Fully Distributed Intrusion Detection System Based On Traffic Matrixes Against Denial Of Service Attack

Badrinath. K
Asst.Prof,Dept of ISE
S.J.C.Institute of Technology
Chickballapur, Karnataka

Pradeep Kumar. G. M
Asst.Prof,Dept of CSE
S.J.C.Institute of Technology
Chickballapur, Karnataka

Abstract

The current intrusion detection systems have a number of problems that limit their configurability, scalability and efficiency. There have been some propositions about distributed architectures based on multiple independent agents working collectively for intrusion detection. However, these distributed intrusion detection systems are not fully distributed as most of them centrally analyze data collected from distributed nodes which may lead to a single point of failure. In this paper, a DIDS(Distributed Intrusion Detection System) named as F-DIDS is built to defense against flooding DoS(Denial of Services) attacks in the paper. F-DIDS is composed of FIDSes which are settled in nodes who need to be protected. FDIDS is a complete DIDS, in which each node with F-IDS can be the detection centre. Due to no central node, single failure can be avoided in F-DIDS. In F-DIDS, Traffic tables help to build up traffic matrixes. By analyzing traffic matrixes, flooding DoS attacks could be detected and three normal flooding DoS attacks are classified. Local and global communication methods are proposed to reduce the overhead brought from fully distributed architecture. The simulation results and performance analysis show that F-DIDS works effectively.

Keywords
Denial of Service, Distributed Intrusion Detection System, SYN Flooding, ICMP Flooding, UDP Flooding

1. Introduction

A denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Typically the targets are high-profile web servers, the attack aiming to cause the hosted web pages to be unavailable on the Internet. Denial of service attack programs, root kits, and network sniffers have been around for a very long time. A distributed denial of service attack (DDoS attack) is a large-scale, coordinated attack on the availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet [1]. As a serious threat to network securities, DDoS(Distributed Denial of Service) is always hard to be detected [2]. In DDoS attacks, the hacker sends malicious flows from a wide area to the victim. On the node near to the sources abnormal signs are inconspicuous; however, while the attacks behavior could be felt, the networks have been throttled and then detecting attacks becomes meaningless. It is the major point and also the most difficult to detect DDoS as near to the source as possible, which is discussed in the paper. Since DIDS(Distributed Intrusion Detection System) gathers data with distributed components to analyze data from the whole area, DIDS is a strong tool to detect and defense against DDoS attacks. Fully distributed architecture is used to build a DIDS named as F-DIDS to detect flooding DDoS attacks in the paper. A single component settled in a specific network element is called F-IDS, which is based on traffic matrixes.

In a local network area, all F-IDSs gather data, communicate with each other and analyze data. All F IDSes compose FDIDS. As a fully DIDS, each F-IDS could be the central processor and make decision by itself. Local and global communication methods are proposed to reduce the overhead brought from fully distributed architecture. Fully architecture avoids the single point failure.

2. Overview of DDoS Attacks

2.1 Attack Strategies

DDoS attacks can be divided into two categories: bandwidth Attack and resource attack. A bandwidth attack simply try to generate packets to flood the victim's network so that the legitimate requests cannot go to the victim machine. A resource attack aims to send packets that misuse network protocol or malformed packets to tie up network resources so that resources are not available to the legitimate users any more.

2.1.1 Bandwidth Attacks

2.1.1.1 Flood Attack

In a direct attack, zombies flood the victim system directly with IP traffic. The large amount of traffic saturates the victim's network bandwidth so that other

legitimate users are not able to access the service or experience severe slow down. Normally in those attacks, the following packets are used.

- **TCP floods** A stream of TCP packets with various flags set are sent to the victim IP address. The SYN, ACK, and RST flags are commonly used.
- **ICMP echo request/reply (e.g., ping floods)** A stream of ICMP packets are sent to a victim IP address.
- **UDP floods** A stream of UDP packets are sent to the victim IP address.

2.1.1.2 Reflected Attack

A reflected denial of service attack involves sending forged requests of some type to a very large number of computers that will reply to the requests. Using Internet protocol spoofing, the source address is set to that of the targeted victim, which means all the replies will go to (and flood) the target. ICMP Echo Request attacks can be considered one form of reflected attack, as the flooding host(s) send Echo Requests to the broadcast addresses of mis-configured networks, thereby enticing a large number of hosts to send Echo Reply packets to the victim. Some early DDoS programs implemented a distributed form of this attack. Nowadays, DNS attacks using recursive name servers can create an amplification effect similar to the now-aged Smurf attack [2].

2.1.2 Resource Attacks

- **TCP SYN Attack** The TCP SYN attack exploits the three-way handshake between the sender and receiver by sending large amount of TCP SYN requests with spoofed source address. If those half-open connection binds resources on the server or the server software is licensed per connection, all these resources might be taken up.
- **Malformed Packet Attack** A ping of death (abbreviated "POD") is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A ping is normally 64 bytes in size; many computer systems cannot handle a ping larger than the maximum IP packet size which is 65,535 bytes. Sending a ping of this size often crashes the target computer.

3. Related Work

IDS(Intrusion Detection System) is the initial system to detect DDoS or DoS, which places detection component in the important network node[3][4]. The data will not be exchanged among IDSs. With the development of networks, DoS attacks arise in distributed way, which makes IDS powerless to defense against DDoS attacks. In order to detect attacks as near to the hacker as possible, DIDS becomes the first selection[5].

There are three architectures of DIDS: Distributed central control systems, distributed hierarchical systems and fully distributed systems[2].

In central-control systems, data gathered by distributed components are sent to a monolithic engine where data are analyzed and decision is made, which is easy to cause a single point failure.

This serious weakness led to research on distributed hierarchical systems[6][7], which describe a cooperative system without centralized analysis components. In this approach, the local intrusion detection components look for local intrusions and pass the results of their analysis to the upper levels of the hierarchy. The components at the upper levels analyze the refined data from multiple lower level components and seek to establish a global view of the system state[8]. The major disadvantages of hierarchical DIDSs are the heavy network load and network latency (the delay between each level in the architecture). Moreover, there is still highest-level entity, which is the bottleneck of this system and leads a single point failure.

In fully distributed systems, each detection node could be central. An intruder can just destroy one point if possible, but other points still work. However, the most common shortcomings in existing fully DIDS architectures are that there are very large amounts of data being transmitted among the detectors which may occupy the networks channel [8] solves the problem with shorter messages. In the paper, different communication schemes help to reduce the communication overhead. A fully DIDS is also discussed in [2]; however, three main flooding attacks are not classified in [2]. By traffic matrix, the type of flooding DDoS attacks is made clear in F-DIDS.

4. Design of F-DIDS

A F-IDS is composed of traffic gathering module, traffic table, traffic matrix and communication module. The organization of F-IDS is described in Figure 1. Traffic gathering module gathers traffic in order to store it in traffic table to set up traffic matrixes. Different packets' incoming rates, such as SYN, ICMP and UDP ones, will be sampled in traffic gathering module. The content of traffic table comes from either its own traffic gathering module or others' communication modules. Data in traffic table are used to set up traffic matrix so that the flooding DoS attacks' alerts could be classified into four levels denoted as 0th, 1st, 2nd and 3rd warnings.

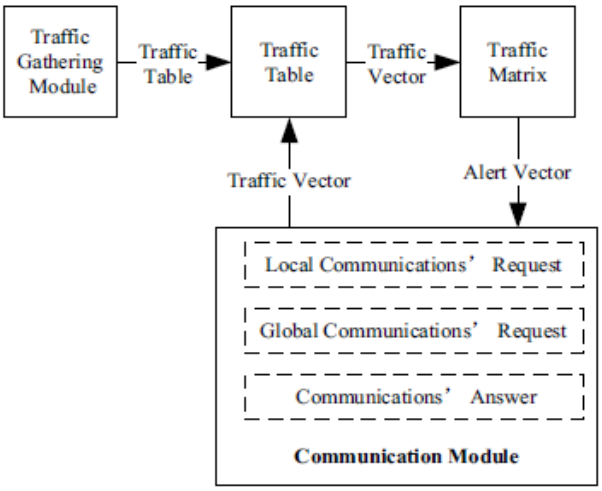

Figure 1 : Organization of F-IDS

4.1 Traffic Gathering Module

Data sampled by traffic gathering module include IPRi(Incoming Packets' Rate), SYNi(Incoming SYN Packets' Rate), ACKi(Incoming Rate of Acknowledgement Packets for SYN), ICMPi(Incoming ICMP Packets' Rate), UDPi(Incoming UDP Packets' Rate). IPR helps to detect flooding attacks. SYN and ACK are used to detect SYN flooding attacks, while ICMP and UDP work for ICMP flooding attacks and UDP flooding attacks respectively. All data are quantized into 8 levels: from 0 to 7.

4.2 Traffic Table

Data in traffic table comes from either Traffic gathering module or communication module.

Table 1: Traffic Table

Address	Fresh	Local	Traffic Vector	Arriving Time

Traffic table is represented as Table 1. *Fresh* is set 1 if traffic vector is valid. Traffic vector is one row of traffic matrix. Arriving time is the time when vector arrives, which is related to *fresh* signal. If *local* is set 1, the node is the local node.

4.3 Traffic Matrix

TM(Traffic Matrix) is a $n \times 5$ matrix. Here, n is below the sum of nodes in the networks.

$$\mathbf{TM}_{n\times 5} = \begin{pmatrix} IPR_0, & SYN_0, & ACK_0, & ICMP_0, & UDP_0 \\ IPR_1, & SYN_1, & ACK_1, & ICMP_1, & UDP_1 \\ & & \cdots\cdots & & \\ IPR_{n-1}, & SYN_{n-1}, & ACK_{n-1}, & ICMP_{n-1}, & UDP_{n-1} \end{pmatrix}$$

The simplest TM is the traffic vector denoted as 1×5 **TM** .
$\mathbf{TM}_{1*5} = \{IPR_0, SYN_0, ACK_0, ICMP_0, UDP_0\}$
$IPR_0, SYN_0, ACK_0, ICMP_0, UDP_0 \in \{0,1,2,3,4,5,6,7\}$
AV(Alert Vector) denotes the level of alert.
AV = (*Flood*, *SYN*, *ICMP*,*UDP*)
Flood, *SYN*, *ICMP*,*UDP*∈ {0,1,2,3}

Flood denotes the possibility of Flooding DoS attacks. Similarly, *SYN* is for SYN flooding attacks; *ICMP* is for ICMP flooding attacks; and *UDP* is for UDP flooding attacks.

Accuracy factor denoted as α could avoid repetitive communications. In 2nd alert, if α is big enough, which means there are enough traffic vectors in traffic table, the global communications will be avoided and communication overhead will be reduced.

$$\alpha = \frac{m}{m + \left\lfloor \frac{n}{2m} \right\rfloor}$$

"*n*" is the sum of nodes in the networks. "*m*" is the sum of nodes whose *fresh* is 1.

$$Flood = \left\lfloor \frac{\sum_{i=0}^{n-1} IPR_i \times \alpha}{2n} \right\rfloor \qquad ICMP = \left\lfloor \frac{\sum_{i=0}^{n-1} ICMP_i \times \alpha}{2n} \right\rfloor$$

$$UDP = \left\lfloor \frac{\sum_{i=0}^{n-1} UDP_i \times \alpha}{2n} \right\rfloor \qquad S_i = \left| \log \frac{ACK_i + \alpha}{SYN_i + \alpha} \right|$$

$$\overline{S} = \left\lfloor \sum_{i=0}^{n} S_i / n \right\rfloor \qquad SYN = \begin{cases} \overline{S} & \overline{S} < 4 \\ 3 & \overline{S} > 4 \end{cases}$$

In summary, the flow chart of a F-IDS is represented as Figure 2.

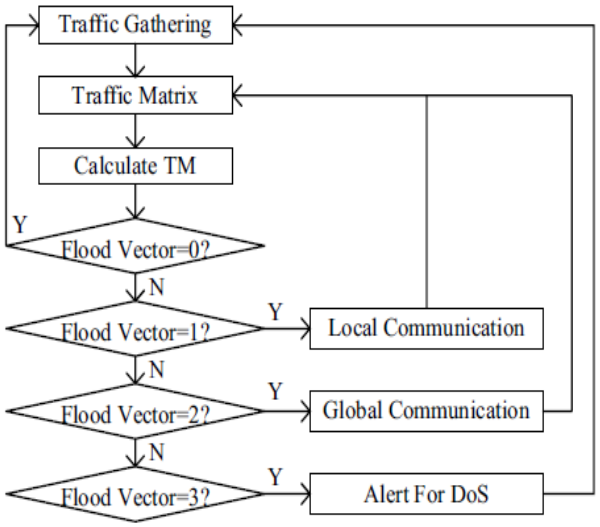

Figure 2: Flow Chart of F-DIDS

5. Analysis of F-DIDS

Assume packets flows sent by DDoS hackers pass through node1 with F-IDS1, node2 with F-IDS2 and node3 with FIDS3. Node0 with F-IDS0 is the victim. Figure 3 gives the Topology of simulated network, Figure 4 shows the incoming packets and Figure 5 represents the *flood* level of AV(Alert Vector) in F-IDS0. From 3rd to 5th second, a warning of attack is given.

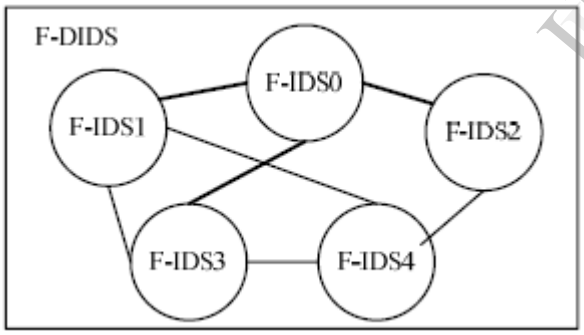

Figure 3 :The Topology of simulated network

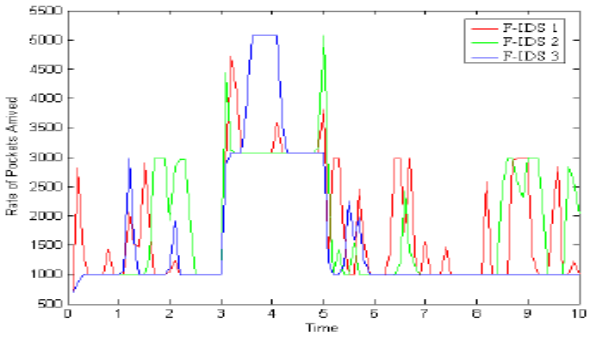

Figure 4 : Incoming Packets in Three FIDS

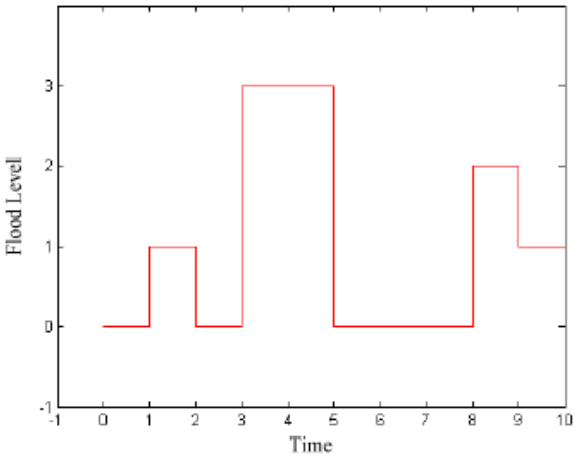

Figure 5 : Flood level for FIDS0

6. Conclusion

Without any central node, single failure can be avoided in F-DIDS. Traffic matrixes help to distinguish three flooding attacks. Local and global communications reduce the overhead of data exchanging.

The simulation results and performance analysis show that F-DIDS works effectively.

7. References

[1] N. Long S. Dietrich and D. Ddittrich, "Analyzing distributed denial of service tools: the shaft case," in *Proceedings of the LISA XIV*.

[2] BAI Yuan, BAI Zhongying: "Design and Simulation of a Tree-Based Intrusion Detection System against Denial of Service". Applied Mechanics and Materials, ISSN: 1660-9336.

[3] D. Novikov, R. Yampolskiy, and L Reznik "Anomaly Detection Based Intrusion Detection". Third International Conference on Information Technology,2006, pp. 420- 425.

[4] H. Kai, H. Zhu, K. Eguchi, N. Sun, and T. Tabata " A Novel Intelligent Intrusion Detection, Decision, Response System" IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences archive, 2006.

[5] Wei Lin, Liu Xiang, Derek Pao, and Bin Liu "Collaborative Distributed Intrusion Detection System", Second International Conference on Future Generation Communication and Networking 2008, pp.172-177.

[6] Martin Chovanec, Liberios Vokorkos, and Ján Perha "Security Architecture Based on Multilayer Distributed Intrusion Detection System", 5th International Symposium on Applied Computational Intelligence and Informatics, 2009, pp.301-306.

[7] Computer Emergency Response Team, “Cert advisory ca-2000-01 denial-of-servic developments,” http://www.cert.org/advisories/CA-2000-01.html, January 2000.

[8] M. Yasin, and A. Awan "A Study of Host-Based IDS using System Calls", International Conference on Networking and Communication ,2004, pp.36- 41.

[9] Safaa Zaman and Fakhri Karray, "Collaborative Architecture for Distributed Intrusion Detection System ", Proceedings of the 2009 IEEE Symposium on Computational Intelligence in Security and Defense Applications ,2009, pp.1-7.