While the queue is nearly full, the time when a connection is terminated is the one when the new space in the queue appears, preventing normal user requests from entering the queue. The server will not respond to any normal requests and implement the denial of service when the attacker requests the entire waiting queue. For reducing the send rate of the attack request and occupying position in the queue effectively, the attacker must control the sending time of the attack request with an accurate niche targeting time mechanism. In LoRDAS attack, the attacker used a strategy to perform accurate forecast of the time finishing each request service, namely the time that request queue-releasing space, and send a small number of requests to get the positions of the request queue only in the time nearby.

b: AGAINST BGP

The security of the inter-domain routing system is a key factor that affects the security of the Internet operation, and has an important impact on the healthy and stable operation of the Internet. Inter-domain routing system mainly uses the BGP (border gateway protocol), however, there are serious
potential safety hazards in the beginning of the BGP design, resulting in inter-domain routing system faces a serious security threat. Because BGP runs on the transport layer with TCP, attacks against TCP can threaten the security of the BGP session. Zhang et al. [21] proposed the TCP-target DoS attack mode for BGP based on the UDP-based low-rate DoS (LDoS), which can lead to the extension of network aggregation time and the reset of BGP session. Based on TCP-target DoS attack, Schuhard et al. [22] proposed a cross-plane attack mode based on BGP data plane named CXPST (Coordinated Cross Plane Session Termination). This type of attack selects part of the critical path in the system carefully, then using distributed attack source-end to carry on LDoS attack on them at the same time, by triggering many routing updates to run out of the router’s storage and computing resources, to achieve the aim of paralyzing the entire system. TCP-target attack against BGP by using the topological structure of the inter-domain routing system and the routing update feature of BGP to magnify the effect of TCP-target DoS attack.

B. ORGANIZATION OF LDoS ATTACKS
According to the organization of LDoS attacks, there is a few types of LDoS attacks, such as single source, distributed aggregation, synchronous and asynchronous attack.

1) SINGLE ATTACK SOURCE
LDoS attack with a single attack source is an LDoS attack launched by a single computer, which can only attack some of the bottleneck links with smaller bandwidth since its pulse rate is limited by the performance of the network card. Therefore, it is less harmful to network security in practice, but it is easy to evade detection.

2) DISTRIBUTED AGGREGATION
Distributed aggregation LDoS attacks refer to LDoS attacks launched by botnets. The botnet launches multiple distributed attacks by the control of the attacker, and the multi-path attack flows gather at the victim to form the final attack flow. Moreover, distributed botnets can also launch LDoS attacks on multiple victims simultaneously to enhance the damage to network services performance. Typical botnet for distributed LDoS attack is shown in Fig. 8 [1], [3].

a: PERIODIC AGGREGATION
LDoS attack is usually launched as a periodic pulse attack, and the attack pulses model is shown in Fig. 9 [3]. Periodic aggregation attack refers to the attacker command makes a botnet send the same periodic pulse attack flow to the victim at the same time, gathering at the victim to form the LDoS attack with higher pulse rate, to implement the LDoS attack on the backbone type of bottleneck with high bandwidth. This type of LDoS attack can be large-scale and serious, which is relatively simple to organize since it sends the same instructions to all zombie agents. However, plenty focuses from many detection and defense mechanisms on the periodic characteristics of LDoS attack make this type of attack easier to detect and defend in advance.

b: NON-PERIODIC AGGREGATION
LDoS attacks can take a non-periodic aggregation form (the attack pulses are shown in Fig. 10 [3]) for reducing the possibility of detection and defense. The attacker command makes each of the attacker in the botnet send aperiodic pulse by sending different orders to zombie agents, eventually forms a periodic attack after converging at the victim, and then the attack will harm the victim immediately. Therefore, the non-periodic LDoS attack can enhance the concealment of the attack while guarantee its harm. However, it improves the complexity of the attacker command sending the attack launching order, moreover, it cannot converge into a periodic attack if there are some zombies failed, and this brings vulnerability to attack itself.

3) SYNCHRONOUS ATTACK AND ASYNCHRONOUS ATTACK
In the LDoS attack method, the main parameters that distinguish between synchronous and asynchronous methods are the arrival interval of the attack pulse and the appearance rule of each attack pulse position. Therefore, the pulses generated according to different rules constitute a pulse sequence (a series of attack pulses), which has a certain period. Therefore, according to the different pulse period of LDoS...
FIGURE 10. Attack pulses model for non-periodic aggregation attack.

FIGURE 11. Synchronous LDoS attack.

FIGURE 12. Asynchronous LDoS attack.

attack, it can be divided into two forms, synchronous and asynchronous.

Synchronous LDoS attack is an ideal form of attack existing in theory, which is intended to cause the same attack effect every time the attack pulse reaches the victim, and the attack pulses model is shown in Fig. 11 [3].

It doesn’t matter whether the attack pulse of this kind of attack is in a periodic form or not. For example, in the reference [3], Luo and Chang proposed an RTO synchronization LDoS attack and an AIMD based LDoS attack. The RTO synchronization LDoS attack would expect the attack pulse to arrive at the retransmission time after the TCP’s timeout, so that the retransmitted TCP packets would always fail again, which makes the time of RTO longer each time and the spacing of the pulse need to increase as well. Nevertheless, this requires accurate access to the victim’s RTO time, and the random method of setting RTO time makes this attack almost invalid. AIMD based LDoS attack hope that the attack pulse will come back when the cwnd reduced to a certain proportion, so that the transmission rate of TCP will be reduced in proportion to the exponential rate. The problem is when the cwnd drops to a certain extent, the needed arrival interval of the attack pulse will be equal to or less than the duration of the attack pulse. In this way, the attack is no longer a pulse form but a flood form, which can no longer be called LDoS attack. In addition, this attack is too difficult to launch because the set model is too ideal.

The asynchronous attack makes the attack pulse reach the victim at the time of the attacker’s expectation by calculating the accurate and reasonable attack period based on the expectation of the attack, and the attack pulses model is shown in Fig. 12 [3].

This kind of attack is easy to be implemented, and the damage can be adjusted by adjusting the period, so most LDoS attacks are initiated in an asynchronous form.

C. LDoS ATTACK AGAINST THE ACTUAL SCENARIO

The targets of LDoS attack mainly include three network areas: terminal system, network node and border router, which are more vulnerable to LDoS attacks. As the terminal system is attacked, the lower quality of service will result in a reduction in the connection speed and resource usage of normal users; attacks on network nodes will directly affect bandwidth usage; attacks against border routers will cause slow queue updating and serious queue delays.

1) LDoS ATTACK AGAINST TERMINAL SYSTEM

In generally, LDoS attack against the terminal system reduces the flow of the sending terminal by exploiting the vulnerability in the protocol. For example, LDoS attacks based on TCP and LDoS attack based on application layer protocol are LDoS attacks against the terminal system. The first one aims at adaptive mechanism of TCP, which makes normal TCP packet loosen by exploiting periodic high-speed pulse attack flow, leading to ACK received the wrong sequence grouping and the congestion control algorithm reduced the transmission speed since the congestion occurred. The latter one leverages the persistent connection (KeepAlive) mechanism provided by the HTTP, which fills the server queue with invalid requests by making connection requests from the attacker to the Web server. This type of attack is more targeted, and its impact is small since it is only harmful to the provider of a service.

2) LDoS ATTACK AGAINST NETWORK NODE

The LDoS attack against network nodes is generally aimed at the router of one or some nodes in the network, which reduces the quality of the router’s queue management, to reduce the throughput of the router. For example, the RoQ attack is defined as the attack technology that prevents AQM from stabilizing its queue. RoQ attack destructs the steady state of the queue by periodically sending the attack pulse as well as it induces the packet loss of the node router through the attack pulse and sends the congestion notification to the sender. Then, the sender will adjust its sending rate after receiving the congestion notification, which causes to the router queue length, has a serious jitter and further breaks the stable state of the broken loop queue. Due to the severe
jitter of the queue and the low efficiency of queuing, the link capacity of the node cannot be fully utilized, and thus reduce the service performance of the link.

3) LDoS ATTACK AGAINST BORDER ROUTER
The LDoS attack against the border routing is generally decreasing the performance of the boundary router by updating the routing information of the border routers in each autonomous region repeatedly. Since router will send routing updates and exchange routing information when a connection interrupted or new constructed in inter-domain routing system, BGP-LDoS can cause many routing sessions into a state of repeated on and off in a short time, resulting in lots of routing updates by implementing TCP-targeted attack to carefully selected link through a lot of zombie nodes. When other peripheral BGP routers seriously consumed CPU computing resources in dealing with a lot of routing update messages, the speed of the routers process routing updates dropped. Moreover, the router processing speed will deteriorate further with the continuous update message, and routing update message will also occupy the router’s storage resources. This type of attack is contagious and has a very wide range of effects.

D. ATTACK EFFECT ESTIMATION
LDoS attack and FDoS (Flooding Denial of Service) attack are two different types of DoS attack. Although the average attack sending rate of LDoS attacks is smaller than FDoS, the LDoS attacks evolve the traditional DoS attack mode by more covert and more efficient periodically attack method. The attack efficiency has been greatly improved. For verifying the performance of LDoS attacks, experiments on the throughput and packet loss rate of TCP flows under LDoS attack are performed.

1) PERFORMANCE OF LDoS ATTACK
Initially, attack performance testing was conducted in an NS-2 environment [1]. Fig. 13 demonstrates the experimental topology and parameter configurations.

TABLE 3. Comparison of the throughputs under LDoS attack and FDoS attack.

| Attack type/sending rate | Throughputs without attack | Throughputs under attack |
|-------------------------|---------------------------|-------------------------|
| LDoS/3Mbps              | 14.2Mbps                  | 2.9Mbps                 |
| FDoS/3Mbps              | 14.2Mbps                  | 11.5Mbps                |
| FDoS/14Mbps             | 14.2Mbps                  | 1.6Mbps                 |

TABLE 4. Comparison of the average loss rate under LDoS attack and FDoS attack.

| Attack type/sending rate | loss rate without attack | loss rate under attack |
|-------------------------|--------------------------|------------------------|
| LDoS/3Mbps              | 1.03                     | 9.69                   |
| FDoS/3Mbps              | 1.03                     | 0.16                   |
| FDoS/14Mbps             | 1.03                     | 4.76                   |

The minRTO is set to 1 second, which is the default value and is the usual setting. The average TCP packet size is 1000 bytes, and the bottleneck link capacity is 15Mbps. Legitimate TCP flow is generated from TCP Sender to TCP Receiver. Attacker generates LDoS attack traffic by sending UDP packets, and the attack packet size is 50 bytes which is the minimal UDP packet size.

a: COMPARISON OF ATTACK EFFECTS BETWEEN LDoS AND FDoS
For comparing the attack effects between LDoS and FDoS, we design the experimental topology as shown in Fig. 13. The link between Router 1 and Router 2 is the bottleneck link. There are four TCP senders link to Router 1 and built four TCP connections through the bottleneck link. The version of TCP is CUBIC, which is the current default option in the Linux kernel. Firstly, we set the LDoS attack parameters as \( \{ L = 240\text{ms}, R = 15\text{Mbps}, T = 1.2s \} \). Secondly, we organize the FDoS attack in the same quantity. The sending rate is 3Mbps. Thirdly, we organize the FDoS attack and the sending rate of the attack is 14Mbps. The test result is shown in Table 3.

In Table 5 we can see that when the quantities of the attack flows are same, the LDoS will get a better attack effect than FDoS. The LDoS reduced the throughput of the bottleneck link from 15Mbps to 1Mbps. However, the FDoS in same quantity only reduced the throughput from 15Mbps to 12Mbps. If we want to get the same attack effect of the LDoS as above, we have to increase the sending rate of the FDoS attack from 3Mbps to 14Mbps. The average loss rates of the TCP flows under different attacks are increased, which is shown in Table 4.

It can be seen from Table 5 that the packet loss rate under normal network conditions in the experiment is 1.03%. As LDoS and FDoS attack the network at the same rate (3Mbps), the impact of LDoS attacks on the parameter of packet loss rate is much greater than FDoS. Even if the FDoS
The experiment results are demonstrated in Table 7.

When the link bottleneck is 15 Mbit / s, the common firewall for the PC, DDoS dedicated firewalls and DDoS firewalls each use three. Among them, the common firewall for the PC, DDoS dedicated firewall for the server. When the link bottleneck is 15 Mbit / s, the experiment results are demonstrated in Table 7.

In Table 8, the experimental results figure out that:

(i) For traditional FDoS attacks, both generic firewalls and DDoS-specific firewalls can correctly detect them.

(ii) For LDoS attacks, generic firewalls I, II and III can not detect a pulse width of 200 ms or 300 ms and single pulse amplitude of 3.3 Mbit / s or 10 Mbit / s.

(iii) Under the same testing conditions, three DDoS firewalls I, II and III can not detect LDoS attacks.

Reason of the above features is that existing firewalls generally detect DDoS according to the rule that when the number of packets per unit of time exceeds a certain threshold, then a DDoS attack is considered. However, LDoS attacks have a low rate as the number of packets per unit time is small, and so it can escape the detection of existing firewalls. These experimental results prove that the concealment of LDoS attacks is hard to find by existing detection methods, therefore, shows the importance of LDoS attack detection research.

### Table 5. Comparison of the throughputs of different TCP versions under LDoS attack.

| TCP version | Throughputs without attack | Throughputs under attack |
|-------------|---------------------------|--------------------------|
| CUBIC       | 14.3Mbps                  | 2.9Mbps                  |
| highspeed   | 14.1Mbps                  | 0.9Mbps                  |
| htcp        | 14.3Mbps                  | 1.4Mbps                  |
| reno        | 14.1Mbps                  | 1.1Mbps                  |
| vegas       | 14.0Mbps                  | 1.0Mbps                  |

### Table 6. Comparison of the loss rate of different TCP versions under LDoS attack.

| TCP version | loss rate without attack | loss rate under attack |
|-------------|--------------------------|------------------------|
| CUBIC       | 1.04                     | 9.69                   |
| highspeed   | 0.30                     | 11.52                  |
| htcp        | 1.08                     | 10.03                  |
| reno        | 0.28                     | 14.57                  |
| vegas       | 0.02                     | 12.67                  |

### 2) FIREWALL SENSITIVITY TEST - LDoS VERSUS FDoS

To verify the covertness of LDoS attacks, LDoS attacks are detected by a general firewall and a firewall dedicated to defense against DDoS attacks. In order to avoid unnecessary misunderstanding and controversy, the specific name and manufacturer of the experimental firewall will be hidden, and a number label will indicate the specific type of firewall. Universal firewalls and DDoS firewalls each use three. Among them, the common firewall for the PC, DDoS dedicated firewall for the server. When the link bottleneck is 15 Mbit / s, the experiment results are demonstrated in Table 7.

In Table 8, the experimental results figure out that:

| Reason of the above features is that existing firewalls generally detect DDoS according to the rule that when the number of packets per unit of time exceeds a certain threshold, then a DDoS attack is considered. However, LDoS attacks have a low rate as the number of packets per unit time is small, and so it can escape the detection of existing firewalls. These experimental results prove that the concealment of LDoS attacks is hard to find by existing detection methods, therefore, shows the importance of LDoS attack detection research.

### E. THE SUMMERY OF LDoS ATTACK

We summarize the various LDoS attacks in Table 8. These include the location of the attack, the target of the attack, the protocol vulnerabilities and mechanisms utilized, and the hazards of the attack. As can be seen from Table 8, most LDoS attacks are similar. For example, attacks are initiated from the Transmission layer. The targets are network nodes and links, and they exploit vulnerabilities in the TCP protocol.

### IV. DETECTION OF LOW-RATE DoS ATTACKS: TIME AND FREQUENCY DOMAIN

The traditional detection and prevention of LDoS attack are always difficult problems in the field of network security, which have not yet been resolved. LDoS attacks not only have common problems as DoS attacks, but also have some new difficulties in detecting and defending. LDoS attacks display many different features, such as the low average attack data flow rate, which causes less fluctuation in the system. Moreover, the distribution of attackers is more scattered, therefore, traditional detection methods are difficult to detect LDoS attacks. According to existing research results, we can divide most detection methods into three categories: feature detection, frequency domain and time domain. Feature detection must first establish a feature library with clear characteristics of attacks against known attacks. Once it is detected that the characteristic parameters of data and features in the library, it is judged as the attack occurred. Frequency domain

**W. Zhijun et al.: LDoS Attacks, Detection, Defense, and Challenges: Survey**
detection is based on the multiple parting characteristics of the network in frequency domain. Researches use Fourier transform and other frequency-domain transformation methods to observe the outliers in the frequency domain, to detect the LDoS attacks. The detection method in time domain uses autocorrelation, time backtracking and other algorithms to detect LDoS attacks by comparing with the trained sets.

A. DETECTION METHODS OF LDoS ATTACKS

Since the LDoS attacks were found, researchers have proposed many different attack methods according to the principle of such attacks, and have also done some researches for the detection and filtering prevention methods. But since the LDoS attack is still in its infancy, researchers have yet to put forward an effective defense scheme. We sum up the existing methods into three categories: feature detection, frequency domain and time domain detection methods. These three types basically contain all the methods that currently detect LDoS attacks.

1) DETECTION METHODS BASED ON FEATURES

Since the LDoS attack was proposed, researchers analyzed and summarized a lot about features of LDoS. Although LDoS attack is not easy to be observed, there are some obvious characteristics for LDoS attacks, for example, the low pulse strength. Attack cycle characteristics and the periodic characteristics are good characteristics for detection. The general process of feature-based detection algorithm is shown in the Fig. 14.

In Fig. 14, we collect one or more features corresponding to the feature library, such as traffic feature, router queue characteristics and other features. Then, different signal processing algorithms process these features. Finally, we set the appropriate criteria for classification of test results.

---

**TABLE 7.** Firewall test.

| Type          | Name | Object | Default rule of UDP number | Attack parameters | Detection result |
|---------------|------|--------|----------------------------|------------------|-----------------|
|               | I    | PC     | none                       | 200 3.3          | \(\checkmark\) \(\times\) |
| General firewall | II   | PC     | none                       | 300 10           | \(\checkmark\) \(\times\) |
|               | III  | PC     | none                       | 300 15           | \(\checkmark\) \(\times\) |
| DDoS firewall | I    | Server | 2000                       | 200 3.3          | \(\checkmark\) \(\times\) |
|               | II   | Server | 10000                      | 300 10           | \(\checkmark\) \(\times\) |
|               | III  | Server | 8000                       | 300 15           | \(\checkmark\) \(\times\) |

**TABLE 8.** Summary of LDoS attacks.

| Name of LDoS attack | Location          | Target            | Protocol | Vulnerabilities | Mechanism | Potency/Damage |
|---------------------|-------------------|-------------------|----------|-----------------|-----------|----------------|
| Shrew               | Transmission layer | Network node & Link | TCP      | Retransmission time out | Low/High |
| RTO-based PDoS      | Transmission layer | Network node & Link | TCP      | Retransmission time out | Low/ Medium |
| AIMD-based PDoS     | Transmission layer | Network node & Link | TCP      | Congestion control | Medium/ Medium |
| Link-saturation Shrew | Transmission layer | Network node & Link | TCP      | Retransmission time out & Congestion control | High/Low |
| Full-buffer Shrew    | Transmission layer | Network node & Link | TCP      | Retransmission time out & Congestion control | High/Low |
| RoQ                 | Network layer     | Network node      | AQM      | RED et. al      | High/Medium |
| LoRDAS              | Application layer | Terminal system   | HTTP     | KeepAlive       | High/High |
| ZMW                 | Application layer | Border router     | BGP & TCP| Updata & Retransmission time out | High/Medium |
| CXPST               | Application layer | Border router     | BGP & TCP| Updata & Retransmission time out | High/Medium |
W. Zhijun et al.: LDoS Attacks, Detection, Defense, and Challenges: Survey

FIGURE 14. Detection methods on feature.

a: DETECTION METHODS BASED ON TRAFFIC FEATURE
When the LDoS attack is initiated, the victim network will fluctuate frequently. At this time, the LDoS attack traffic will display abnormal multi-fractal features, which lays the foundation for determining LDoS attack traffic, so that legitimate network traffic and LDoS attack traffic can be correctly classified.

Network traffic measurements indicate that aggregated network traffic is multi-fractal. Researchers have developed simple mathematical models to reveal complex multifractal structures so that network traffic can be better described and analyzed. Although the LDoS attack traffic is small, changes in the multifractal characteristics of network traffic still exist. Therefore, Wu et al. studied the multifractal characteristics of small-scale network traffic caused by LDoS attacks [26], and proposed a multi-fractal trend analysis (MF-DFA) algorithm. Through wavelet analysis, the Hölder index is used to estimate the singularity and burstiness of network traffic under LDoS attack. They have tested the performance in the simulation platform and the test bench network, and the experimental results obtained are completely consistent with the theoretical analysis [19].

We proposed a method based on network traffic singularity [27]. The network traffic is reconstructed by wavelet transform, and the low frequency signal of LDoS attack is obtained. The detection window is obtained by Gauss wavelet convolution, and the Euclidean distance based on the mean of the detection window and the standard deviation is calculated to determine whether there is an LDoS attack. For the data judged as attack window, the attack time is determined according to the singularity theory of signal. Simulation results show that the detection success rate is 90.6%, which indicates that this proposed method can detect LDoS attacks effectively.

b: DETECTION METHODS BASED ON ROUTER QUEUE CHARACTERISTICS
Although detection method based on traffic flow characteristics can distinguish accurately LDoS attack flows and legitimate TCP traffic, if there are bursts for normal flow, the false positive rate for attacks will be high, such as streaming media on-demand RTSP protocol and VoIP business generated by the instantaneous burst flow. The principle of LDoS attacks is the use of TCP congestion control, so to achieve the effect of the attack. Attack must prepare a reasonable flow parameter only because of the end system into RTO and AIMD, and then RED queue feature is abnormal, so the attacker is not easy to counterfeit.

Professor HU proposed a kind of LDoS attack detection method based on the average length of buffer queue (Average Size of Packet based on Queue, ASPQ) [28]. He analysed the occupancy ratio of the attack packets in the queue and the relationship between the size and the effect of the attack by using the average queue length (ASPQ value), and then detected LDoS attacks based on the router.

Dr. ZHANG proposed a LDDoS attack detection and filtering method based on congestion participation [29], and proved the congestion participation in routers through data proving, which can detect and filter LDDoS attacks efficiently.

c: DETECTION METHODS BASED ON OTHER FEATURES
We proposed a joint feature-based LDoS attack detection method [30], which first extracted three internal characteristics of LDoS attack traffic. Then, established a BP neural net-based LDoS attack classifier, and finally combined three internal characteristics of LDoS attack into the input of BP neural network, and achieved the purpose of detecting LDoS attack through pre-set decision index. We use the LDoS attack traffic specific generation tool, test and verify the detection algorithm in the NS2 simulation platform and test-bed network environment. The experimental results indicate that the detection rate is 96.68% through hypothesis testing. The method of LDoS attack detection based on joint features is superior to single feature and has high computing efficiency.

2) DETECTION METHODS IN FREQUENCY DOMAIN
Feature detections need clear attack features. The method can match the right sample to detect attacks through features, but for the new type of attack feature emerging in an endless stream, false alarm rate of feature detection will be very high. Meantime, the characteristics of the detection method is easy
to be influenced by some external interference. Therefore, in order to solve these problems, some of the detection algorithms used by researchers have begun to correlate with the frequency domain in recent years. The approach of detecting LDoS attack through frequency domain has attracted more and more attention of researchers. This approach combines the technologies of signal processing and traffic data processing, among which the most typical is the classical signal detection theory and filtering theory, to effectively detect and filter the LDoS attack flows. So far, the researchers have proposed wavelet analysis, spectrum analysis and some other methods in frequency domain [31]. The general process of frequency-domain detection algorithm is shown in the Fig. 15.

In Fig. 15 we usually use traffic characteristics as the basis of frequency domain detection. The collected normal and abnormal traffic transformed by DFT are processed by signal processing to detect.

a: WAVELET ANALYSIS

Wavelet transform can simultaneously highlight the local characteristics of signals in frequency domain. Almost all signals can represent the signal according to some characteristics extracted from the original data [32], [33].

Based on the analysis of features in LDoS attack flow, HE et al. transformed the network traffic into fifth-order wavelet coefficients through wavelet multi-scale analysis. They proposed a detection system called detection system based on wavelet analysis (DSBWA) [19], which uses a trained BP neural network to comprehensively diagnose network traffic. If LDoS attack is determined, the successful detection can be achieved through systematically locating the malicious pulses.

b: SPECTRUM ANALYSIS

During LDoS attacks, TCP normal flow and abnormal flow attack periodically in transmission, and periodic and non-periodic signals in the frequency domain show different characteristics, therefore, can be used to detect these differences in the Fourier transform in the spectral domain.

In the frequency domain, Barford et al. [33] reveal the anomalous traffic by evaluating network traffic at different points. They proposed method adopts the concept of deviation scores for signal variations in the high and mid bands, in which abnormal traffic can effectively detected especially when a large amount of network traffic is aggregated.

Chen-Mou Cheng at al. proposed a method of identifying DoS attacks through spectral analysis [34]. The method uses the number of times the service packet arrives as a signal of a fixed length time interval to estimate the signal power spectral density, so implement the target of detecting LDoS attacks. This method reduces unnecessary slowdown or stop of normal traffic with a low false alarm rate.

Joel and Rishie [35] used discrete Fourier transform (DFT) detection and evaluated the effects in different attack scenarios. The results show that spectrum analysis is an effective method to detect abnormal traffic in the network. Through comparative analysis, they believe that detecting LDoS attacks is a more challenging task.

Chen and Hwang [36] and Chen et al. [37] proposed a novel cooperative defense method for periodic shrew attacks, which is implemented in the frequency domain. They studied a similar approach that detects LDoS attacks through collaborative detection and filtering. The method detects a shrew attack flows hidden in a legitimate TCP/UDP stream by performing spectrum analysis on a pre-stored average spectral feature template. This method does not increase the burden on the router when it is properly executed, and it can minimize the devastating impact of the attack flow on legitimate traffic. Chen et al. [37] also presented a new digital processing (DSP) method of detecting shrew attacks form legitimate traffic. The method can realize cooperative detection across multiple routers, and has stronger robustness and intelligence in network.

3) DETECTION METHODS IN TIME DOMAIN

The method of frequency domain detection usually uses the multifractal characteristics of the network to transform the network traffic characteristics to the frequency domain to detect the LDoS attack. Nevertheless, the Fourier transform is cumbersome and will increase the cost of the time. Therefore, some researchers have proposed a square method of time domain detection that is using the small signal model directly. We directly deal with the characteristics of LDoS attack in time domain. The advantage of this method is to simplify the detection process and reduce the detection time. The process of detecting LDoS attacks based on time domain is similar to frequency domain detection, but only removes the process of converting signals to frequency domain.
a: STATISTICAL ANALYSIS
Statistical analysis needs to establish a statistical model before detecting. If the actual distribution of statistical model and real data are consistent, the accurate rate of anomaly detection is very high. Hence, in actual application, it is very difficult to establish statistical models in the case of high dimensional data. We propose a detection method of LDoS attack based on the hidden Markov model [38]. First, a hidden Markov model is established for the network state. The observed value of the model is the result of the normalized cumulative power spectral density (NCPSD) method. By using the forward algorithm, the similarity of different observation values in this model is obtained as the basis for detection. The detection method is tested in NS-2. The experimental results indicate that the method can detect LDoS attacks effectively and has better detection performance compared with other methods. The test rate is 99.96% by hypothesis test.

b: SMALL SIGNAL CORRELATION
We proposed a method for detecting LDoS attacks based on small signal modeling, using small signal detection theory [39]. We use the method of eigenvalue estimation matrix (3000 sampling points to the number of data packets in statistics), which can be accurately detected and the calculated values of the periodic LDoS attack. The simulation results in NS-2 platform show that this method has high detection rate.

c: INFORMATION MEASUREMENT
The basic idea of information measurement is entropy and conditional entropy. The information entropy is used to determine the degree of disorder and discrete network system, Zhang and Qin proved that the entropy is very suitable for detecting DDoS attacks and it has high real-time and detection accuracy [40]. Wang et al. presented a DDoS attack detection approach based on entropy measurement [41]. Based on the characteristics of cloud environment, they can identify the attack target based on the priority location source and detect the DDoS attack initiated by cloud system. The distributed detection architecture is proposed, the detection agent is used to discover the suspected attack traffic of the potential attack source, and the detection server identifies the real attack stream of the DDoS attack. The effectiveness and feasibility of the presented approach are verified through theoretical and experimental analysis.

B. COMPARISON OF DETECTION METHODS
Studies have shown that there is a variety of detection and defense methods for LDoS attacks. Different methods are distributed in different fields and apply to different features. In order to express the features of each method clearly, we listed a form to compare detection methods respectively. Table 9 is the comparative analysis of detection methods.

Table 9 lists and summarizes three categories for identifying LDoS attacks. Comparative analysis shows that each method has certain advantages. The first category method is based on network traffic, which has good performance in detection speed. The second type is based on router queue, which has an advantage in the amount of detection data. The third type is based on network behaviors, which has the advantage of high detection accuracy due to the use of precise characteristics. Therefore, it is necessary to take advantage of each method.

It is well known that not all methods for detecting LDoS attacks are effective and perform well. Therefore, we put forward some improvement suggestions for some detection methods, as shown in Table 10.

In Table 10, we put forward suggestions for improvement of different detection methods. It is necessary to establish a perfect feature library for feature detection methods. However, it is a hard work to find LDoS features because of its concealed characteristics. We can make use of data mining algorithms, such as apriori methods to mine the support and confidence of each feature. Moreover, the support and confidence can be the basis for the establishment of a feature library. The common problem for detection method in frequency domain is high false positive rate. We can handle this problem by matching the sampling rate and the packet rate to make sure each detection point is one-to-one correspondence. The detection method in time domain is slightly worse than the other two methods in comprehensive performance. We can introduce a preprocessing system to assist the detection algorithm in time domain for further detection.

V. DEFENSE AGAINST LDoS ATTACKS: MEASURES AND COUNTERMEASURES
In terms of LDoS attack, detecting LDoS attack by the traditional detection method is very difficult, and the general filtering defense method will not completely filter the LDoS attack. At present, researchers are aiming at improving network protocol parameters and reintegrating network resources to defend LDoS attacks. However, there are shortcomings in current defense methods.

A. DEFENSE METHODS FOR LDoS ATTACKS
Research shows that it is hard to eliminate LDoS attacks flow through filter and other tools directly. It’s necessary to change control parameters of filters or find some new methods to defense LDoS attacks.

The classification of existing defense methods is shown in Fig. 16.

1) FILTERING OF LDoS ATTACKS
We presented a method of defending against LDoS attack based on comb filter [45]. This method filters LDoS attack traffic and TCP traffic from the time domain to the frequency domain, thereby filtering the LDoS attack flow. By analyzing the amplitude spectrum, it is found that the n/RTT point is the main concentration point of TCP traffic energy, so that the periodic parameters of the LDoS attack can be estimated. Therefore, an effective dressing filter is designed. The biggest
TABLE 9. Qualitative comparison of detection against LDoS attacks.

| Category                        | Detection method       | Applicability | False positive rate | Speed | Implementation complexity | Characteristics                      |
|--------------------------------|------------------------|---------------|---------------------|-------|--------------------------|--------------------------------------|
| Based on network traffic       | DSBWA [28]             | LDoS          | High                | High  | Low                      | Overall accuracy is not high         |
|                                | CD [22]                | LDoS & LDDoS  | High                | Medium| Low                      | Needs to preprocess data             |
|                                | Small signal correlation [29] | LDoS          | High                | Low   | Medium                   | Needs a known attack to compare      |
|                                | Statistical analysis [30] | LDoS & LDDoS  | High                | Medium| High                     | Difficult to implement               |
|                                | ASPQ [28]              | LDoS & LDDoS  | High                | Low   | Medium                   | Large amount of queue data           |
|                                | KPCA & ANN [31]        | LDoS & LDDoS  | High                | Low   | Medium                   | Accurate features but need to reduce dimensionality |
|                                | HAWK [42]              | LDoS          | Medium              | Medium| Low                      | Depends on threshold value selection |
|                                | ACK [43]               | LDoS          | High                | Low   | High                     | Depends on accurate feature          |
| Based on router queue          | Combined features [32] | LDoS & LDDoS  | High                | Low   | Medium                   | Using neural networks but need training data set |
|                                | Arrival of packets [44] | LDoS          | Medium              | Medium| Low                      | Depends on ports selection           |

TABLE 10. Improvements for detection methods.

| Type of detection method       | Suggestions for improvement                                      |
|--------------------------------|------------------------------------------------------------------|
| Feature based detection methods| Set up a complete set of features                                |
| Detection methods in frequency domain | The matching of the sampling rate and the packet rate            |
| Detection methods in time domain | Processing System                                                |

feature of this filter is the infinite impulse response (IIR), which can achieve the effect of filtering the LDoS attack flows in the frequency domain. This is because most of the normal TCP traffic energy located at the n/RTT point passes through the comb filter. The test results of the maximum pass rate indicator show that the value of this indicator of legal TCP traffic reaches 92.6%, while the value of the LDoS attack stream is only 81.4%. This proves the effectiveness of the method, and the impact of this method on legitimate TCP traffic is minimal.

2) IMPROVING NETWORK PARAMETER

Although the comb filter can prevent most LDoS flow, the legitimate TCP traffic will be removed by filtration. When being hit by LDoS attacks, the most common defense strategy of active queue management technology is to improve the router. Its purpose is to meet the characteristics of the data.
set against the discarded packet and try to protect the TCP data stream from LDoS attacks.

\textbf{a: DEFENSIVE MEASURES BY USING RED ALGORITHM}

The first and most common application of the AQM algorithm is the RED algorithm. AQM technology is a kind of router cache management technology to deal with the congestion control problems of Internet. It has the characteristics of active defense. AQM will calculate a certain probability to lose packets in advance, to reduce and avoid network congestion and improve service quality. The average queue length calculates the probability of using packet loss in the RED algorithm, and the probability is used for packet loss. However, an attacker can exploit the vulnerability of this algorithm to launch an LDoS attack. Therefore, it is possible to defend the LDoS attack in principle by improving the algorithm using RED algorithm. In reference [46], ZHANG et al. proposed an algorithm called Robust RED (RRED) to defend against LDoS attacks through improving the TCP throughput. The main idea of the RRED algorithm design is to detect and filter out the LDoS attack packets first, and then apply the regular RED algorithm to the router queue. Tests indicate that the RRED algorithm can almost completely retain the existence of LDoS attacks.

Kuzmanovic and Knightly [1] proposed methods to defend the LDoS attack by using AQM mechanism. These methods can monitor the change of data flow dramatically, effectively filtering mechanism of RTO attacks based on flow. However, the effect of the existing routing mechanism for AQM to adjust high-speed data is more obvious for long-term flows. If you change the AQM mechanism to the short-time high rate flow also plays a role in filtering, it may cause a large number of normal TCP data flow to be identified as illegal data flow together across the filter.

Chang et al. proposed a simple and efficient protection mechanism, which does not need to track and isolate shrew attackers and can effectively defend against shrew attacks, often referred to as shrew attack protection (SAP) [47]. It can identify TCP victims by monitoring the loss rate of port packet, giving priority to sending packets from the victim’s packet loss rate into the output queue. TCP dialogues can be shared by bandwidth. Under shrew attacks, SAP can prevent TCP dialog off, effectively making TCP traffic maintain a high throughput. Otherwise, SAP is a port-based terminal mechanism, but only a few attackers can find potential victims, making SAP easy to use on existing routers.

Most researchers will use an AQM mechanism in the router to deploy defense method for LDoS attacks and make corresponding changes to the AQM algorithm. When the LDoS attack launch, the router can feel congestion in the receive data stream and reduce the effect of the attack.

\textbf{b: RANDOMIZED RTO}

At present, the most typical LDoS attack form is based on the interval of RTO. LDoS attack sends attack packets periodically based on the RTO interval in the network protocol. The time interval between LDoS attacks is usually 3 to 4 RTO.

Therefore, we can design randomized RTO for LDoS attacks, so that LDoS is not easy to calculate RTO and achieve the effect of organization attack. This method can destroy the periodicity of RTO by randomization minRTO, which makes it impossible for attackers to predict the time of TCP sending packets accurately, and to send the attack data stream at the exact time, so that it can effectively defend against LDoS attacks.

Yang et al. put forward a similar view, and further verified it through simulation experiments [48]. By studying a real system, Efstathopoulos proved the effectiveness of using RTO randomization to achieve LDoS attack defense [49]. Although this method can reduce the attack to a certain extent, it will bring many negative effects, such as when there is no LDoS attack, the RTO randomization will reduce the performance of TCP. In addition, this method could not detect whether there is an LDoS attack. Moreover, the cost of this method is so high that it is not very feasible.

\section{3) REALLOCATION OF RESOURCES}

Liu et al. presented a real-time LDoS attack defense mechanism based on Q-learning [50]. This mechanism in terminal adaptive control system as the object of protection, periodically extracts the characteristic of attack parameters as the input parameters of the Q learning module, which is learned by Q for the optimal selection of the optimal defense, defense measures and end system dynamic resource allocation based on service execution. Defense measures dynamically adjust the service resources following current system status, to ensure the normal response rate of service request. Finally, the system uses colored Petri nets combined with BP neural network to defense attacks. The results demonstrate that the method has good real-time performance and the real-time response to the LDoS attacks, significantly improving the degree of automation of the defense system.

\section{B. COMPARISON OF DEFENSE METHODS}

Compared to the detection methods of LDoS attacks, defense measures for LDoS attacks are still in the research stage, and there are no large-scale deployment examples in actual scenarios. For finding out the differences among each defense method, a form to comparison of each approach in some aspects is listed as Table 11.

From the comparative analysis of the methods in Table 11, it can be concluded that each method has advantages in practical applications and also has certain problems. Therefore, the defense method for LDoS is still a problem worth studying. For achieving comprehensive defense, we can integrate the advantages of each method and avoid disadvantages to carry out the overall defense deployment.

\section{VI. CHALLENGES AND RECOMMENDATION}

Since it has been discovered in 2001, the threat of LDoS attacks has received increasing attention. There are many
TABLE I. Qualitative comparison of defense mechanisms against LDoS attacks.

| Category       | Defense method | Implementa- | Accuracy | Effectiveness | Weakness          |
|----------------|----------------|-------------|----------|---------------|------------------|
|                |                | tion       | Location |               |                  |
| Filter         | LIR filter     | Firewall,  | Low      | Impact on the legitimate TCP | Poor Effectiveness |
|                |                | Router     |          | traffic       |                  |
| RRED           | Router         | Good       |          | Depends on probing attack pulses | Can not defend distributed attacks |
| SAP            | Router         | Medium if the victims are monitored | Increase Bandwidth Utilization | Depends on port selection |
| Improving      | RED (1)        | Router     | TCP data flow may be filtered | Fast to filter illegal data flow | Hard to implement |
| routing        | RED-PD         | Router     | TCP data flow | Effective for LDoS attacks | Only Detecting |
| strategy       |                |            |          |               |                  |
| Randomized     | RED-PD         | Router     | TCP data flow | Could not defend LDoS attacks | Only Detecting |
| RTG            |                |            |          |               |                  |

A. CHALLENGES

Presently, three factories make the LDoS attack hard to detected and defense:

The protocol that LDoS use is legal. LDoS attacks generally use UDP or TCP packets. These two are the two most common types of packets in a normal network. LDoS and many normal UDP-based applications such as streaming media on demand RTSP and the instantaneous bursts generated by protocols and VoIP, etc. are very similar. Therefore, from the perspective of traffic behavior, LDoS attacks are basically no different from normal traffic, so it is impossible to distinguish between LDoS and normal traffic.

The average flow rate of LDoS is low. From the perspective of attack traffic, LDoS attack traffic is a periodic pulse traffic. In an attack cycle, only about one-fifth to one-sixth of the time there is attack traffic, so the average attack traffic is even lower than the average of normal traffic. From the perspective of attack mode, LDoS attacks can adopt a distributed attack mode. Wide-distributed attackers launch attack traffic aggregate at the end of victim router. As a result, the distribution of attack traffic is more dispersed throughout the network, and the average traffic is lower and more difficult to detect.

The LDoS attack is more intelligent. The intelligence of LDoS attacks is mainly manifested in its attack mode and attack rate. The attack modes of LDoS attacks are gradually diversified. In addition to the traditional forms of attacks, attacks in the form of full queues and in full-rate form are gradually evolved. From the perspective of attack rate, LDoS’s attack rate is no longer a simple fixed rate, and its attack rate changes with changes in the external network environment. In general, the degree of intelligence of LDoS attacks is increasing, and the detection of attacks is more complicated.

B. RECOMMENDATION

To detect and defend against LDoS attacks, following suggestions are proposed according to the current hotspot technology.

1) RECOMMENDATIONS ON DETECTION

a: SDN-BASED DETECTION

By analyzing the network traffic through the flow table, the software-defined network (SDN) can be effectively used to the application of detection and prevention of LDoS attacks [52].

b: DEEP LEARNING-BASED DETECTION

In order to achieve an accurate detection of LDoS attacks, deep learning can be used to design an accurate network traffic detection model and extract deep features of network traffic. The collected network traffic data is classified and dimensionally reconstructed, and the hidden features
of the LDoS attack are extracted as well. The extracted LDoS attack traffic features are input into the designed deep learning network traffic detection model to determine whether the input feature data packet belongs to the LDoS attack.

Although the deep learning network has a higher accuracy, it also has been found to be extremely vulnerable to adversary attacks. Compared with the SVM method and DNN method in traditional machine learning, the hybrid deep learning model has higher detection accuracy and lower false positive rate, which makes up for the existing LDoS attack detection methods. Because the input feature of the detection method is the flow table feature in the SDN switch and the self-built flow table feature, it is a lightweight detection method and can be directly deployed on SDN controller.

c: DETECTION BASED ON BIG DATA ANALYSIS
A huge amount of network traffic can be collected, stored, organized and classified by big data analysis. Moreover, the detection judgement and defense decision can be achieved by analyzing unknown patterns and correlations in network traffic, and grasping other relevant intrinsic information in network traffic.

2) RECOMMENDATIONS ON DEFENSE
There are several suggestions for the defense against LDoS attacks.

a: STATE DETECTION-BASED DEFENSE
The firewall based on the state detection technology can not only detect the data packet, but also detect the basic state information of the control communication, which includes the communication information, the communication state, the application state, and the information operability. The dynamic state table can be maintained by the state detection virtual machine, which can record all connection communication information and communication status, and complete detection and filtering of the data packet.

b: INTELLIGENT FILTERING BASED ON TRAFFIC DATA
Intelligent filtering technology refers to a dynamic filtering technology that covers all levels of the network. It can filter or dynamically filter at a specified network level according to the specific security needs of users. For example, the data packet is intercepted at the network layer, and it is handed over to a specific detection process for further detection if it belongs to a specific network application.

c: ID-BASED DATA NAMING DEFENSE
The identity and source of the data can be divided into a piece of data have a name by intelligently filtering through the name of date. Every data has a uniquely identified name, and the data name can be used to determine whether the data conforms to the security policy.

The existing research results are quite clear in the principle of LDoS attack and its utilization mechanism (such as TCP congestion control algorithm) and the configured parameters (Attack square wave duration and period and the TCP option of minRTO, etc.). Moreover, the introduction of the LDoS attack concept is in place and easy to understand. Therefore, it is very easy for us to reproduce some of the attack scenarios and obtain test results for attacks, detections, and defenses. However, for our research work, we face a double challenge.

(i) Accurately adjust the Mininet’s link parameters, such as the RTT and queue size of the bottleneck link, to simulate the various configurations of the LDoS attack theoretically. This work requires a lot of actual testing and analysis, and finally these parameters are fixed correctly.

(ii) Ensure that the TCP kernel parameters are configured correctly. In the specific configuration, we usually disable Reno for fast retransmissions. We have found through experimentation that it is useful to disable the fast retransmission option of TCP, although this may not be necessary.

Many of the research results used the Network Simulation Version 2 (NS2) simulator in their verification test, and no source code was released. Therefore, we must adjust some parameter settings frequently in the experiments to reproduce the excellent work of the former researchers. If the parameters are configured correctly, we find it easy to reproduce their work in Mininet.

VII. CONCLUSION
The detection and prevention methods of LDoS attack are important problems for network security. Moreover, the research of this kind of field is worth. According to our research results combined with existing research production, we can divide the detection types into three categories, which are feature detection methods, detection methods in frequency domain and time domain. In above sections, we give example of different types of detection methods, and analyze the advantages and disadvantages of different algorithms with the same index. Through the comparison of their respective advantages and disadvantages, various improvement suggestions are put forward.

The defense method for LDoS attacks is still at the stage of research. At present, researchers are aiming at LDoS attacks to improve network protocol parameters and reintegrate network resources to defend LDoS attacks. And we divided the defensive measures into three categories, which are filtering methods for LDoS attacks, improving network parameter and reallocation of resources and analyze the performance of defense methods from aspects of location, main advantages and weaknesses. By analyzing each defense method, we propose a comprehensive deployment of joint defense.

In this paper, firstly, we discuss about LDoS attacks and provide a classification of LDoS attacks, and we categorize the characteristics of each kind of LDoS attacks. Secondly, we explore the security vulnerabilities exploited by LDoS attacks, the organization of LDoS attacks, different scenarios LDoS attacks occur in, and the assessment of LDoS attacks effect. Thirdly, we present a discussion of detection and defense of LDoS attacks. Then, we give comparisons among different detecting methods and defense methods.
Although there have been many detection and defense methods, the existing methods still have many problems and challenges, which are needed for future researchers to overcome. Hence, we draw the conclusions as follow.

(i) Each detecting method has its own advantages and weaknesses. There common point is high positive rate. Therefore, we should consider which detection method is more suitable for deployment. Compared to other methods, the feature detection methods are more practical and easier to implement. It did not need to match the sending rate of packets, and could also achieve higher detection performance. In addition, features in feature libraries are not easy to counterfeit compared to traffic characteristics.

(ii) The defense measure is still at the stage of research. None of the defense methods can fully defend against LDoS attacks. It is very necessary to integrate the advantages and disadvantages of different methods and make overall deployment.

REFERENCES

[1] A. Kuzmanovic and E. Knightly, “Low-rate TCP-targeted denial of service attacks (the shrew vs. the mice and elephants),” in Proc. ACM SIGCOMM, Karlsruhe, Germany, Aug. 2003, pp. 75–80.

[2] M. Guirguis, A. Bestavros, and I. Matta, “Exploiting the transients of adaptation for RoQ attacks on Internet resources,” in Proc. 12th IEEE Int. Conf. Netw. Protocols (ICNP), Oct. 2004, pp. 184–195.

[3] X. P. Luo and R. K. Chang, “On a new class of pulsing denial-of-service attacks and the defense,” in Proc. Netw. Distrib. Syst. Secur. Symp., San Diego, CA, USA, 2005, pp. 1–19.

[4] Y. Wang, J. Ma, D. Lu, X. Lu, and L. Zhang, “From high-availability to resource consumption in the cloud,” in Proc. IEEE/ACM Workshop Network Secur. (ICITCS), Aug. 2015, pp. 133–139.

[5] Y. Zhang, Z. M. Mao, and W. Jia, “Low-rate TCP-targeted DoS attack disrupts Internet routing,” in Proc. IEEE ICDM Workshop Network Secur., Feb. 2006, pp. 1–14.

[6] M. Schuchard, A. Mohaisen, and D. F. Kune, “Losing control of the Internet: Using the data plane to attack the control plane,” in Proc. Netw. Distrib. Syst. Secur. Symp., San Diego, CA, USA, Feb. 2011, pp. 726–728.

[7] S. Ha, I. Rhee, and L. Xu, “CUBIC: A new TCP-friendly high-speed TCP variant,” ACM SIGOPS Operating Syst. Rev., vol. 42, no. 5, pp. 64–74, Jul. 2008.

[8] S. Floyd, High-Speed TCP for Large Congestion Windows, document RFC 3649, Dec. 2003.

[9] R. Shorten and D. Leith, “H-TCP: TCP for high-speed and long-distance networks,” in Proc. 2nd Int. Workshop Protocols Fast Long-Distance Netw., Argonne, IL, USA, Feb. 2004, pp. 1–16.

[10] Z. Wu, L. Zhang, and M. Yue, “Low-rate DoS attacks detection based on network multifractal,” IEEE Trans. Dependable Secure Comput., vol. 13, no. 5, pp. 559–567, Sep. 2016.

[11] X. Y. Zhang, Z. J. Wu, and M. Yue, “LDoS attacks detection approach based on singularity feature of network traffic,” Comput. Eng. Des., vol. 37, no. 1, pp. 50–54, 2016.

[12] J. Zhang, H. P. Hu, and B. Liu, “Detecting LDoS attack based on ASFPQ,” J. Commun., vol. 33, no. 5, pp. 79–84, 2012.

[13] C. W. Zhang, J. Y. Yin, and Z. P. Cai, “An approach of detecting distributed low-rate DoS attack based on the congestion participation rate,” Comput. Eng. Sci., vol. 32, no. 7, pp. 49–52, 2010.

[14] Z. J. Wu, J. A. Zhang, and M. Yue, “Approach of detecting low-rate DoS attack based on combined features,” J. Commun., vol. 38, no. 5, pp. 19–30, 2017.

[15] L. Li and G. Lee, “DDoS attack detection and wavelets,” IEEE Trans. Inf. Theory, vol. 5, no. 3, pp. 421–427, Mar. 2003.

[16] P. Chaovilat, A. Gangopadhyay, G. Karabatis, and Z. Chen, “Discrete wavelet transform-based time series analysis and mining,” ACM Comput. Surv., vol. 43, no. 2, pp. 1–37, Jan. 2011.

[17] Y. K. Kwok, R. Tripathi, and Y. Chen, “Halting anomalies with weighted choking to rescue well-behaved TCP sessions from shrew DoS attacks,” in Proc. 3rd Int. Conf. Netw. Mobile Comput. (ICCNMC), 2005, pp. 423–432.
[43] Z. J. Wu, Q. B. Pan, and M. Yue, “Detection method of LDoS attack based on ACK serial number step-length,” J. Commun., vol. 39, no. 7, pp. 139–147, 2018.

[44] C. Jin, H. Wang, and K. Shin, “Hop-count filtering: An effective defense against spoofed DoS traffic,” in Proc. ACM CCS, 2003, pp. 30–41.

[45] Z. Wu, M. Wang, C. Yan, and M. Yue, “Low-rate DoS attack flows filtering based on frequency spectral analysis,” China Commun., vol. 14, no. 6, pp. 98–112, 2017.

[46] C. Zhang, J. Yin, Z. Cai, and W. Chen, “RRED: Robust RED algorithm to counter low-rate denial-of-service attacks,” IEEE Commun. Lett., vol. 14, no. 5, pp. 489–491, May 2010.

[47] C.-W. Chang, S. Lee, B. Lin, and J. Wang, “The taming of the shrew: Mitigating low-rate TCP-targeted attack,” IEEE Trans. Netw. Service Manage., vol. 7, no. 1, pp. 1–13, Mar. 2010.

[48] G. Yang, M. Gerla, and M. Y. Sanadidi, “Defense against low-rate TCP-targeted denial-of-service attacks,” in Proc. 9th Int. Symp. Comput. Commun., Jun. 2004, pp. 345–350.

[49] P. Efstathopoulos, “Practical study of a defense against low-rate TCP-targeted DoS attack,” in Proc. Int. Conf. Internet Technol. Secured Trans. (ICITST), Nov. 2009, pp. 1–6.

[50] T. Liu, Y. X. He, and Q. Xiong, “A Q-learning based real-time mitigating mechanism against LDoS attack and its modeling and simulation with CPN,” J. Comput. Res. Develop., vol. 48, no. 3, pp. 432–439, 2011.

[51] Z. J. Wu, L. Liu, and M. Yue, “Detection method of LDoS attacks based on combination of ANN & KPCA,” J. Commun., vol. 39, no. 5, pp. 11–22, 2018.

[52] A. Mendiola, J. Astorga, E. Jacob, and M. Higuero, “A survey on the contributions of software-defined networking to traffic engineering,” IEEE Commun. Surveys Tuts., vol. 19, no. 2, pp. 918–953, 2nd Quart., 2017.

**WU ZHIJUN** received the B.S. and M.S. degrees in information processing from Xidian University, China, and the Ph.D. degree in cryptography from the Beijing University of Posts and Telecommunications, China. He was a Professor with the Department of Communication Engineering, Civil Aviation University of China. His research areas are denial-of-service attacks, and security in big data and cloud computing.

**LI WENJING** received the B.S. degree in Internet of Things engineering from Qufu Normal University, China. She is currently pursuing the master’s degree in network security with the Civil Aviation University of China. Her main research interests include denial-of-service attacks and security in SDN.

**LIU LIANG** received the B.S. degree in electronic information engineering from the Harbin Institute of Technology, China, and the M.S. degree in information security from the Civil Aviation University of China, China. His research area is denial-of-service attacks.

**YUE MENG** received the B.S. degree in electronic information engineering from the Hebei University of Science and Technology, China, and the M.S. degree in information security from the Civil Aviation University of China, China. He was a Lecturer with the Department of Communication Engineering, Civil Aviation University of China. His research area is denial-of-service attacks.

* * *