

Research and Survey of Low-rate Denial of Service Attacks

QIAO Zhu*, ZHANG Yizhi*, XIE Chuiyi**

* School of Electronics & Information Engineering, Liaoning University of Technology, China

** College of Mathematics and Information Science, ShaoGuan University, China

**Information Security Center, Beijing University of Posts and Telecommunications, China

gdxcy@163.com

Abstract—As a new breed of DoS(Denial of Service) attacks, LDoS (Low-rate DoS) attacks have attract attentions of scholars. The vulnerabilities of TCP(Transmission Control Protocol) and the principle of low-rate attacks are discussed. A variety of definitions and aliases of LDoS are listed. 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.

Keywords—Denial of Service, Low-rate DoS, Transmission Control Protocol, Shrew, RoQ

I. INTRODUCTION

DoS(Denial of Service) is the serious threat of current networks which could be aroused in an easy way but followed by an almost disaster. Being a typical DoS attacks, flooding DoS attacks has been deeply investigated and the corresponding detection systems have been built. However, a new breed of DoS attacks called as LDoS(Low-rate DoS) appears and begins to attract the scholars' attentions. The first observe of LDoS attacks came from the Internet2 Abilene backbone in 2001[1].

Aelksandar Kuzmanovic and Edward W. Knightly are the first scholars who investigate LDoS[2]. YU CHEN, KAI HWANG and YU-KWONG KWOK detected LDoS with the frequency-domain characteristics from the autocorrelation sequence of Internet traffic streams and proposed a new digital signal processing (DSP) approach[3]. Petros Efstathopoulos studied the results of the attack on a real system, and evaluated the effectiveness the of RTO(Retransmission Time Out randomization) in defending against low-rate DoS attacks, showing that the method can prevent a TCP(Transmission Control Protocol) flow from being throttled from attack traffic[4]. [5] proposed a simple protection mechanism, called SAP (Shrew Attack Protection), for defending against a LDoS attack. [6] proposed a mathematical model for the LDoS attack.

There are two important techniques to protect from LDoS. One is to improve TCP, and the other one is to find out the characteristics of LDoS attacks. Randomizing minRTO(Retransmission Time Out) is one of former methods which discussed in the first paper of LDoS[2]. G. Yang, M. Gerla, and M. Y. Sanadidi developed and validated an analytic

performance model on the throughput of randomized TCP[7]. [7] shows that randomization can effectively mitigate the impact of such DoS attacks while maintaining fairness and friendliness to other connections. [4] follows the results and test the mothod on a real system (Linux). [8] demonstrated empirically that BGP routing sessions on the current commercial routers are susceptible to low-rate attacks launched remotely, leading to session resets and delayed routing convergence, seriously impacting routing stability and network reachability.

The hackers attack the weakness of TCP in LDoS. Periodic and high-speed packets' spurt occupies the networks link in short time and reduces the utilization of link. With low average flow transmission rate, LDoS is difficult to be detected therefore causing serious harm to networks. It is very necessary to give LDoS a survey and a research before it causes a disaster in Networks, which is the work of the paper.

This paper is organized as follows. Section 2 introduces the principle of LDoS attack and the vulnerabilities of TCP. A variety of definitions and aliases of LDoS are listed in section 3. The harm of LDoS is summarized in section 4 and the simulation of attacks is investigated in the last section.

II. HOW LDoS ATTACKS WORKS

Generally all attacks against Networks adaptation mechanisms could be called low-rate DoS or Low-rate DDoS(Distributed DoS); especially the most important case is those against congestion control of Transmission Control Protocol. Congestion control algorithm varies the packets' transmission rate with the congestion degree of the link in order to reduce link congestion. The increment of packets' transmission rate happens when networks link is vacant; on the contrary few packets are sent into the crowded link. It is no doubt that congestion control mechanism could improve the performance of system; however, it also provides hackers opportunities to arose a new attack such as low-rate DoS. Since the sender will reduce the packets transmission rate when the networks link being congested, low-rate DoS attacker sends high speed but short time packets flow to cheat system that networks link are being occupied. As the legal senders accept wrong congestion messages from the receiver and reduce the number of sending packets, the system

performance declines. This kind of attack is defined as low-rate DoS. Short-time packets spurt can occupy the link suddenly and avoid to be detected by current intrusion defense system for low average packets' speed.

TCP congestion control operates on two timescales[2]. On smaller timescales of round trip times (RTT), typically 10's to 100's of msec, TCP performs additive-increase multiplicative-decrease (AIMD) control with the objective of having each flow transmit at the fair rate of its bottleneck link. At times of severe congestion in which multiple losses occur, TCP operates on longer timescales of Retransmission Time Out (RTO).

In order to keep balance between transmitting packets and avoiding congestion, the windows with alterable length are used to control traffic. Receiver window(rwnd) is set the current value depending on the receiver memory capacity and sent to the sender in the head of TCP packets.

LDoS attacks flow is shown in Figure 1 in which the attacker transmits periodic and square bursts[11]. A successful LDoS attack will have rate large enough to induce loss, and duration of attack should be long enough to induce congestion but short enough to avoid detection.

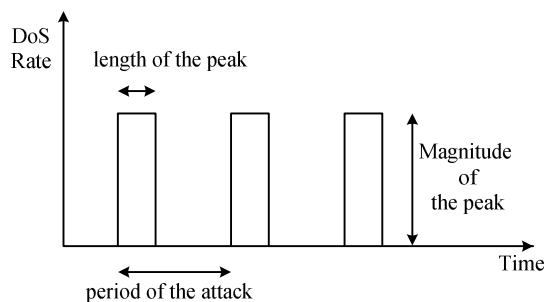


Figure 1. Periodic and high-speed attack spurt

III. ALIASES OF LDoS ATTACKS

Being a new-breed attacks, low-rate DoS attacks are given different names those are listed as follows.

A. Shrew Attack

In 2003, low-rate DDoS attack got its initial name, shrew attack, given by Aleksandar Kuzmanovic and Edward W. Knightly[2]. A shrew is a small but aggressive mammal that ferociously attacks and kills much larger animals with a venomous bite. LDoS attacks attempt to deny bandwidth to TCP flows while sending at sufficiently low average rate to elude detection by counter-DoS mechanisms. LDoS attacks could hurt Networks just like shrew attacks the elephants, so "shrew" is a visual name for LDoS attack.

B. Pulsing DoS Attacks

Xiapu Luo and Rocky K. C. Chang named low-rate DoS attacks as Pulsing Denial-of-Service (PDoS) attacks[11]. A PDoS attacker generates a sequence of false congestion signals to a TCP sender using attack pulses, so that the sender's cwnd is constrained to a low value. Therefore, that could seriously degrade the throughput of TCP flows.

C. Reduction of Quality Attacks

LDoS attacks are termed as one of important examples of Reduction of Quality[10]. RoQ is an attack that exploits system dynamics—i.e., the characteristics of a system's transient behavior as opposed to its limited steady-state capacity—to achieve the adversarial goals. In particular, a determined adversary could bleed a system's capacity or significantly reduce service quality by subjecting the system to a fairly low-intensity (but well orchestrated and timed) request stream that causes the system to become very inefficient, or unstable. LDoS attack is one of RoQ attacks.

D. Low-Rate DoS Attacks

Low-rate DoS attacks are the most general term for shrew attacks. Generally, LDoS is one of low-rate attacks.

E. LDDoS

As an abbreviation for low-rate distributed DoS, LDDoS are widely used in most Chinese paper.

IV. REASONS TO INVESTIGATE LOW-RATE DOS ATTACKS

In 2001, low-rate DoS attacks are detected by Asta Networks[1]. Reliable report of low-rate DoS attacks in China appears in 2004 when www.qq.com was attacked by low-rate DoS. Compared with traditional DDoS attacks, it is more difficult to detect low-rate DoS attack for its low average speed. The detection algorithms for flooding DoS attacks will not work for low-rate DoS attacks.

Being easy to implement with low cost, DoS attacks are always one of the most important threats for Networks' securities. With all attentions to flooding DoS attacks, it is very possible that low-rate DoS attacks will be the main attack in the future.

A. Difficult to be detected

Low average packets' speed is the main reason that low-rate DoS attacks are easy to escape from detection. Common to traditional DoS attacks is a large number of compromised machines or agents involved in the attack and a "sledgehammer" approach of high-rate transmission of packets towards the attacked node. While potentially quite harmful, the high-rate nature of such attacks presents a statistical anomaly to network monitors such that the attack can potentially be detected, the attacker identified, and the effects of the attack mitigated[2]. However, the purpose of low-rate DoS attacks is to break the balance of networks' link rather than to occupy the link. Only a high speed packets' spurt could serve the purpose. When the high speed spurts are short enough, the average packets' speed will be so low that the general IDS for flooding DoS attacks can't work.

B. Lower cost for hackers

If hackers want to be succeeding in flooding attacks, they had to drive Zombies to send out continual packet flows. However, for hackers of low-rate DoS attacks, sending out much shorter high speed packet flows could have the same

consequence. For flooding DoS attacks, distributed attacks are necessary; on the contrary, a single node could harm the networks in low-rate DoS attacks. Being lower cost for the same hazard, low-rate DoS attacks are “charming” for hackers.

C. Difficult to be found

When the victim is attacked by flooding attacks, the link of networks is occupied and the server is extraordinary busy. Low-rate DoS attacks cheat the nodes in the networks with busy signal and force the system to adjust its state, and therefore the link is relatively empty. Since server is idle when attacks work, the networks may be attacked for a long time without awareness.

V. SIMULATION OF LOW-RATE DOS ATTACKS

Figure 2 depicts the experimental setup that could be used for the simulation of low-rate DoS attacks[10]. The Internet experiments consists of a router (R), a local content server (S0), three client machines(C1, C2, and C3), a source of attack traffic (As) and a sink of attack traffic (Ak). The router’s server-side interface is connected to a 100Mbps switch that connects the whole setup to the Internet, the content server machine (S0) and the attack source (As). The router’s client-side interface is connected to another 100 Mbps switch that connects it to the local subnet where client machines (C1, C2, and C3) and attack sink(Ak) reside. The network interface cards on all machines run at 100 Mbps except for the router’s client-side interface, representing the bottleneck link, which runs at 10 Mbps.

Attack traffic is sent from As(Attack source) to Ak(Attack sink) with 1s as period and 300ms as peak length. Periodic attack spurt is shown in Figure 3. Normal packets flows with attack flows compose input for Router(R) which is shown in Figure 4. Since low-rate DoS flows are periods, it is difficult to detect attack in time domain. In frequency domain, low-rate attack flows occupy more in low-frequency which is represented in Figure 5 and 6. Figure 6 is the exaggeration of Figure 5 in low-frequency. Table 1 lists the parameters monitored in router(R) when it is attacked by LDoS packets shown in Figure 3.

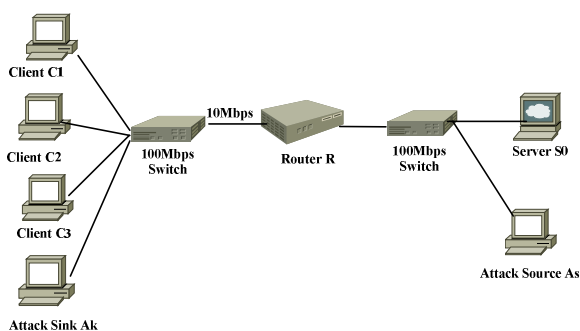


Figure 2. Experimental Setup for Simulation

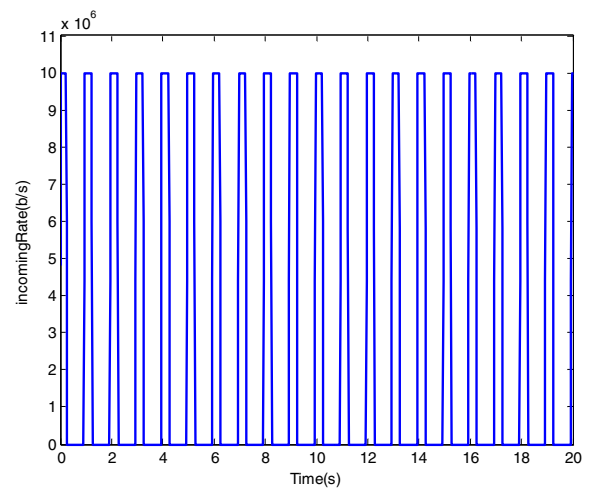


Figure 3. Periodic LDoS Packets Flows

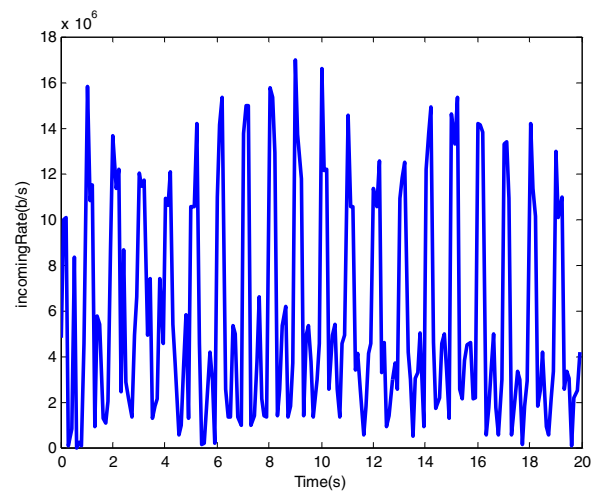


Figure 4. Incoming Flows with LDoS Packets

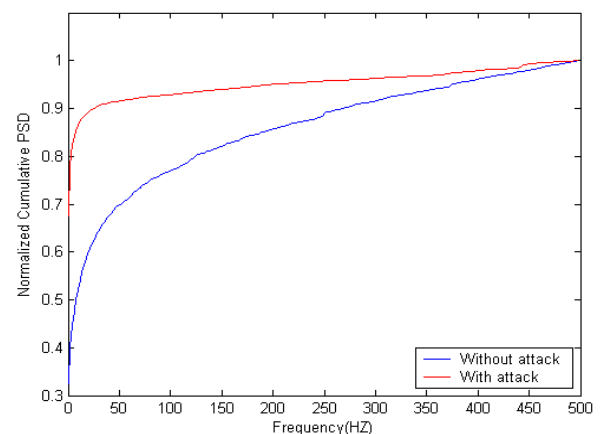


Figure 5. Normalized Cumulative PSD

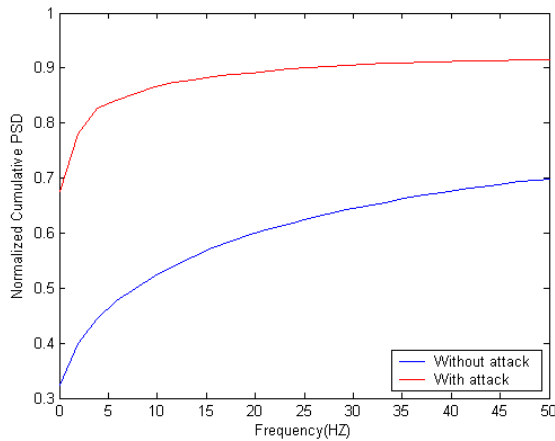


Figure 6. Normalized Cumulative PSD in Low Frequency

TABLE 1. PARAMETERS FOR ROUTER

Parameters	Value
Period of the Attack	1s
Length of the Peak	0.3s
Channel Utilization Ratio	0.7428
Packet Loss Ratio	0.1867
Incoming Packets' Number	750,989
Average Congestion Window	18.7496
ACKs' Number	221,130

VI. CONCLUSIONS

Research about LDoS attacks is still in laboratories. The mode of DoS is becoming various. Since LDoS could harm networks with low cost for hackers, it is kind of danger for Internet if there are no protection schemes. It is gratified that LDoS has attracted enough attentions. Practical detection solutions for LDoS are expectative.

REFERENCES

- [1] Michelle Delio. New Breed of Attack Zombies Lurk[OL]. <http://www.wired.com/science/discoveries/news/2001/05/43697:wired>, 2001.
- [2] Aleksandar Kuzmanovic and Edward W. Knightly. Low-Rate TCP - Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants)[C]// SIGCOMM'03, Karlsruhe, Germany, August 2003:75-87.
- [3] YU CHEN, KAI HWANG, and YU-KWONG KWOK. Collaborative Defense against Periodic Shrew DDoS Attacks in Frequency Domain[J]// ACM Transactions on Information and System Security (TISSEC) on May 3, 2005:1-30.
- [4] Petros Efstathopoulos. Practical Study of a Defense Against Low-Rate TCP-Targeted DoS Attack[J]// Internet Technology and Secured Transactions, 2009. London:ICITST, 2009:1-6.
- [5] Chia-Wei Chang, Seungjoon Lee, Bill Lin and Jia Wang. The Taming of The Shrew: Mitigating Low-Rate TCP-Targeted Attack[C]// 2009 29th IEEE International Conference on Distributed Computing Systems, Montreal, Quebec, Canada, 2009:137-145.
- [6] Gabriel Maciá-Fernández, Jesús E. Díaz-Verdejo, and Pedro García-Teodoro. Mathematical Model for Low-Rate DoS Attacks Against Application Servers[J]// IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 4, NO. 3, SEPTEMBER 2009:519-530.
- [7] G. Yang, M. Gerla, and M. Y. Sanadidi. Defense against lowrate tcp-targeted denial-of-service attacks[C]// ISCC '04: Proceedings of the Ninth International Symposium on Computers and Communications 2004 Volume 2 (ISCC'04), Washington, DC, USA, 2004:345-350.
- [8] ZHANG Y, MAO Z M, WANG J. Low-rate tcp-targeted dos attack disrupts internet routing[C]// Proc 14th Annual Network & Distributed System Security Symposium (NDSS'07). San Diego, CA, USA, 2007:1-15.
- [9] LUO, X. and CHANG, R. K. C. On a New Class of Pulsing Denial-of-Service Attacks and the Defense[C]// Network and Distributed System Security Symposium (NDSS'05), San Diego, CA, February 2005:1-19.
- [10] Mina Guirguis, Azer Bestavros, Ibrahim Matta. Exploiting the Transients of Adaptation for RoQ Attacks on Internet Resources[C]// Proceedings of the 12th IEEE International Conference on Network Protocols (ICNP'04), Oct. 2004 : 184 -195.
- [11] Aleksandar Kuzmanovic and Edward W. Knightly. Low-Rate TCP-Targeted Denial of Service Attacks and Counter Strategies[J]// IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 14, NO. 4, AUGUST 2006:683-697.