Journal of Computer Science 7 (8): 1218-1223, 2011
ISSN 1549-3636

Flooding Distributed Denial of Service Attacks-A Review

Khadijah Wan Mohd Ghazali and Rosilah Hassan
Department of Computer Science, Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia

Abstract: Problem statement: Flaws either in users' implementation of a network or in the standard specification of protocols has resulted in gaps that allow various kinds of network attack to be launched. Of the kinds of network attacks, denial-of-service flood attacks have caused the most severe impact. **Approach:** This study reviews recent researches on flood attacks and their mitigation, classifying such attacks as either high-rate flood or low-rate flood. Finally, the attacks are compared against criteria related to their characteristics, methods and impacts. **Results:** Denial-of-service flood attacks vary in their rates, traffic, targets, goals and impacts. However, they have general similarities that are the methods used are flooding and the main purpose is to achieve denial of service to the target. **Conclusion/Recommendations:** Mitigation of the denial-of-service flood attacks must correspond to the attack rates, traffic, targets, goals and impacts in order to achieve effective solution.

Key words: Denial of service, high-rate flood, low-rate flood, Distributed Denial of Service (DDoS), flood attacks, International Telecommunication Union's (ITU), Time-Out (RTO), Active Queue Management (AQM), UDP flood attack

INTRODUCTION

Flooding distributed denial of service attacks are the attacks launched by multiple attackers through the action of flooding, i.e. sending traffics in a quantity that is able to bring a network or a service down. Distributed denial of service (DDoS) flood attacks have been among the most frequently occurring attacks and badly threaten the reliability and usability of the services of the Internet. Hence, DDoS flood attacks (hereafter flood attacks) present severe threats to individuals, business organizations and even political entities such as a country. Reported impacts of DDoS floods include disgruntled customers, losses of business profits, disruption of critical infrastructures such as train operations and Internet disconnection of a country from the outside world.

The problem of flood attacks has been studied extensively in order to anticipate new attacks and to solve problems caused by the attacks. Studies of flood attacks also reveal that attacks are caused not only by vulnerabilities in network implementation, but also by flaws in protocol specifications and in the Internet system architecture. This research triggers even more research on improvements and innovations to the current network mechanisms in order to prevent flood attacks.

This study reviews recent publications on flood attack research. Flood attacks are categorized into high rate flood and low rate flood. This study is organized as follows: Introduction introduces the topic and important terms used in this study. Result and discussions reviews and compares high rate flood attacks and low rate flood attacks, respectively. Conclusion concludes the study.

MATERIALS AND METHODS

Distributed denial of service: The most direct definition of DoS comes from International Telecommunication Union's (ITU) recommendation X.800as: "The prevention of authorized access to resources or the delaying of time-critical operations" (ITU, 1991).

In the context of information systems, a DoS attack happens when an attacker explicitly attempts to prevent a service from being used by its legitimate users through many ways including by flooding a network with useless traffic to prevent legitimate network traffic (CERT, 1997). Among the area affected by DoS attacks are electronic information systems (Curran and Nichols 2005) and wireless sensor network (Hanapi *et al*., 2009).

A DoS victim will be more affected by the attack if the amount of flood traffic is bigger. An attacker achieves this through launching the distributed DoS attack. DDoS attack is a DoS attack that employs multiple attacking entities to achieve denial of service at the victim site (Jelena and Reiher, 2004), called zombies (Xia, Lu and Tang, 2010), bots (Michael *et al*., 2010), or slaves (Safa *et al*., 2008).

Corresponding author: Khadijah Wan Mohd Ghazali, Department of Computer Science, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia

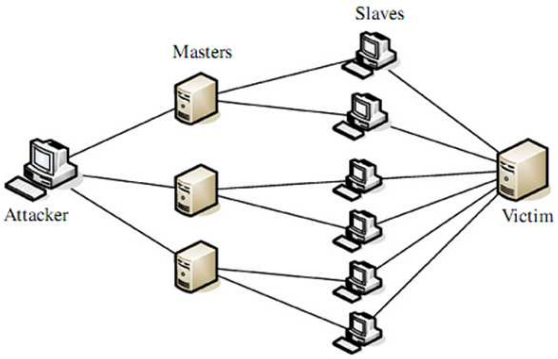

Fig. 1: Distributed denial of service attack

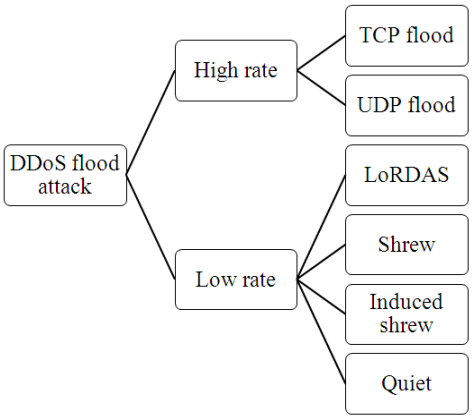

Fig. 2: Classification of DDoS flood attack

The zombies, bots or slaves are multiple hosts, which may be hundreds or thousands of Internet-connected computers located anywhere in the world. The employed army have earlier been compromised or commandeered by the attacker (master) to direct massive traffic to overwhelm the victim without their own awareness (Li *et al*., 2009), (Michael *et al*., 2010). Figure 1 illustrates the DDoS flood attack.

A DDoS flood hence is launched to deny legitimate users or significantly degrade the performance of service rather than breaking into the victim's site (Li, 2006).

RESULT AND DISCUSSION

Flood attack: From the introduction, it is known that flooding is the method used in order to launch a DDoS attack. The distributed nature of the Internet and other distributed systems such as openness, resource sharing and accessibility gives unfair advantages to the attacker (Li *et al*., 2009). As the Internet servers process all queries without being able to recognize bad clients from good clients from the request alone, the victim will waste its resources by processing the false requests sent by the army of attackers until it gets overwhelmed (Michael *et al*., 2010). The attack process is a relatively simple, yet very powerful technique to attack the Internet resources (Xia *et al*., 2010).

Although it seems that bigger amount of flood will cause more severe impact to the victim, the more sophisticated attackers have devised other flooding techniques which require smaller amount of flood traffics. These flooding techniques are known as low rate flooding. Due to this, this article classifies DDoS flooding as high rate flood attack and low rate flood attack as illustrated in Figure 2 and further elaborated in the following topics.

High rate flood attacks: Originally, flood attacks are high rate flood. This is accomplished by generating traffics from many machines, which may number thousands, distributed all over the world. Bombards of the flood packets from the attackers will overwhelm the target hence degrading its performance to the extent of rendering it unusable.

The high rate flood attacks reviewed in this study are the UDP attacks and TCP attacks. They are categorized as high rate flood attacks because the attacks are launched by flooding a massive amount of TCP or UDP datagrams to overwhelm the victim.

Li *et al*. (2008), quantitative behaviors of flood attacks under different protocols and intensities were studied through simulations using ns2. Quantitative behavior of the attacks become the focus in (Li *et al*., 2008) in order to describe the attacks quantitatively due to the scarcity of traffic data of the real attack events. The reason is that in many events of attacks, they will only be reported after the target machines are already overwhelmed and traffic data is lost.

The study observed that both types of TCP and UDP attacks carried out did not affect UDP clients but were able to cause TCP clients to drop legitimate packets.

The connection-oriented nature of the TCP clients means the receiving end will inform the transmission node to reduce its transmission rate if it exceeds its receiving ability. This makes the TCP clients to be more vulnerable to bandwidth attacks compared to UDP clients.

While UDP-type attacks aim at consuming the link bandwidth, the TCP-type attacks are usually launched to exhaust resources at the victim site. Under the same attack intensity, UDP attacks are more severe in terms of its ability to cause more degradation of legitimate traffics (Mirkovic *et al*., 2009), (Li *et al*., 2008). However, TCP attacks are more common because 80% of Internet traffic is based on TCP (Maciá-Fernández,

Díaz-Verdejo and García-Teodoro, 2009). Hence, more than 90% of DoS attacks exploit the TCP (Chen and He, 2008), (Yu *et al*., 2008).

Low rate flood attacks: Contrary to the high rate flood, low rate flood uses carefully crafted attack packets. The attack traffic rate is adjusted in order to make them undetected by the traditional flood detector which regards high rate of incoming traffic as attack.

Four low rate flood attacks are reviewed in this study: Low rate DoS attack against application servers (LoRDAS) (Maciá-Fernández *et al*., 2009), Shrew attack (Chang *et al*., 2009), Induced-shrew attack (Kumar *et al*., 2009) and Quiet attack (Shevtekar and Ansari, 2009).

Low Rate DoS attack against Application Servers (LoRDAS): LoRDAS (Maciá-Fernández *et al*., 2009) is an evolution of low rate DoS attack against iterative servers which extends its ability against concurrent systems. Taking advantage of the capacity of application servers, the attack traffic is intelligently sent in order to make the server busy attending the requests of the attacker, hence reducing its ability to attend to legitimate clients' requests.

This attack exploits the servers' capacity to forecast the instance at which the responses to incoming requests for a given service occur.

Shrew attack: Shrew attack (Aleksandra and Knightly, 2003) is designed to stealthily deny bandwidth of a TCP flow. An attack burst, which is a short pulse of high intensity traffic, gives illusion to TCP that the link is highly congested. The target router buffer is filled up; causing packet drops (Kumar *et al*., 2009). If within a window of transmitted packet a certain amount of packets are dropped, the transmission is suspended for a Retransmission Time-Out (RTO) period (Fall and Floyd, 1996). After the RTO expires, the next retransmission however will encounter another attack bursts as the Shrew attack interval is synchronized to the RTO value; causing another drop. This will happen continuously in a successful Shrew attack until the throughput is reduced to almost zero or the session is closed or reset.

The strength of the Shrew attack is the rate of the attack flow is low enough that it can escape detection by traditional DoS detectors. As for the attack time interval, it can be easily synchronized to the RTO of the TCP flow because most TCP implementations use fixed minimum RTO value (Chang *et al*., 2009), (Kumar *et al*., 2009).

Among the works proposed to mitigate the Shrew attacks are using Active Queue Management (AQM) (Aleksandra and Knightly, 2003), taking drop history of each flow into account (Mahajan *et al*., 2001), randomizing the fixed minimum RTO in TCP parameter in to make the synchronized attack more difficult, router-based detection using auto-correlation, fair resource allocation, detection at edge routers, halting anomaly with weighted choking, frequency domain spectrum analysis, wavelet-based approach, Shrew attack protection techniques based on signal analysis (Yu, Kai and Yu-Kwong, 2005), (Xiapu and Chang, 2005) and simple priority-tagging filtering mechanism (Chang *et al*., 2009).

Induced-shrew attack: Unlike the Shrew attack in which the attacker sends direct flood, the Induced-shrew attacker, as a master, controls a remote host, as a slave, to be the source for launching low rate flood attacks. The slaved remote host must be a TCP sender such as the Internet web and ftp servers (Kumar *et al*., 2009).

The attack is made possible by the shortcomings in the standard of TCP congestion control process in which it is the TCP receiver who controls the data transmission rate and pattern, yet lack of a mechanism to ensure that the receiver obeys the standard.

To launch the attack, an attacker establishes a connection with a slave e.g., a web server and initiates, e.g., a file download through the normal three-way handshake. After receiving the first data packet, the attacker (TCP receiver) starts sending optimistic ACKs to the slave (TCP sender). Optimistic ACK is a mechanism done by a greedy receiver to extract data from the sender faster than a standard receiver. In optimistic ACKing, the receiver sends ACK to data which the sender is expected to send in response to its previous ACKs. The receiver sends a series of ACKs in which the ACK number of successive ACK packets is incremented. The overall traffic is maintained low by sending the ACKs in batches with high inter-batch gap. The optimistic ACKing done by the attacker made the response traffic from the web server will flood its Internet access router with low rate flood. As a TCP transmission is controlled by the receiver, the attacker as the receiver now controls the sender as the attack slave. The TCP sender starts, stops and change transmission rate as instructed by the attacker.

To mitigate the Induced-shrew attack, RTO randomization can also be used, as applicable to Shrew (Kumar *et al*., 2009). Other proposals include a challenge-response mechanism by the TCP sender to the TCP receiver to validate incoming ACKs (Savage *et al*., 1999) and the cumulative nonce scheme (Kumar *et al*., 2009).

Table 1: Comparison of flooding DDoS attacks

Attack name	UDP flood	TCP flood	LoRDAS	Shrew	Induced-shrew	Quiet
Attack rate	High	High	Low	Low	Low	Low
Attack traffic	UDP flow	TCP flow	No info	TCP flow	Optimistic ACK packets	Short-lived TCP flows
Attack target	UDP or TCP clients	UDP or TCP clients	Application servers	Routers in TCP flows	Internet access routers	Routers in TCP flows
Attack goal	Exhaust resources at target machine	Consume bandwidth	DoS: reduce availability of servers to serve legitimate users	Deny bandwidth to TCP flows, close session	DoS at Internet access routers	Reduce throughput

Quiet attack: The Quiet attack (Shevtekar and Ansari, 2009) is a stealthy DDoS attack that can significantly reduce the throughput of a TCP flow. It uses botnets to launch short-lived TCP flows disguised as legitimate traffics. As the short-lived TCP flows are injected persistently undetected as attack, the victim ISP is made to believe that the routers are in a real congestion. Like the Induced-shrew, the Quiet attack also originates from the underlying shortfall in the TCP specification, specifically the end to end window flow control.

The Quiet attack is executed as follows:

- Reconnaissance phase: decide a botnet, a target router, web servers and a network feedback mechanism
- Execution phase: a set of bots are instructed to request web pages from web servers at an interval T, a random number between 0-1s
- Using network feedback control, the attacker gathers network feedback from the target router at every threshold (e.g., more than 1Kbps in 5 sec) to add more attack traffic

Experiments in (Shevtekar and Ansari, 2009) shows that the Quiet attack cannot be mitigated by mechanisms used to mitigate Shrew, Reduction of Quality, TCP Vs TCP, typical DDoS, UDP flood, or ICMP flood; due to the different properties of the attack (See the next topic for comparisons). Hence, botnet mitigation such as better CAPTCHAs is suggested as the defense strategy for the attack.

Comparison between attacks: The six attacks introduced above are compared in Table 1 above in terms of attack rate, attack traffic, attack target, attack goal and attack impact.

Attack rates: The attack rates are categorized into two. UDP flood and TCP flood are high-rate flood attacks, whereas other attacks reviewed in this study are low-rate flood attacks.

Attack traffics: Most of the traffics used to launch the attacks reviewed in this study are TCP traffics, except UDP flood attacks. This is due to the nature that 80% of all Internet traffics are TCP traffics.

Attack targets: Flood attacks reviewed here target either client machines, servers or routers. While the high-rate TCP and UDP attacks target network clients and the LoRDAS attack targets network application servers, the Shrew and Quiet attacks target routers in TCP flows. Meanwhile, the Induced-shrew attack targets Internet access routers, as the attacker is the machine that receives the TCP connection assisted by a slaved TCP sender machine.

Attack goals: All flood attacks are aimed at causing denial of service at the targets by exhausting them. High-rate UDP flood attack exhausts the resources at client machines while high-rate TCP flood floods the bandwidth in the network of a TCP client.

Low-rate flood attacks, in the other hand, still cause denial of service at the target, even with a lower degree of flooding. An application server which is the target of a LoRDAS attack will not entertain clients' requests other than the attacker. A Shrew attacker can cause session close and bandwidth deny by continuously causes the router to drop packets following injection of attack traffic at a particular interval. An Internet access routers attacked by an Induced-shrew attack is overpowered by the TCP sender and receiver that execute the attack, hence will route, change transmission rate, or stop routing according to instructions from the attacker. The Quiet attack causes reduction in the throughput of the real traffic through injection of attack traffic in a random interval, which in turn gives illusion of a real congestion at the routers involved.

Attack impacts: All flood attacks cause severe impacts at the victim side. In the high-rate flood attacks, the UDP flood attack causes more degradation of the legitimate traffic than the same intensity of a TCP flood attack. This is because the UDP flood attack exhausts the resources at the target client machines due to its connectionless nature. As for the low-rate flood attacks, the impacts of each attack vary according to factors such as the intensity of the attack and attack duration. As the goal of each attack also varies, comparison on the impact of the attacks must be made based on the similarities of the goal each attack is about to achieve.

CONCLUSION

This study has reviewed six flooding attacks studied in recent years. Most of the flood attacks reviewed in this study are the new breed of flood attacks which are more stealthy yet cause more severe impacts of denial of service, such as those attacks categorized under the low-rate DoS attacks.

Future works include more thorough studies of the flood attacks existing both in IPv4 and IPv6 environments in preparation for the transition to IPv6. A new technique to mitigate one of the flood attacks is to be proposed based on the research conducted.

In order to carry out these tasks, experiments will be carried out both in simulation and test bed environments. Details related to attacks and their impacts will be collected, compared and analyzed.

Next, a model of attack mitigation will be designed based on the characteristics of one attack. This model will then be implemented on a network and will be tested thoroughly, where improvements will be made as needed.

ACKNOWLEDGEMENT

The researchers would like to thank the government of Malaysia for the funding of this study. The first author is studying in University Kebangsaan Malaysia, under study leave from Universities Technical Malaysia Melaka. Both authors join the Network Management Group at University Kebangsaan Malaysia http://www.ftsm.ukm.my/network. The authors also would like to thank Mrs Alena Lee Sanusi and Mr Khairil bin Sailan for constructive suggestions and pre-review done to this article.

REFERENCES

Aleksandar, K. and E.W. Knightly, 2003. Low-rate TCP-targeted denial of service attacks: the shrew Vs. the mice and elephants. Proceeding of the 2003 Conference on Applications, Technologies, Architectures and Protocols for Computer Communications, (CATAPCC'03), ACM New York, NY, USA., pp: 75-86. DOI: 10.1145/863955.863966

CERT, 1997. Denial of Service Attacks. Carnegie Mellon University. http://www.cert.org/tech_tips/denial_of_service.html

Chang, C.W., L. Seungjoon, B. Lin and W. Jia, 2009. The Taming of the Shrew: Mitigating Low-Rate TCP-Targeted Attack. Proceeding of the 29th IEEE International Conference on Distributed Computing Systems, June, 22-26, IEEE Xplore Press, Montreal, QC, pp: 137-144. DOI: 10.1109/ICDCS.2009.9

Curran, K. and Eric Nichols, 2005. E-Democracy. J. Soc. Sci., 1: 16-18. DOI: 10.3844/JSSP.2005.16.18

Fall, K. and S. Floyd, 1996. Simulation-based comparisons of tahoe, reno and SACK TCP. Rev. ACM SIGCOMM Comp. Commun. Rev., 26: 5-21. DOI: 10.1145/235160.235162

Hanapi, Z.M., M. Ismail and K. Jumari, 2009. Priority and random selection for dynamic window secured implicit geographic routing in wireless sensor network. Am. J. Eng. Applied Sci., 2: 494-500. DOI: DOI:10.3844/AJEASSP.2009.494.500

ITU, 1991. Security Architecture for Open Systems Interconnection for CCITT applications. International Telecommunication Union. http://net.infocom.uniroma1.it/corsi/sic_tlc_rieti/dispense/ITU_T_X_800.pdf

Kumar, V., P. Jayalekshmy, G. Patra and R. Thangavelu, 2009. On remote exploitation of TCP sender for low-rate flooding denial-of-service attack. Rev. Commun. Lett., IEEE 13: 46-48. DOI: 10.1109/LCOMM.2009.081555

Li, M., 2006. Change trend of averaged hurst parameter of traffic under DDOS flood attacks. Rev. Comp. Secur., 25: 213-220. DOI: 10.1016/j.cose.2005.11.007.

Li, M., J. Li and W. Zhao, 2009. Experimental study of DDOS attacking of flood type based on NS2. Rev. Int. J. Elect. Comp. 1: 143-152. http://www.umac.mo/rectors_office/docs/weizhao_cv/pub_refereed_journals/2009_ref_journals/IJEC_Dec%202009.pdf

Li, M., L. Jun and Z. Wei, 2008. Simulation study of flood attacking of DDOS. Proceeding of the Internet Computing in Science and Engineering, 2008. ICICSE 08. International Conference, pp: 286-293. DOI: 10.1109/ICICSE.2008.14

Maciá-Fernández, G., J.E. Díaz-Verdejo and P. García-Teodoro, 2009. Mathematical model for low-rate dos attacks against application servers. Rev. IEEE Transa. Inform. Forensics Secur., 4: 519-529. DOI: 10.1109/TIFS.2009.2024719

Mahajan, R., S. Floyd and D. Wetherall, 2001. Controlling high-bandwidth flows at the congested router. Proceeding of the 9th International Conference Network Protocols, pp: 192-201. DOI: 10.1109/ICNP.2001.992899

Michael, W., M. Vutukuru, H. Balakrishnan and D. Karger *et al*., 2010. DDoS defense by offense. Rev. ACM Trans. Comp. Syst., 28: 1-54. http://doi.acm.org/10.1145/1731060.1731063.

Mirkovic, J., A. Hussain, S. Fahmy, P. Reiher and R. K. Thomas, 2009. Accurately measuring denial of service in simulation and testbed experiments. Rev. Dependable Secure Comp. IEEE Trans., 6: 81-95. DOI: 10.1109/TDSC.2008.73.

Safa, H., M. Chouman, H. Artail and M. Karam, 2008. A collaborative defense mechanism against SYN flooding attacks in IP networks. Rev. J. Network Comp. App., 31: 509-534. DOI: 10.1016/j.jnca.2007.12.004.

Savage, M. and P. Reiher, 2004. A taxonomy of DDoS attack and DDoS defense mechanisms. Rev. SIGCOMM Comp. Commun. Rev., 34: 39-54. http://direct.bl.uk/bld/PlaceOrder.do?UIN=151967806&ETOC=RN&from=searchengine

Savage, S., N. Cardwell, D. Wetherall and T. Anderson, 1999. TCP congestion control with a misbehaving receiver. Rev. ACM SIGCOMM Comp. Commun. Rev., 29: 71-78. DOI: 10.1145/505696.505704.

Shevtekar, A. and N. Ansari, 2009. Is it congestion or a DDoS attack? Rev. Commun. Lett., IEEE 13: 546-548. DOI: 10.1109/LCOMM.2009.090628

Xia, Z., S. Lu and J. Tang, 2010. Note on studying change point of lrd traffic based on li's detection of Ddos flood attacking. Review Math. Problems Eng., DOI: 10.1155/2010/962435

Xiao, B., W. Chen and Y. He. 2008. An autonomous defense against SYN flooding attacks: Detect and throttle attacks at the victim side independently. Rev. J. Parallel Distributed Comp., 68: 456-470. DOI: 10.1016/j.jpdc.2007.06.013

Xiapu, L. and R.K.C. Chang, 2005. On a new class of pulsing denial-of-service attacks and the defense. Proceeding of the Network and Distributed System Security Symposium, (NDSS). CiteSeerx, USA., pp: 61-79. http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.143.8143

Yu, Chen, H. Kai and K. Yu-Kwong, 2005. Filtering of shrew DDoS attacks in frequency domain. Proceeding of the IEEE Conference on Local Computer Networks, 30th Anniversary, Nov. 17-17, IEEE Xplore Press, Sydney, NSW., pp: 8-793. DOI: 10.1109/LCN.2005.70

Yu, J., H. Lee, M.S. Kim and D. Park, 2008. Traffic flooding attack detection with SNMP MIB using SVM. Rev. Comp. Commun., 31: 4212-4219. DOI: 10.1016/j.comcom.2008.09.018