Extending of IDS for Detecting Abnormal Intrusion Traffic Simulations based on SSFNet

Kwan Jong Yu , Seung Kyu Park, Kyung Hee Choi, GiHyun Jung
Graduate School of Information and Communication
Ajou University
Suwon, Republic of Korea.

Abstract : The cyber attacks become more and more complex and variable. So, common type of Intrusion Detection System (IDS) which uses Rule Based matching process is hard to detect such malicious traffics. We propose more intelligent IDS system. Our system can detect dynamic abnormal traffics without the exact detection rules. This paper proposes an IDS which have rule based matching features and ability of detecting some unpredictable malicious traffic by itself. We implement this IDS based on SSFNet simulation framework. Performing various types of simulations for network intrusion, the implemented IDS on the simulation show that it plays the same property as that of actual networks.

Keywords : IDS, Detect abnormal traffic, Simulation framework

1. Introduction

With rapid technological advances being made in the area of internet, we can easily reach a plenty of useful information via internet. While the internet gives us many benefits, the risk of being exposed to malicious intrusions grows higher due to higher availability of networks. Recently, the management of secure network became a critical issue for system administrators.

Such issues include understanding and analyzing the properties of the large network and issue of how to detect malicious intrusions. With recognizing various patterns of intrusions and observing current situation of a given system, the system administrators should be able to detect the intrusion property by analyzing packets and patterns of network intrusions so as to defend against them.

The best method to observe the real intrusion detection is to execute an actual intrusion on diverse network environments. Actual execution produces the information on the properties and behavior of its corresponding network. The experiment on the actual network, however, costs too much or sometimes it is impossible to make the real environment for experiments. Considering the enormous scale of recent networks, it is not practical to build a complex network to experiment an actual intrusion. Such network reveals the lack of theoretical study and the diversity of intrusions.

The simulation is a good candidate to replace the ineffective experiments on the actual network. The simulation allows a flexible means to analyze and study the behavior of intrusion and detection of the network. Various studies on simulations have been carried on in the area of network intrusion, which includes the methods for analyzing behaviors [1,2].

Scalable Simulation Framework Network Model (SSFNet) is one of popular network simulation frameworks. We can easily construct a large simulation environment using Domain Modeling Language (DML). Since the simulation environment constructed by SSFNet is based on the host model which reflects the

properties of modern real networks, users can get relatively as accurate result from the simulation as those from real network on the behavior of network intrusions.

This paper is composed as follows : in chapter 2, we define the IDS, and look around some related works. In chapter 3, explain how our IDS is constructed. In chapter 4, we go further about the behavior of detecting and how detect an abnormal traffic without rule-set. In chapter 5, we examine our IDS via some simulation. And, finally, in chapter 6, we talk about future works.

2. Related Works

A. Intrusion Detection System

Great efforts were made to find out the malicious intrusion attempts and their patterns based on the log analysis using an accumulated audit. However, the analysis of intrusion detection after real intrusion could not be of any help for the prevention of actual intrusion. In the case of an attemptto delete audit record from intruders, it was impossible to detect and analyze the intrusions. Furthermore, since the network architecture gets distributed and open, providing a real-time feature becomes indispensable for intrusion detection system. It allows to detect and to react in the real-time manner against various intrusions of the type on distributed and complex intrusion patterns.

B. classification of intrusion detection system

Misuse detection vs. Anomaly detection: In misuse detection, the IDS analyzes the information it collected and compares it with large databases of attack signatures. Essentially, the IDS looks for a specific pattern of attack that has already been documented. In anomaly detection, the system administrator defines the baseline, or normal, state of the network's traffic load, breakdown, protocol, and typical packet seize. The anomaly detector monitors network segments and compares network states with the normal baseline so as to look for anomalies.

C. The character of Worm traffic

Worm attacks some common special service's weak point and get the administrator's right. And archive some commands which attacker wants. And then, victim host spread worm again. Cause of this special feature, when some worm activated, there are many packets that started from numerous hosts and have special destination port.

D. Detecting abnormal traffic via dynamic analysis

IDS looks up packets and analyze the packet's source address distribution and its destination port distribution in real-time. If the distribution's degree exceed given threshold, IDS will alert about it, although there are no such rules.

3. System architecture

Proposed IDS is composed of a packet queue which stores packets from the additional module of packet capture, a packet decoder which trans-codes packets to the proper type to search the rules of IDS, a detection engine which matches packets to corresponding rules, a rule table which stores the rules for detection, and finally a log engine which records log messages about the detected intrusions. Figure 1 shows the system architecture of the proposed IDS.

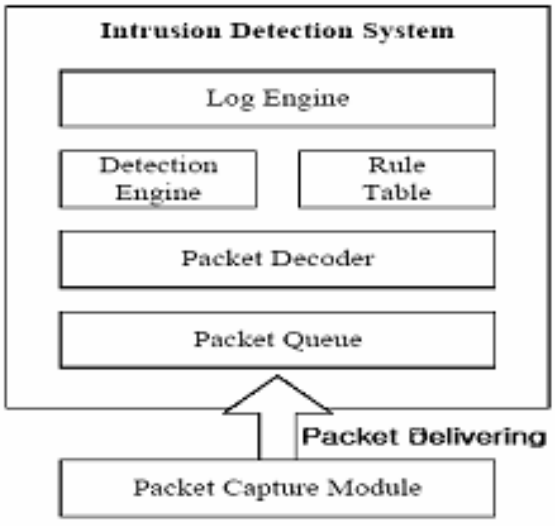

Fig.1 System architecture of proposed IDS

A. Class diagram

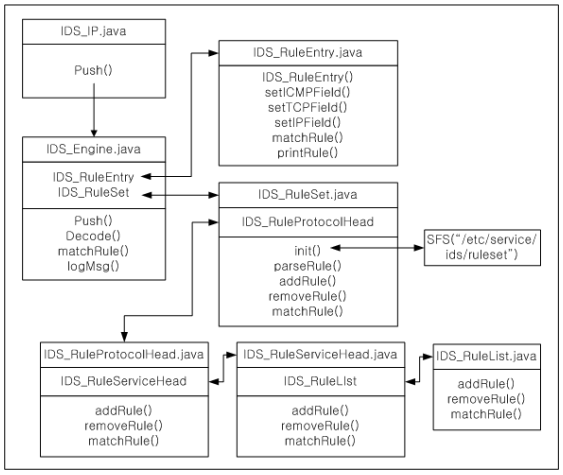

Fig.2 Class Diagram

IDS is composed with seven classes and its function is like this.

- IDS_IP : delivering packets to IDS Engine
- IDS_Engine : packet decoding, rule matching, logging.
- IDS_RuleSet : managing rule entrys.
- IDS_RuleProtocolHead : managing rules by protocol type.
- IDS_RuleServiceHead : managing rules by service type.
- IDS_RuleEntry, IDS_RuleList : manage each rule entry.

B. System flow

The proposed intrusion detection system works as follows. Firstly, the packet capture module configured on Network Interface Card(NIC) stores the captured packet in the packet queue. Secondly, the packet decoder loads the packets stored in the packet queue to transform them into the format which is usable to the IDS, and then transmit them to IDS engine. Thirdly, based on the decoded packets, IDS engine compares if they match with the rule-sets installed initially by IDS engine performs the command logging system to produce the log message if matched rules are found.

Each rule is classified by protocol and the rules are stored in corresponding format. In the case of TCP and UDP protocol, the stored rules are classified again by ICMP or port numbers. Figure 3 shows the structure of rule-sets.

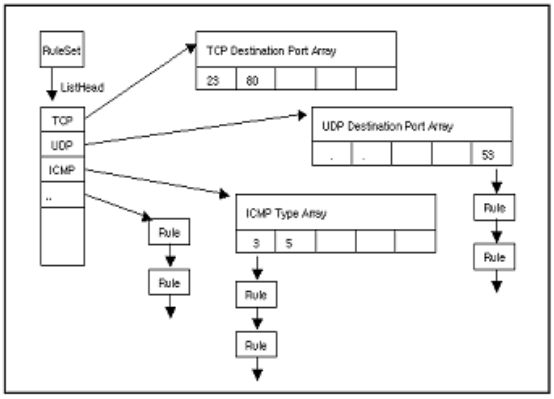

Fig.3 Structure of rule-set

B. IDS Rule format

The format of rules and the definition of detection rule are described in this section. The rules are for detecting intrusion pattern. The setting rules are classified into rule header and rule option. Following tables describe each format and definition.

Rule Header	
Name	Description
Action	Describe the behavior when this packet matches to detection rule. There are three types of this value: ALERT, LOG, IGNORE
Protocol	Support TCP, UDP, and ICMP. They are classified by their protocol types.
srcAddr	NHI address of source
srcPort	Port number of source
dstAddr	NHI address of destination
dstPort	Port number of destination

Table 1. IDS Rule set header

Rule option	
Name	Description
TTL	Time to live of IP header
TOS	Type of service of IP header
Icmp_type	ICMP message type
Icmp_code	ICMP message code
Icmp_id	ICMP message ID
Tcp_flags	Flags for TCP: SYN,FIN,ACK
Tcp_seq	Sequence of TCP message
tcp_ack	Sequence number of TCP ACK message
Payload	Data payload information for each service. IDS Engine will check this payload with captured packet's payload field. It is determined by

	intrusion patterns.
Rate	Number of packets per second. If the number of following packets received is higher than this rate, these packets are assumed as an intrusion.
Msg	Name of intrusion patterns determined by IDS engine.

Table 2. IDS Rule set option

The process of rule matching is like this.

① Analyze the captured packet's type of protocol and get the protocol's rule set list.
② If the packet is a TCP or UDP, IDS will search rule list with packet's destination port number. And if it is a ICMP , look up the ICMP type.
③ If the matched rule sethas payload information, IDS will compare the rule set's payload with packet's payload.
④ If the matched rule set has rate information, IDS will check if this rule set matched higher than the rate.
⑤ IF the above elements are all matched, IDS will write a log message.

4. Detecting an abnormal traffic

A. SYN Flooding

Check the ratio of TCP SYN packets of total inbound packets. If the ratio is more than threshold (0.8) IDS alerts it during unit time (1sec).

$$\text{if} \quad \left(\frac{\text{TCP SYN Packets}}{\text{Total inbound packets}} > 0.8\right) \text{ then ALARM}$$

B. ICMP Flooding

This feature is familiar with SYN Flooding. If the ratio of ICMP request packet's number is so many to more than 80% of total inbound packets then IDS alerts it.

$$\text{if} \quad \left(\frac{\text{ICMP Request Packets}}{\text{Total inbound packets}} > 0.8\right) \text{ then ALARM}$$

C. Valdes' work

The normal traffic has a locality of IP address' set. It means some group of source address is formed, and also has a large range of destination ports. But abnormal traffic – especially kind of worm attack traffics – has a large number of source address distributions and thin destination port distribution. Based on this character, we can establish a detection policy about an abnormal traffic. Equation is like this.

```
if ( (E(srcAddr) > A) && (E(destPort) < B) ) then ALARM
```

E is entropy of them, A and B is a threshold for each element.[9,10]

5. Simulation

We composed some attack scenarios based on SSFNet to test IDS system. First, we composed a virtual network. And implement on SSFNet simulation framework. It has 1775 hosts, and divided in 14 sub networks.

IDS is on S1 network. A attacker will make malicious traffics and the abnormal traffic will grow more and more.

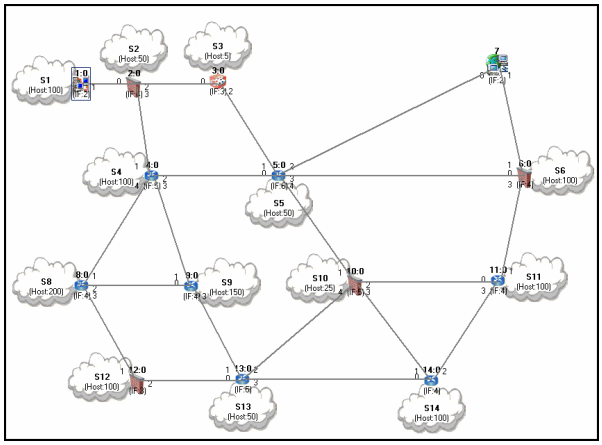

Fig.4 The simulation network

The simulation scenario is like this.

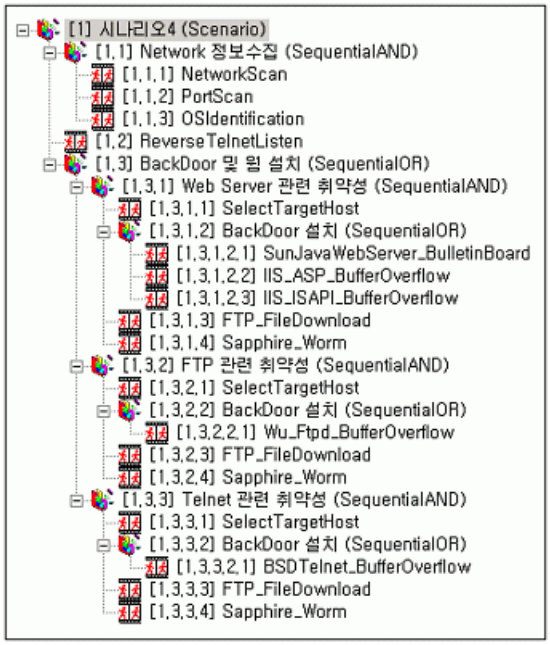

Fig.5 Simulation scenario

This scenario, firstly, does Network scan and

select targets. And then attack them with each service's weak point. And if the attack succeeds, try to spread Sapphire worm again. We can find a special traffic patterns in each step. When a network scan occurred there are many ICMP Request packets and when attacking a weak point, there are many packets that have a specific destination port (i.e. Sapphire uses a TCP 1434 port).

Let's see examples of rule-sets.

① Rule-set for detecting a kind of network scan

- Action=ALERT useProtocol=icmp srcAdd=* srcPort=* destAdd=* destPort=* (icmp_code=0 icmp_type=8 rate=10 msg=[ICMP Ping Flood])

②Rule-set for detecting a kind weak point attack (case of FTP)

- Action=ALERT useProtocol=tcp srcAdd=* srcPort=* destAdd=* destPort=21 (payload={BUFFEROVERFLOW} msg=[FTP Buffer overflow])

③Rule-set for detecting Sapphire Worm

- Action=ALERT useProtocol=tcp srcAdd=* srcPort=* destAdd=* destPort=1434 (msg=[Sapphire Worm])

We get log messages as a result of simulation.

(1) Log messages by abnormal traffic detection.

```
[IDS-Log] 1.01 [IDS=1:0] 7:3:1(0) 1:*(0) Abnormal traffic : ICMP Flooding
[IDS-Log] 2.02 [IDS=1:0] 7:3:1(0) 1:*(0) Abnormal traffic : ICMP Flooding
[IDS-Log] 3.02 [IDS=1:0] 7:3:1(0) 1:*(0) Abnormal traffic : ICMP Flooding
.
[IDS-Log] 221 [IDS=1:0] 7:3:1(0) 1:*(0) Valdes' work - dest port 21
[IDS-Log] 222 [IDS=1:0] 7:3:1(0) 1:*(0) Valdes' work - dest port 21
[IDS-Log] 223 [IDS=1:0] 7:3:1(0) 1:*(0) Valdes' work - dest port 21
.
[IDS-Log] 521 [IDS=1:0] 7:3:1(0) 1:10(0) Valdes' work - dest port 1434
[IDS-Log] 522 [IDS=1:0] 7:3:1(0) 1:11(0) Valdes' work - dest port 1434
[IDS-Log] 523 [IDS=1:0] 7:3:1(0) 1:12(0) Valdes' work - dest port 1434
```

(2) Log messages by Rule set matching

```
[IDS-Log] 1.01 [IDS=1:0] 7:3:1(0) 1:*(0) ICMP Ping Flood Attack Detected
[IDS-Log] 2.01 [IDS=1:0] 7:3:1(0) 1:*(0) ICMP Ping Flood Attack Detected
[IDS-Log] 3.01 [IDS=1:0] 7:3:1(0) 1:*(0) ICMP Ping Flood Attack Detected
.
[IDS-Log] 221 [IDS=1:0] 7:3:1(0) 1:*(0) FTP Buffer Overflow Attack Detected
[IDS-Log] 222 [IDS=1:0] 7:3:1(0) 1:*(0) FTP Buffer Overflow Attack Detected
[IDS-Log] 223 [IDS=1:0] 7:3:1(0) 1:*(0) FTP Buffer Overflow Attack Detected
.
[IDS-Log] 522 [IDS=1:0] 7:3:1(0) 1:11(0) Sapphire Worm Attack Detected
[IDS-Log] 523 [IDS=1:0] 7:3:1(0) 1:11(0) Sapphire Worm Attack Detected
[IDS-Log] 524[IDS=1:0] 7:3:1(0) 1:12(0) Sapphire Worm Attack Detected
```

6. Conclusion and future work

In this paper, we extended the SSFNet to include IDS which is one of the core elements like firewall in the network management system. The proposed system is based on the basic concept of Snort system. It can analyze protocols of inbound and outbound packets to a network. It also allows system administrators to detect the set of intrusion patterns by searching contents of packets and matching them with detection rules.

Further more, proposed IDS can detect malicious traffic by analyzing packets although there are no matched rule-sets. This function is driven from various papers which analyzing the abnormal traffic like traffic made by some worms. [9,10]

The experiments with the simulator, which includes the IDS developed in this research, show that the proposed system can, in a significant level of detail, reflect the behavior of actual IDS in the networks.

References:

[1]SSFNet, http://www.ssfnet.org

[2]NS2, http://www.isi.edu/nsnam/ns/

[3]Snort System, http://www.snort.org/

[4]Anderson, D. Frivold, T. and Valdes A.: Next Generation Intrusion Detection Expert-System (NIDES) - A Summary, Technical Report SRI-CSL-95-07, SRI International, 1995

[5]Donald Welch, Greg Conti, "A Framework for an Information Warfare Simulation", Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 5-6 June, 2001.

[6]Information Warfare and Security, Addison-Wesley, 1999

[7]Jea-hyuk Lee, Eul-guy Im, Joo-beom Yoon, Seung-kyu Park, "Network Intrusion and Defense Simulation Framework based on SSFNet", The 6th international conference on advanced communication technology, 2004

[8]Jin-hyuk Kim, Eul-gyu Im, Joo-beom Yoon, Seung-koo Park, "Network Intrusion Model for analyzing intrusion patterns", The 6th international conference on advanced communication technology, 2004

[9]Alfonso Valdes, "Detecting novel scans through pattern anomaly detection", DARPA Information Survivability Conference and Exposition, 2003.

[10]Guangzhi Qu, Salim Hariri, Santosh Jangiti, Suhail Hussain, Seungchan Oh, "Abnormality Metrics to Detect and Protect against Network Attacks", he IEEE/ACS International Conference on 19-23 July 2004