DDoS Attack Detection Method and Mitigation Using Pattern of the Flow

Ahmad Sanmorino[1], Setiadi Yazid[2]
Faculty of Computer Science
Universitas Indonesia
Depok, Indonesia
e-mail: [1]ahmad.sanmorino@ui.ac.id, [2]setiadi@cs.ui.ac.id

***Abstract*— Distributed denial-of-service attack (DDoS Attack) is one of the types of attacks that use multiple hosts as attacker against a system. There is a difference between Distributed Denial-of-Service (DDoS Attack) and Denial-of-Service (DoS Attack). DDoS attacks are distributed, meaning spread using multiple hosts, while the DoS attack is one-on-one. DoS attacks requires a powerful host, either from the resource or operating system used to carry out the attack. In this study, we discuss how to handle DDoS attacks in the form of detection method based on the pattern of flow entries and handling mechanism using layered firewall. Tests carried out using three scenario that is simulations on normal network environment, unsecured network, and secure network. Then, we analyze the simulations result that has been done. The method used successfully filtering incoming packet, by dropped packets from the attacker when DDoS attack happen, while still be able to receive packets from legitimate hosts.**

***Keywords*— distributed denial-of-service attack, simulation**

I. INTRODUCTION

Distributed denial-of-service attack (DDoS Attack) is a type of attack uses many hosts as attacker to spend the resources of a system or networks that are become targets of attacks. DDoS attacks are widely used because it is considered the most effective way to cripple a server or a network. The purpose of DDoS attacks is to spend server resources that become targets of attacks, namely by flooding victim computer with huge traffic, preventing legitimate users to access services on the server [1, 2]. It is still very difficult to detect of DDoS attack at an early stage. DDoS attacks are usually discovered when a server or network already down or exhaustion for a while. Lags of detection of DDoS attacks because of the difficulty distinguishing between legitimate packets on normal traffic and packets sent by zombie computers. Another difficulty is caused by the huge number of packets sent that required much time to analyze each incoming packet and it causes DDoS detection accuracy decreases. DDoS attack is very popular because of the ease of doing it. There are many tools that can be used to attack, with friendly user interface, even users who have little knowledge of computer networks can do a massive DDoS attack against a server.

Usually the target of the attack is a high-profile web servers or servers that provide specific services, such as banks, auction website, credit card payment gateways or even social network. In 2010, a massive DDoS attacks happen on social networks Twitter, that resulting it server down for a few hours after the attack [3]. As one of the most difficult problems in network security, DDoS attacks have posed a serious threat to the availability of Internet services [4, 5, 6]. In common, the term of DDoS attacks usually used in discourse of computer network. But the truth it is not limited to computer network only, DDoS can also be used as a reference for CPU resource management problem [7].

This paper discussed about the mechanism of Distributed Denial-of-Service attack (DDoS Attack) that is to simulate DDoS attack using a network security simulator tool (NeSSi2). Then, we analyze the types and patterns of packets involved in this attack. Finally, we give a solution to handle DDoS attacks in the form of detection method based on the pattern of flow entries and handling mechanism using layered firewall.

II. DDOS ATTACK

Along with the advancement of technology, the type and mechanism of DDoS attacks continues to grow. Currently, there are various types of DDoS attacks that are widely used, such as:

A. *SYN Flooding*

SYN Flooding is one of DDoS attack that was first appears and until now is the most widely used. SYN flooding works by exploiting weaknesses on transmission control protocol (TCP). Fig. 1 shows the mechanism of SYN flooding attack. SYN packet is a type of packet in the Transmission Control Protocol (TCP) which required to establish a connection between two hosts. It is a request sent by the host to make a connection.

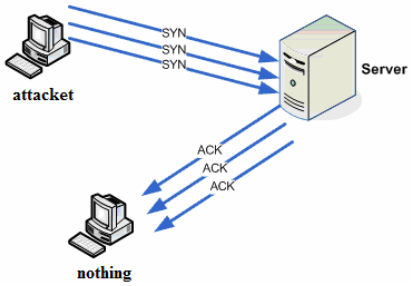

Figure 1. SYN flooding mechanism

In SYN Flooding attack hackers will send SYN packets to the ports that are in a state of 'Listening' in the target host. Normally, SYN packets transmitted contains the source address that shows the actual host, but SYN packets in a DDoS attack is designed so that these packets have a source address that does not represent the actual host. When the target receives SYN packets that have been modified, the target will respond with an SYN / ACK packet addressed to the address listed in the SYN packet that it received, which means the system does not exist, and then it will wait for packet acknowledgment (ACK) in reply to complete the connection process. However, because the source address in the SYN packet sent by the attacker invalid, ACK packet will never come to the target, and the target of attacks port will wait until the connection timed-out [8]. If a listening port is receiving a lot of SYN packets, then that port will respond with an SYN / ACK according to the number of SYN packets in the buffer capacities that are allocated by the operating system.

B. Low-rate Denial-of-Service Attack

Low-rate denial-of-service attack exploits retransmission time-out mechanism (RTOs) on TCP protocol, with the goal of lowering TCP throughput. A hacker creates TCP flow at RTO state continuously, by sending high-rate packet with a short duration. This causes TCP throughput on the target decreased significantly, while the transmission of computer attackers remained in low-rate state, making it very difficult to be detected [9].

C. ICMP Flooding

Internet control message protocol (ICMP) flooding is a type of DDoS attacks that exploits configuration errors on network devices involved. That will let the whole packets sent throughout a host on the network via broadcast address, which should be sent to a host specifically. At time when DDoS attack happen, the hacker will send a large number of IP packets with a fake return address since this address will appear on the host that become target of attacks. This makes the network bandwidth drain, causing legitimate packets blocked achieve its request [10]. The following illustration shows the mechanism of distributed denial-of-service attack [11].

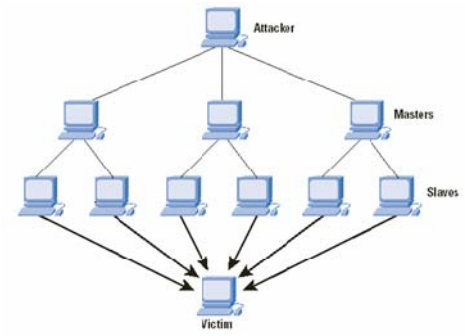

Figure 2. DDoS attack mechanism

Attacker is running the controller program (can be a Trojan horse) on the master computer, and the master computer instructed slave to carry out attacks on a victim's computer [11]. Although the scheme of DDoS attack used are very simple, but because it comes from tens or even hundreds of zombie computers, the amount of network traffic created become very large, it can easily drain resources on server that become the target of attack.

To remove the traces, an attacker can distribute the attacks through computers master in a different time zone, or with a different system administrator. Attackers also make network traffic visible from different computers. The technique to spoof an IP address is called IP spoofing. IP spoofing is a common method used to disguise the source of the attack. If the source of the attack is not known, then it is difficult to do anything, provide an opportunity for an attacker to do what he wants.

III. RELATED WORKS

Research focus on handling of DDoS attacks has been studied for a long time. One of these studies was done by Lee et al. [12] by using cluster of features extracting from some variable traffic. Clustering is performed to classify the phase in packet delivery. From this clustering it will be known the phase of the current DDoS attacks. Then, traced back traffic variables which are used on that phase can be performed. But first we must know the characteristics of DDoS attacks. Cluster analysis method is less precise in the process of DDoS detection due to its time complexity. Such is a general problem of clustering methods which, requires several iterations to create a stable cluster. So that the time required to perform a DDoS attack detection becomes twice as long.

Other studies conducted by Feng et al. [13] using five statistical features of IP Flow. These five features are composed by four features of Micro-Flow and one feature of Macro-Flow. Micro-Flow is a package that is part of a group of packages that have the same characteristics and intervals. While Macro-Flow is the whole package is sent at the same time interval. The use of five statistical features of IP Flow is considered good, but it should be 'signed' from the calculation of the five IP Flow features that some kind of flow pattern that comes in, so that when the next attack happens, do not bother to do the calculations again.

Different from two other studies described earlier, DDoS attacks detection method proposed by Wang et al. [14] take advantage of multi-core technology on CPU. However, the challenge for this research is how the detection method divides it phase into several parts without neglecting the dependence of each's data. Another problem is how to maintain a balance of work between each core that used.

Other methods have been proposed that is the use of source IP as a trace-back direction to detect sources of attacker. But apparently by using IP spoofing techniques, hackers can manipulate source IP or disguised it. In other words, it is not the original IP of the attacker.

We propose a method that is expected to cover the limitations of the other methods that have been explained before. The use of pattern-based method of flow entries are expected to reduce time complexity that required to detect DDoS attacks. The use of patterns of flow entries also allows detection of the source IP address of the attacker can be more accurate. IP spoofing method that used by hacker become

useless. The use of the proposed detection method is believed to reduce the cost of infrastructure because it system only use switches or routers that already exists, do not require high-tech computer resources, such as Multi-Core CPU technology, etc.

IV. SOLUTION

A. *Flow Entries Pattern Detection*

The solution is the use of flow patterns that are transmitted to server. Based on this flows pattern, we can determine whether a packet is coming from DDoS attacks. The pattern of flow entries is implemented on a router or switch that became a liaison between the botnet and server that become the target of the attack. While handling mechanism is in the form of firewall that becomes a gateway for incoming traffic to the server. Illustration of this solution is as follows:

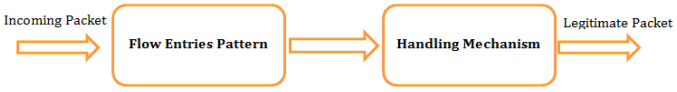

Figure 3. DDoS attack handling mechanism

Three steps DDoS attack detection using pattern of the flow are as follows:

1. Take the required data from the flow table, the data will be used in detection process. Perform detection using flow header based on model of normal flow. If the flow is detected as normal, then run the second step.

2. Perform detection based on pattern of DDoS flow, if detected, then execute the next step.

3. Perform handling mechanism using layered firewall against packet that coming from the second step.

Pattern of a flow can be learned from the information extraction of each incoming flows. The information obtained from a flow such as source IP, source port, destination IP, destination port, transfer protocol, flow size, and number of packets.

src IP	src port	dst IP	dst port	protocol	flow size	num of packet

Figure 4. Information on flow entries

One of the flow entries patterns of DDoS attack is the magnitude of the average number of packets per flow in a specified time interval. The average number of packets per flow can be obtained by summing all incoming packets and then divided it by the number of flow. If the number of incoming packets is very small with huge amount of flow, then we can predict at that time happening DDoS attacks. One of the characteristics of DDoS attack types SYN Flooding is the huge amount of flow and small number of packets (per flow). Based on this information, we can be traced every source of IP packet (usually more than one or distributed). Then, we can make a sort of 'blacklist' for packets who using same source.

B. *Layered Firewall*

The next phase is to drop packets that are coming from the attacker. This phase involves the participation of firewall as a handling mechanism. In the simulations we used double-layer firewall. The illustrations can be seen in Fig. 7. The first firewall architecture includes a plurality of network layers. The layers send packets and packet information to the first firewall engine, maintain and pass packet context to subsequent layers, and process the packets. The first firewall engine compares the packet information to one or more installed filters and returns an action to the layers indicating how to treat the packet [15]. So it can be ascertained that the packet was able to move on only it comes from the legitimate users.

V. SIMULATION

We do the simulation using Network Security Simulator tool *(NeSSi2)* [16]. The simulations conducted in three different scenarios:

A. Simulate a network with a server and legitimate host (Normal Network)

B. Simulate a network with a server (as target of the attack), legitimate host and botnet (Unsecured Network).

C. Simulate a network with a server (as target of the attack), legitimate host and botnet, with an implementation of the detection method based on flow entries pattern and handling mechanism (Secure Network).

The purpose of these three scenarios is to see the comparison between network traffic in normal network, unsecured network and secure network by implementing detection method based on pattern of flow entries and handling mechanism. More explanation about each of the simulation scenarios can be seen in the following section.

A. *Normal Network Simulation*

The first scenario describes traffic of packets that occurs between hosts and a server. Traffic was normally, the process of sending and receiving packets running smoothly.

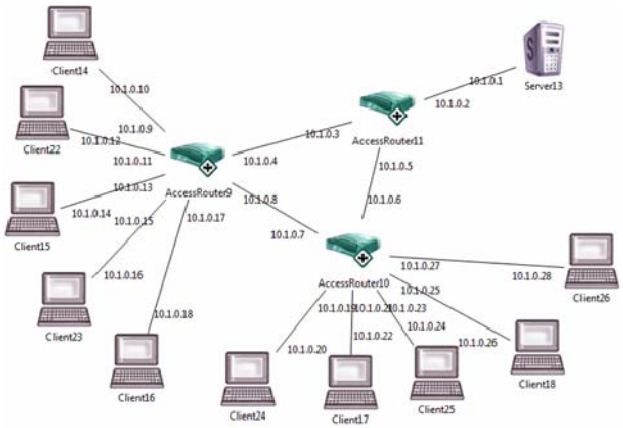

Figure 5. Normal network

B. *Unsecured Network Simulation*

The second scenario illustrates network with half of the users are botnet that take part in the attack against server (Fig. 6). Handling mechanism has not been implemented so that the traffic between hosts and server becomes very high.

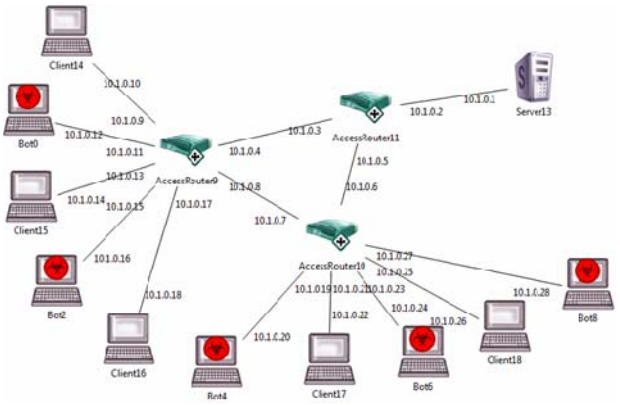

Figure 6. Unsecured network

C. *Secure Network Simulation*

The third scenario describes a network with combination of legitimate and botnet clients that are communicate with network server (Fig. 7). The difference between second scenario and this scenario is the implemented detection mechanism using pattern of flow entries and handling mechanism to handle DDoS attacks that carried by botnet. Detection based on pattern of flow entries is implemented on the router or switch that connect each client to server. The mechanism for packet handling is implemented in the layered firewall to ensuring every packet that can still move on is only coming from legitimate users.

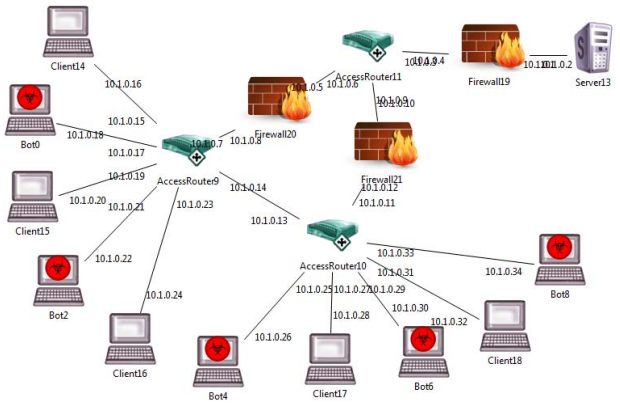

Figure 7. Secure network

VI. RESULT AND DISCUSS

In this section we describe the results of three simulations that have been conducted. Fig. 8 shows the number of packets that transmitted successfully on normal network scenario. There is nothing unusual in this network, traffic was normal. Fig. 9 shows the number of packets transmitted successfully on unsecured network scenario. Total number of packets that transmitted on insecure network scenario is eight times than normal network. Although the number of clients that are owned by the attacker in the first scenario and the second scenario is the same. Furthermore, fig. 10 shows the results of simulation scenarios on secure network. It can be seen handling mechanisms successful dropped out approximately 95% from total amount of packets.

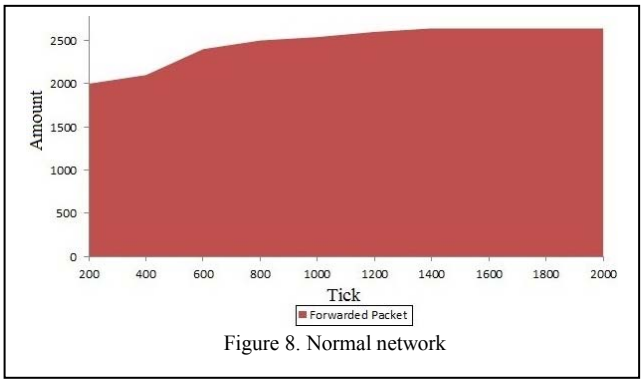

Figure 8. Normal network

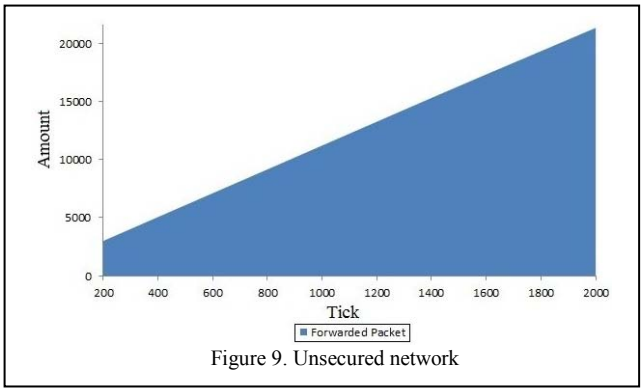

Figure 9. Unsecured network

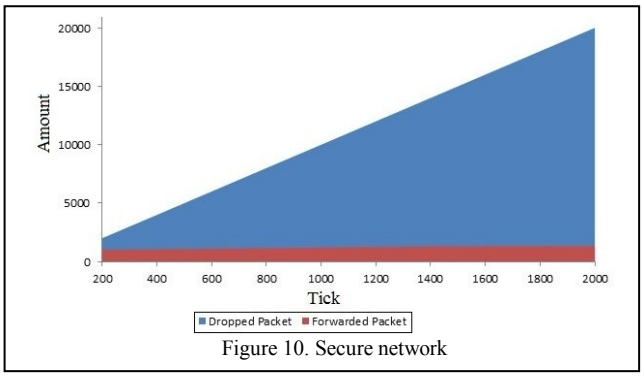

Figure 10. Secure network

VII. CONCLUSION

DDoS attack detection based on pattern of flow entries and handling mechanism can successfully handle the incoming attacks from the hacker. This is evident from the results of secure network scenario simulations that have been done. From the comparison between second scenario and third scenario, the large number of forwarded packets that delivered on the second scenario were dropped on the third scenario. In these simulations we ignored the external factors that may cause packet drop. For further research we expected to resolve this matter, by implementing the proposed solution into the real network. In the real network there are several factors that can cause packet drop such as signal degradation, channel congestion, and faulty networking hardware. All that needs to be taken and measured how much influence on our proposed method. Also if it will be implemented in a real network, we

need to adjust our simulation with the configuration and real condition of the infrastructure in the field.

ACKNOWLEDGMENT

This study was supported by Faculty of Computer Science, Universitas Indonesia.

REFERENCES

[1] CERT Advisory CA-96.21, "TCP SYN flooding and IP spoofing," November 2000. Available: http://www.cert.org/advisories/CA-96-21.html.

[2] W. Wang, S. Gombault, "Efficient Detection of DDoS Attack with Important Attributes," Third International Conference on Risks and Security of Internet and Systems: CRiSIS'2008, pp. 61-67, 2008.

[3] "Twitter hit by denial-of-service attack," 2009. Available: http://www.cnn.com/2009/TECH/08/06/twitter.attack/index.html

[4] C. Jin, H. Wang, K. G. Shin, "Hop-Count Filtering: An Effective Defense Against Spoofed DDoS Traffic," CCS'03, Washington D.C., ACM 1-58113-738-9/03/0010, pp. 30-41, 2003.

[5] D. Moore, G. Voelker, and S. Savage, "Inferring internet denial of service activity," In Proceedings of USENIX Security Symposium 2001, Washington D.C., 2001.

[6] L. Garber, "Denial-of-service attack rip the internet," IEEE Computer, April 2000.

[7] F. Yuval, K. Uri, E. Yuval, D. Shlomi, Chanan, "Google Android: A Comprehensive Security Assessment," IEEE Security & Privac, doi:10.1109/MSP.2010.2, 2010.

[8] "RFC 4987 – TCP SYN Flooding Attacks and Common Mitigations," 2011. Available: http://tools.ietf.org/html/rfc4987

[9] C. Zhang, J. Yin, Z. Cai, and W. Chen, "RRED: Robust RED Algorithm to Counter Low-rate Denial-of-Service Attacks," IEEE Communications Letters, vol. 14, pp. 489-491, 2010.

[10] "Types of DDoS Attacks," 2001. Available: http://anml.iu.edu/ddos/types.html

[11] "Distributed Denial of Service Attacks," The International Journal – Volume 7, Number 4, 2004. Available: http://www.cisco.com/web/about/ac123/ ac147/archived_issues/ipj_7-4/dos_attacks.html

[12] K. Lee, J. Kim, K.H. Kwon, Y. Han, S. Kim, "DDoS attack detection method using cluster analysis," ELSEVIER Expert Systems with Applications, vol 34, pp. 1659-1665, 2008.

[13] Y. Feng, R. Guo, D.Wang, and B. Zhang, "Research on the Active DDoS Filtering Algorithm Based on IP Flow," in 2009 Fifth International Conference on Natural Computation. IEEE, 2009, pp. 628–632.

[14] D. Wang, Z. Yufu and J. Jie, "A Multi-core Based DDoS Detection Method," 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), pp. 115-118, 2010.

[15] B. D. Swander, P. G. Mayfield, "Multi-layered firewall architecture," Microsoft Corporation, Redmond, WA (US), 2009.

[16] "NeSSi: Network Security Simulator," 2012. Available: http://www.nessi2.de/