Detection of flooding ddos attack using anomaly and signature based intrusion detection system

D.VANITHA
Post Graduate Student - CSE
Dr.Mahalingam College of Engineering and Technology, Pollachi.
Email: vanitha.navanithan@gmail.com

MR.R.CHANDRASEKAR M.E
Assistant Professor(SG) - CSE
Dr.Mahalingam College of Engineering and Technology, Pollachi.
Email: sekar.vrc@gmail.com

***Abstract*- Distributed denial-of-service (DDoS) attacks remain a major security problem. Network security has become an essential assert for each and every organization. Network Intrusion Detection System (NIDS) provide an important security function to help defend against network attacks like DDoS attacks. IDSs collect network traffic information from some point on the network or computer system and then use this information to secure the network. Intrusion detection systems can be anomaly based detection or signature based detection. Anomaly based IDSs like firecol detect new or unknown attacks by using heuristic methods whereas signature based IDSs detect known attacks whose attack behavior is already known. In this paper we propose a hybrid IDS by combining the two approaches in one system. The hybrid IDS is obtained by combining signature based intrusion detection system with anomaly based intrusion detection system.**

***Index terms*: Intrusion Detection System(IDS), Network Security, Anomaly based IDS, Signature based IDS**

I. INTRODUCTION

More than five years after the initial flurry of network attacks, and the news articles and research papers that followed DDoS remains the number one concern for large IP network operators. Sixty-four percent of the survey participants said, “DDoS is the most significant operational security issue we face today[1].” It causes severe damage to servers and raise as a greater intimidation to the development of new Internet services. A flooding-based DDoS attack is a very common way to attack a victim machine by sending a large amount of malicious traffic.

Current security measures such as firewalls, security policies, and encryption are not sufficient to prevent the compromise of private computers and networks. With increasing connectivity between computers, the need to keep networks secure progressively becomes more vital. Intrusion detection systems (IDS) have become an essential component of network security. It can be signature based detection or anomaly based detection.

Anomaly based detection system, flags observed activities that deviate significantly from the established normal usage profiles as anomalies. Signature based IDS detects attacks by matching against a database of known attacks. The signatures are used to match with incoming traffic to detect intrusions. The obvious drawback is that only known attacks can be detected, whereas new attacks or even slight variations of old attacks go unnoticed.

In the existing system, anomaly based intrusion detection system namely FireCol is used. The incoming traffic is periodically compared with the constructed profile to detect the attack. The disadvantage is that to detect similar kind of attack, firecol does the same comparison with the profile which is a time consuming process.

To overcome this problem, a hybrid approach is used in the proposed system. Both signature based and anomaly based detection systems are employed where known attacks are detected by signature based IDS and unknown attacks(anomalies) are detected by FireCol. The signature generation unit characterizes the detected anomalies and extracts their signatures. These signatures are then added to the signature based intrusion detection database for future detection of similar attacks.

II. RELATED WORK

Distributed denial of service (DDoS) attacks are widely regarded as a major threat to the Internet. A flooding-based DDoS attack is to attack a victim machine by sending a large amount of unwanted traffic. Hackers and intruders have made many successful attempts to bring down high-profile company networks and web services. Although a number of techniques have been proposed to defeat DDoS attacks, it is still hard to detect and respond to flooding based DDoS attacks due to a large number of attacking machines, the use of source address spoofing, and the similarities between legitimate and attack traffic. DDoS attacks put the victim out of business by consuming the bandwidth at the victim end. To protect the victim from a flooding-based DDoS attack, the response mechanism should be as close to the attack source as possible. The source-end response mechanism has a few advantages over the victim-end response mechanism [2]. It can control and avoid congestion more effectively. Existing system uses FireCol which detects flooding DDoS attacks as close as possible to the attack source(s) at the Internet service provider (ISP) level.

Kai Hwang, (2007) also presented a new distributed approach to detecting DDoS (distributed denial of services) flooding attacks at the traffic flow level [8]. The source end defense system is suitable for efficient implementation over the core networks operated by Internet service providers (ISP). The source-end defense is not a complete solution to flooding attacks, since networks that do not deploy the proposed defense can still be misused for successful attacks. Still, source-end defense is necessary for precise differentiation of legitimate and attack traffic. In cooperation with victim-end or core-based defenses, source-end defense could ensure safe delivery to the victim of all and only legitimate traffic from the defense-deploying networks. This makes source-end defense one of the key building blocks of the complete DDoS solution and essential for promoting Internet security.

Rocky K. C. Chang, 2002 proposed DDoS attack detection approaches [3]. In that various DDoS attack methods, a systematic review and evaluation of the existing defense mechanisms are discussed. The author discussed a longer-term solution, dubbed the Internet-firewall approach that attempts to intercept attack packets in the Internet core, well before reaching the victim.

There are three lines of defense against the attack:

- Attack prevention and preemption(before the attack)
- Attack detection and filtering (during the attack),
- Attack source traceback and identification

Existing system comes under attack detection and filtering method.

Munivara Prasad, 2011 proposed various anomaly based intrusion detection techniques, based on a host or network [4]. Many distinct techniques are used based on type of processing related to behavioral model. Profiling program and user behaviors is an effective approach for detecting hostile attacks to a computer system. A new model based method by non-negative matrix factorization (NMF) to profile program and user behaviors for anomaly intrusion detection. In this method, the audit data streams obtained from sequences of system calls and UNIX commands are used as the information source. The audit data is partitioned into segments with a fixed length. Program and user behaviors are, in turn, measured by the frequencies of individual system calls or commands embedded in each segment of the data, and NMF is applied to extract the features from the blocks of audit data associated with the normal behaviors.

The model describing the normal program and user behaviors are built based on these features and deviation from the normal program and user behaviors above a predetermined threshold is considered as anomalous . Under statistical based detection method multi-variate model is used in the existing system[7]. Frequency and entropy are the two metrics used.
Jonnalagadda, 2011 proposed hybrid structure to identify threats to the network across multiple network segments [5]. Distributed hybrid system consists of several IDS over a large network(s), all of which communicate with each other, or with a central server that facilitates advanced network monitoring. In that snort is the signature based IDS used to detect known attack through signature matching with the database[9]. The proposed system simulates the signature based IDS and detects the known attack. Anomaly-based systems are supposed to detect unknown attacks. In that a machine learning based anomaly detection technique is used [10] whereas in the existing system firecol is used as anomaly based IDS.

III. EXISTING WORK

FireCol, an anomaly based Intrusion Prevention System(**IPS**) detects flooding DDoS attacks as far as possible from the victim host and as close as possible to the attack source. In the existing system, a statistical based anomaly detection approach (Firecol) detects unknown attack. FireCol construct profiles of users using their normal behaviors. These profiles are produced using the data that is accepted as normal. After the profile construction, detectors monitor new event data compare the new data with obtained profile and try to detect deviations. These deviations from normal behaviors are flagged as attacks.

A. *Ring based protection*:

- It is designed in a way that makes it a service to which customers can subscribe.
- When a customer subscribes for the FireCol protection service, The trusted server adds an entry with the subscribing rule and the supported capacity.
- As shown in the Fig 1. The IPSs form virtual protection rings around the host they protect. The virtual rings use horizontal communication when the degree of a potential attack is high.

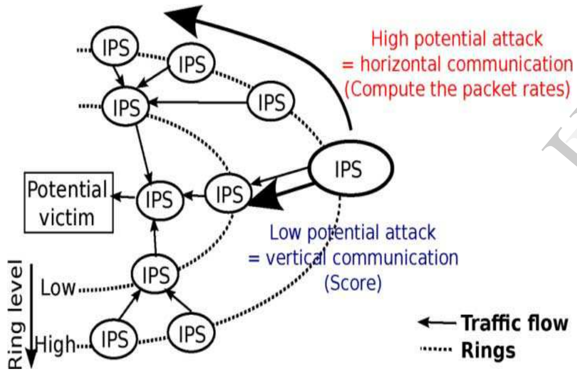
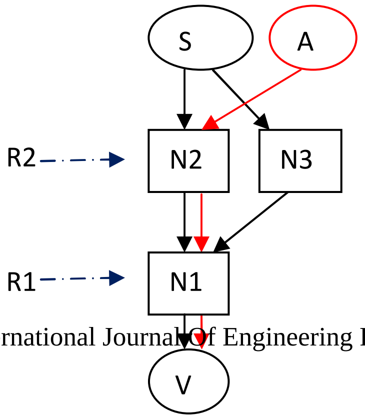

IPS
IPS
IPS
IPS
IPS
IPS
IPS
IPS
IPS
IPS
Potential victim
High potential attack = horizontal communication (Compute the packet rates)
Low potential attack = vertical communication (Score)
Ring level
Low
High
Traffic flow
Rings

Fig 1. Horizontal and vertical communication in FireCol.

B. *Simulation of Topology for DDoS Attack*

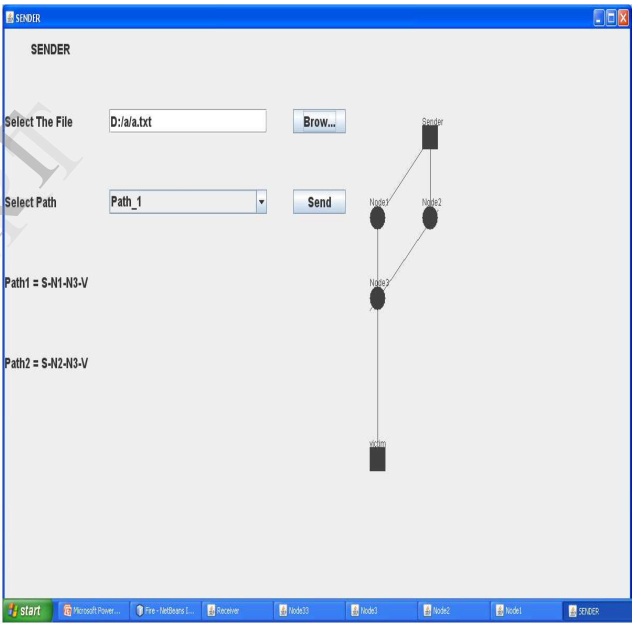
In order to detect the DDoS attack using FireCol - anomaly based detection system, a sample network is created with normal sender, attacker and the victim.



S-Sender
A-Attackers
V-Victim
(N1toN3)- IPS
R1-Ring level1
R2-Ring level2

Fig. 2. Sample network

As in the Fig. 2. nodes which are one hop from the victim form ring level1, two hop from the victim form ring level2. Here the node N1 forms ring level1, nodes N2 and N3 forms ring level2. Firecol IPS(Intrusion Prevention System) is installed at N1, N2 and N3.



SENDER

Select The File D:/a/a.txt

Select Path Path_1

Path1 = S-N1-N3-V

Path2 = S-N2-N3-V

Fig. 3. Sample Output

Sample output is shown in the Fig. 3. for the simulated topology.

C. *Profile Construction*

Firecol IPS in the network constructs profiles of normal traffic flow by computing frequency and entropy values.

Frequency: The frequency is the proportion of packets f_i matching rule within a detection window

$$f_i = \frac{F_i}{\sum_{j=1}^{n} F_j}$$

where F_i is the number of packets matched by rule during the detection window.
The frequency distribution is then defined as
f = $\{f_1, f_2, \ldots f_n\}$

***Entropy**:* The entropy **H** measures the uniformity of distribution of frequencies.

$$H = -E[\log_n f_i] = -\sum_{i=1}^{n} f_i \log_n(f_i)$$

Table 1: Profile for normal traffic flow

Time(10s)	Number of packets received	Number of packets matching the rule	Frequency	Entropy
T1	1000	550	0.55	**0.42563**
T2	1000	636	0.636	
T3	1000	312	0.312	

Decision table is constructed with the computed frequency and entropy values. It consists of score and conclusion which decides the traffic as normal flow or attack flow.

D. Attack Detection using Firecol

Attacker sends the data continuously (flood) towards the victim. For the attack flow FireCol IPS computes the frequency and entropy values, if it is deviated from the stored ones, then the score is assigned using decision table. After assigning the score, using attack detection algorithm FireCol detects the flooding attack by computing packet rate.

If the rate is higher than the rule capacity, an alert is raised. Otherwise, the computed rate is sent to the next IPS on the ring. FireCol fails to detect the similar attacks as earlier as possible. It uses the attack detection algorithm for detecting the attacks of similar types, which is a time consuming process.

IV PROPOSED WORK

A. Implementation of Hybrid Intrusion Detection System

In the proposed system hybrid intrusion detection system(IDS) is used to detect the similar attacks detected by FireCol as earlier as possible using signature based intrusion detection system.

Initially the incoming traffic is given to the signature based IDS, which has to identify the known attack. Signature based detection is the most widely type of detection used by IDS nowadays. The IDS uses a local database with multiple packet signatures known as being malicious. Each data packet going through the IDS is compared to a list of known malicious patterns.

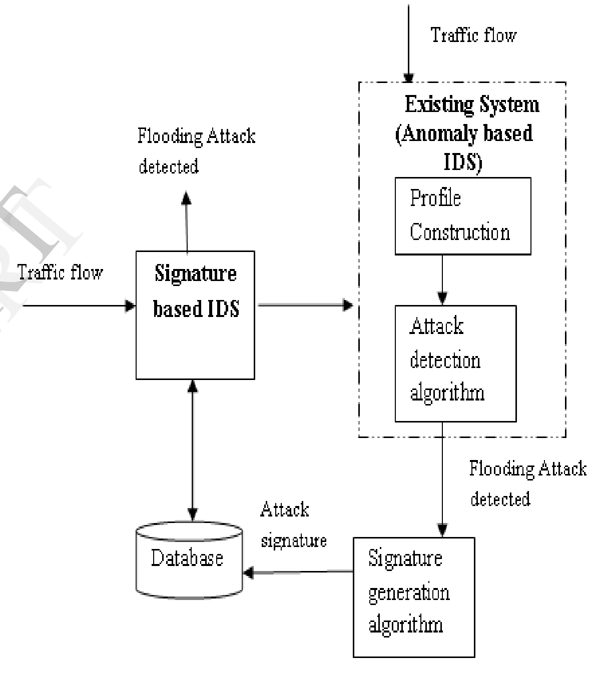


Fig. 4 Block diagram of proposed system

Whenever a positive match is found, it means that a malicious packet has been detected. After detecting known attack the traffic is given to FireCol which has to identify any unknown or new attacks using the attack detection algorithm.

B. Signature Generation and Attack Prevention

New attack signature for the attack detected by FireCol is generated and it is updated with the database of signature based IDS. Using the attack signatures the

IDS can filter out future occurrences of the attacks. The < attribute; condition > pair form an abstract signature for the attack [6].

The < attribute; condition > pairs form an abstract signature of the flooding attack.

The < attribute; condition > pair is decoded as follows:

(ip proto = icmp), (icmp type = echo req),
(1,480 <= src bytes < 1,490),(dst count > 10)

Using the attribute mappings attack signature is translated into signature based IDS’s rule. The generated signature is updated with signature based IDS database. So that similar attacks are detected and prevented earlier by blocking IP address.

V. CONCLUSION

This paper proposed hybrid intrusion detection system (anomaly and signature based), a scalable solution for the early detection of flooding DDoS attacks. The hybrid IDS is said to be more powerful than the anomaly-based on its own because it uses the advantages of signature-based approach for detecting known attacks. Using the attack signatures the IDS can filter out future occurrences of the attacks. Generating more signatures will further enhance the overall performance of the hybrid IDS.

VI. ACKNOWLEDGEMENT

I would like to express my gratitude to Mr.R.Chandrasekar M.E., Assistant Professor (SG), Department of CSE, Dr.Mahalingam College of Engineering and Technology for his useful comments, remarks and engagement through the learning process of this project. Furthermore I would like to thank Ms.G.Anupriya M.E., Assistant Professor (SG), Department of CSE, Dr.Mahalingam College of Engineering and Technology for introducing me to the topic as well as for the support. Also, I would like to thank my family members, who have supported me throughout entire process, both by keeping me harmonious and helping me. I will be grateful forever for their love.

VII. REFERENCES

[1] A. Networks, Arbor, Lexington,MA, “Worldwide ISP security report,”Tech. Rep., 2010

[2] J. Mirkovic and P. Reiher, "D-WARD: A Source-End Defense Against Flooding DoS Attacks," IEEE Trans. on Dependable and Secure Computing, pp. 216-232, July 2005.

[3] Rocky K. C. Chang,” Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial”, Communication Magazine, IEEE, Volume 40 Issue 10, October 2002.

[4] V. Jyothsna, V. V. Rama Prasad, K. Munivara Prasad,”A Review of Anomaly based Intrusion Detection Systems,” International Journal of Computer Applications (0975 – 8887) Volume 28– No.7, August 2011.

[5] Sravan Kumar Jonnalagadda, and Subha Sree Mallela, “ An Intelligent Hybrid Structure for Improving Intrusion Detection,” International Journal of Research and Reviews in Software Engineering (IJRRSE) Vol. 1, No. 2, June 2011.

[6] Kai Hwang, Min Cai, Ying Chen and Min Qin, “Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes,” IEEE Transactions on Dependable and Secure Computing, Vol. 4, No. 1, January 2007.

[7] Jerome Francois, Issam Aib, and Raouf Boutaba, “FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks”, IEEE/ACM Transactions on Networking, April 2012.

[8] Yu Chen, Kai Hwang, Wei-Shinn Ku, “ Collaborative Detection of DDoS Attacks over Multiple Network Domains,” IEEE Transactions on Parallel and Distributed Systems, Volume 18 Issue 12, December 2007.

[9] Raven Alder, Jacob Babbin, Adam Doxtater, James C. Foster and Michael Rash “Syngress Snort.2.1.Intrusion.Detection Second.Edition”May2004.

[10] Barbara, D., Wu, N., Jajodia, S.,” Detecting novel network intrusions using Bayes estimators.” In: Proceedings of First SIAM Conference on Data Mining, Chicago, IL (2001).