Distributed intrusion detection system using sensor based mobile agent technology

Vineet Kumar Chaudhary
Department of Computer Science & Engineering
Galgotia,Uttar Pradesh, India

Santosh Kumar Upadhyay
Department of Computer Science & Engineering
Galgotia, Uttar Pradesh, India

Abstract- The Internet and computer networks are exposed to an increasing number of security threats. With new types of attacks appearing continually, developing flexible and adaptive security oriented approaches is a severe challenge. Intrusions detection systems (IDSs) are systems that try to detect attacks as they occur or after the attacks took place. IDSs collect network traffic information from some point on the network or computer system and then use this information to secure the network. In this context, signature-based network intrusion detection techniques are a valuable technology to protect target systems and networks against malicious activities. Signature-based detection is the most extensively used threat detection technique for (IDSs). One of the foremost challenges for signature-based IDSs is how to keep up with large volume of incoming traffic when each packet needs to be compared with every signature in the database. When an IDS cannot keep up with the traffic flood, all it can do is to drop packets, therefore, may miss potential attacks. This paper proposes a new model called Signature-based Multi-Layer IDS using mobile agents, which can detect imminent threats with extremely high success rate by dynamically and automatically creating and using small and efficient multiple databases, and at the same time, provide mechanism to update these small signature databases at regular intervals using mobile agents.

Keywords – Intrusion detection systems, Mobile Agent, Snort, WEKA Tool, Honeyd

I. INTRODUCTION

Due to rapid growth of Internet and network based services; security becomes the primary concern for organizations.There are several ways in which an attacker can attack the network of an organization. These can be accessing information for which he is not authorized, bringing down the whole network, etc. A survey[1,2] show that the number of hosts connected to the Internet has increased to almost 550 million and more than 1.5 billion users are currently using the Internet. The recent survey of Mini Watts Marketing Group [2] estimated that the total number of Internet users was 1,802,330,457 on December 31st 2009. In 2010, the Kaspersky system logged 1,311,156,130 network attacks. That number was just 220 million in 2009. The review[3] shows the major attacks seen in recent years. Review shows that with the increasing number of Internet users, the cyber crimes also have been increased worldwide to a great value. Fortunately, some intrusion prevention techniques as a first line of defense, such as user authentication (e.g. using passwords and biometrics), avoiding programming errors, and information protection (e.g. encryption) have been applied to protect computer systems.In the current article we are preparing a security network based on Intrusion Detection System(IDS)[4,5]. We are capturing the packets using packet sniffer tool (Honeyd[6]) and convert those packets in a log file. Weka workbench tool[7] access those log files for association rule mining and convert them in a SNORT compatible format[8,9] to generate an alarm if any unauthorised intruder wants to access. Mobile agent technology is used through sensors to detect attacks.

II. INTRUSION DETECTION SYSTEMS (IDSS)

Intrusion detection are the activities that violate the security policy of system.Intrusion detection is the process used to identify the intrusions.Types of intrusion detection system:

Based on the sources of audit information used by each ids the IDSs may be classified into:

Host based IDSs

Distributed IDSs

N/W based IDSs

The current Internet faces escalating threats form more sophisticated, intelligent and automated malicious codes [17].

HOST-BASED IDSS

1.GET AUDIT DATA FROM HOST AUDIT TRAILS.

2.DETECT ATTACKS AGAINST A SINGLE HOST

DISTRIBUTED IDSS

1.GATHER AUDIT DATA FROM MULTIPLE HOST AND POSSIBLY THE NETWORK THAT CONNECTS THE HOSTS

2.DETECT ATTACKS INVOLVING MULTIPLE HOSTS

NETWORK-BASED IDSS

1.USE NETWORK TRAFFIC AS THE AUDIT DATA SOURCE, RELIEVING THE BURDEN ON THE HOSTS THAT USUALLY PROVIDE NORMAL COMPUTING SERVICES

2.DETECT ATTACKS FROM NETWORK.

III. PROPOSED FRAMEWORK FOR INTRUSION DETECTION SYSTEM

SYSTEM FRAMEWORK

Intrusion Detection Approaches:

1. Define and extract the features of behavior in system.
2. Define and extract the Rules of Intrusion.
3. Apply the rules to detect the intrusion.

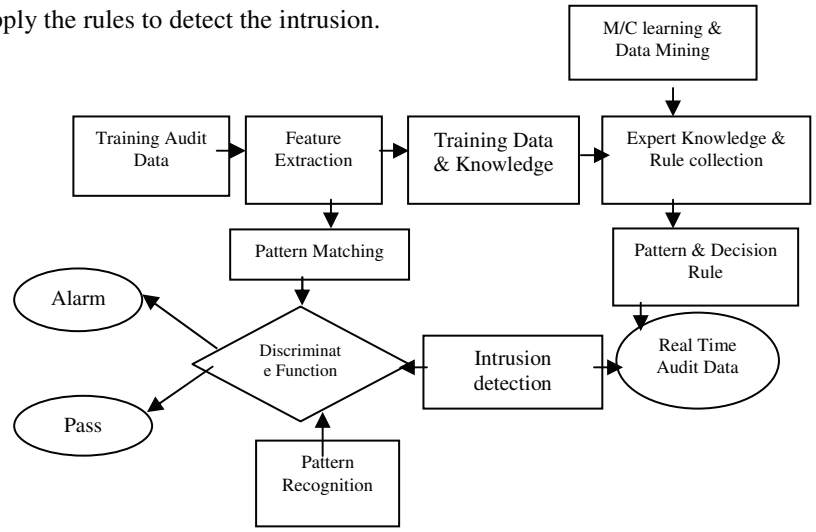

Fig. 1 System Design

IV. AUTOMATIC SNORT COMPATIBLE SIGNATURE GENERATION SYSTEM (ASSG)

As already pointed out that the main problem with signature based IDS is that their limited attack signature database. Also regularly updating the signature database manually is very hectic. To deal with this problem, this system is put along with other systems. As shown in figure, this system takes input from the honeypot

V. EXPERIMENT AND RESULT

The experiments were performed choosing two different hardware platforms to simulate attacks and run IDS, one more powerful than the other. The objective was to simulate DDoS attacks on IDSs by running IDS on the slower machine and attacking tools on the faster machine. The aggregate computational and networking resources of attackers usually overwhelm the resources on the IDS machine. In this case, we would like to evaluate the effects of having multiple smaller signature databases and how effectively it helps in improving the throughput and decreasing packet loss rate. A small packet loss rate directly leads to small possibility to miss real attacks that might be hidden in false positive storms. The results should be optimized is our aim.The detailed hardware and software configurations of systems used for performing experiments are as follows

Attacking System:

1. 2GB memory / Windows 7
2. CPU: Intel Core i3 at 2.10 GHz\
3. 10/100Mbps NIC

IDS System:

1. 4GB MEMORY / UBUNTU LINUX (BASED ON VIRTUAL OPERATING SYSTEM)
2. CPU: INTEL CORE I3 AT 2.10 GHZ

Attacking Tools:

During the period, following tools were used: Demarc SQL Injection, ICMP Destination, DOS UPnP malformed advertisement, PROTOCOL-DNS SPOOF, INDICATOR-SHELLCODE x86 inc ecx NOOP and INDICATOR-SCAN UPnP Service to trigger alert by the IDS and create a bseline of the most frequent attacks on the network (Fig 1).

ANALYSIS OF RESULTS

For performing experiment, we considered any attack that appeared at least once as a frequent attack. In addition, all the threats detected in the training period are to be included in the database. Our program scanned all the rule files of Demarc SQL Injection and created a new rule file called “signature.rule” containing the most frequently signatures detected during the training period to be referenced by the snort.conf file as the only signature rule file. In addition, our program created complementary rule files taking out the most frequently used signatures for the secondary IDS. Demarc SQL Injection was restarted on both systems pointing to the new signature files. To test the performance of all IDS, we conducted our experiment using two tests in two different scenarios. In the first scenario, we manually enabled 546 packets and attacked the network-using Demarc SQL Injection. In the second scenario, we let our algorithm do its job by enabling only the most frequent signatures (in this case 33). Table 1, 2 and Figure 1, 2 show the results of our tests in regards of the effects on packet drop rate[10].

S.No	Parameter		Value
S.No	Parameter		Value
1	No. of virtual systems created in honeypot		10
2	No. of log records considered at a time		1000
3	Support value in Apriori	Upper bound	1.0
		Lower bound	0.05
4	Confidence value in Apriori	Upper bound	1.0
		Lower bound	0.01

TABLE 1

Detail by Signatues						
Num	**Prio**	**Signature**	**#Alerts**	**# Sources**	**# Dest.**	**Detail**
1	0	SERVER - WEBAPP Demarc SQL Injection attempt [sid 2063] [cve 2002-0539] [bugtraq 4520]	91	6	8	Summary
2	3	PROTOCOL - ICMP Destination Unreachable Port Unreachable [sid 402]	871	1	3	Summary
3	2	DOS UPnP malformed advertisement [sid 1384]	37	1	1	Summary
4	2	PROTOCOL - DNS SPOOF query response with TTL of 1	78	2	1	Summary

		min. and no authority [sid 254]				
5	1	INDICATOR - SHELLCODE x86 inc ecx NOOP [sid 1394]	54	3	7	Summary
6	3	INDICATOR - SCAN UPnP service discover attempt [sid 1917]	10	2	1	Summary

Table 2

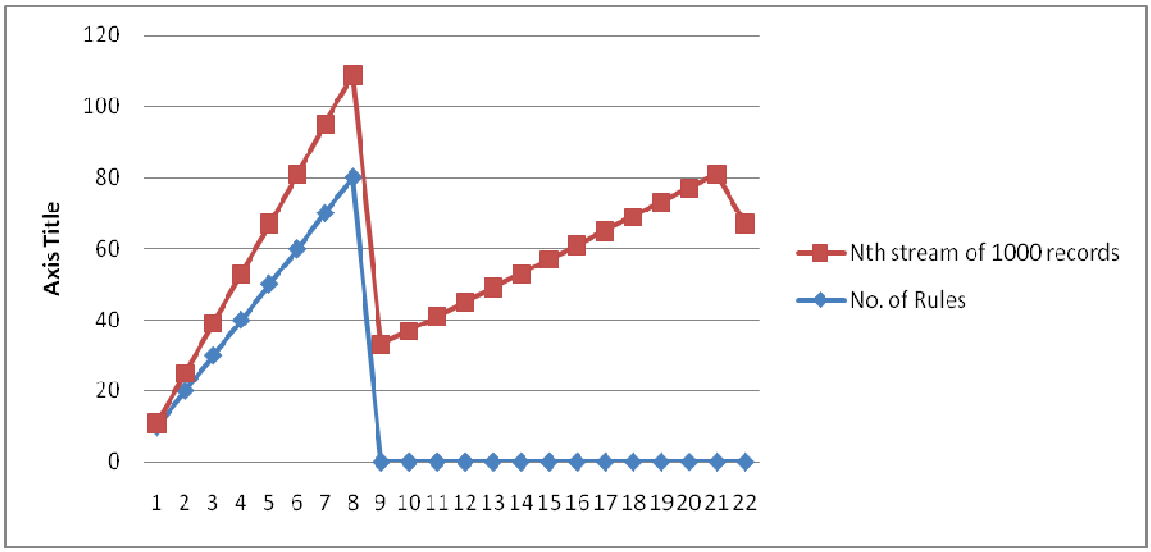

Fig. 1 Rules generated by Weka and accession in Snort against successive stream of attack records (number of attributes considered in frequent item set is 7).

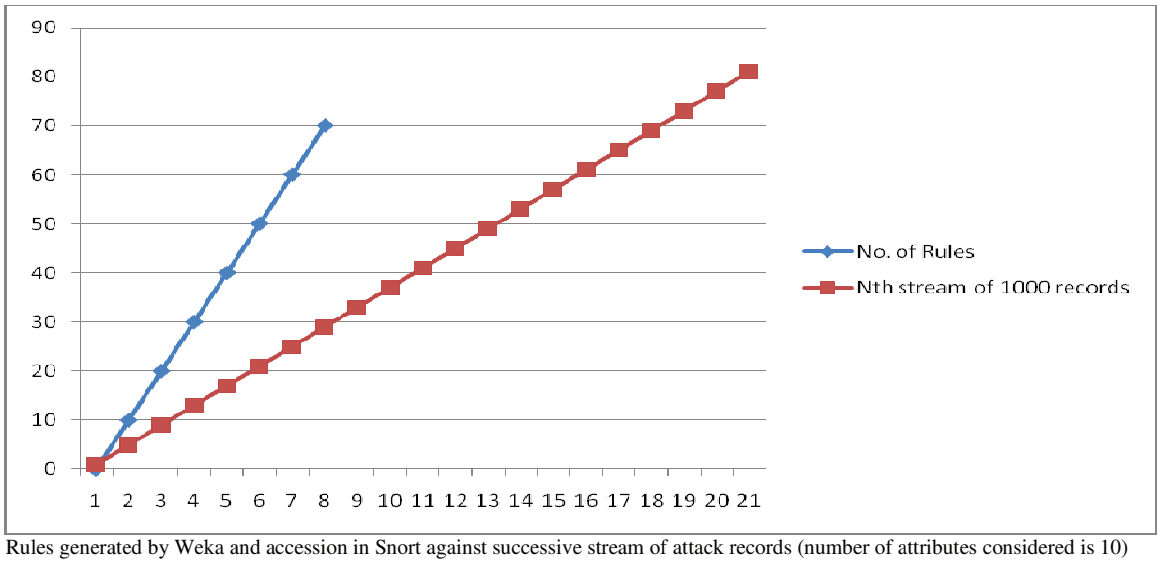

Fig.2 Rules generated by Weka and accession in Snort against successive stream of attack records (number of attributes considered is 10)

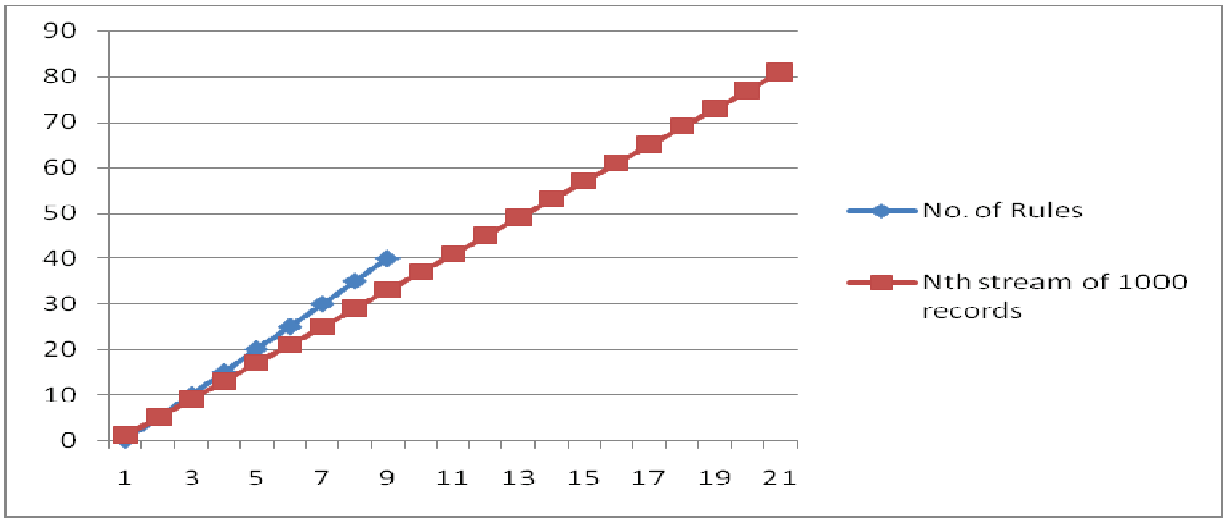

Fig.3 Rules generated by Weka and accession in Snort (after removing redundancy) against successive stream of attack records (number of attributes considered is 10)

VI. RESULTS AND DISCUSSION

Our test results clearly show the difference in the performance of the IDS using small signature database comparing to just enabling all signatures. In our environment with our specific configuration, by reducing the size of the database almost 97 times (546/6), on average, we were able to decrease the percentage of the dropped packets by 6.74 times. This is a significant improvement reducing the possibility of a real worm attack sneaking in the midst of dropped packets by the IDS while ensuring all imminent threats can be detected by the IDS.

VII. CONCLUSIONS

This paper has focused on the efficiency and performance of the new IDS: called signature-based multi- layer IDS using mobile agents. It then discusses the development of a new signature- based ID using mobile agents.The proposed system uses mobile agents to transfer rulebased signatures from large complementary dataset small signature database and then regularly update those databases with new signatures detected.It then describes an experimental setup used to perform the analysis for the verification and validation of proposed SIDS, so that it can be implemented in a large network environment. The results clearly indicate that proposed IDS model performs much better than normal systems with only one database for string signatures. Our experiments proved a significant

decrease in the packet drop rate, and as a result, a significant improvement in detecting threats to the network. The paper also highlights the foundations of IDS s and their advantages over other technologies, together with their general operational architecture, and provides a classification for them according to the type of processing related to the behavioural model for the target system. Further, the proposed model can be improved by providing a more comprehensive and automated system that can distribute, add and remove the signatures across databases of multiple IDS systems based on the frequency of their appearance and their level of threat to the network. Finally, we believe more research needs to be done to determine the criteria to choose the optimal training period for a network.

VIII. ACKNOWLEDGMENTS

First and foremost, I would like to extend my heartfelt gratitude to my guide and mentor Dr. Santosh Kumar Upadhyay, Professor, Department of Computer Science & Engineering, Galgotia College Of Engineering & Technology, for his invaluable advices, guidance, encouragement and for sharing his broad knowledge. His wisdom, knowledge and commitment to the highest standards inspired and motivated me. He has been very generous in providing the necessary resources to carry out my research. He is an inspiring teacher, a great advisor, and most importantly a nice person.

REFERENCES

[1] Internet System Consortium, "ISC Domain Survey: Number of Internet Hosts." http://ftp.isc.org/www/survey/reports/2010/04/. Last updated: May 12, 2010.
[2] Internet World Stats, "Internet User Statistics – The Internet Big Picture: World Internet Users and Population Stats." http://www.internetworldstats.com/stats.htm. Last updated: May 3, 2010.
[3] R. Miller, "Twitter is Latest Victim in Series of Attacks." Internet:http://www.datacenterknowledge.com/archives/2009/08/06/twitter-is-latest-victim-in-series-of-attacks/.Last updated: Aug 6, 2009.
[4] R. G. Bace, Intrusion detection: Sams, 2000.
[5] R. Base and P. Mell, Intrusion Detection Systems, National Institute of Standards and Technology (NIST), Special Publication, vol. 51, pp. 800-831, 2001.
[6] D. Dagon, X. Qin, G. Gu, W. Lee, J. Grizzard, J.Levine, and H. Owen, "Honeystat: Local worm detection using honeypots," RAID 2004, LNCS 3224,pp. 39-58, 2004.
[7] Ian H. Witten; Eibe Frank, Mark A. Hall (2011). "Data Mining: Practical machine learning tools and techniques, 3rd Edition". Morgan Kaufmann, San Francisco. Retrieved 2011-01-19.
[8] D.Bailey,Sneeze.(http://archives.neohapsis.com/archives/snort/2001-08/0180.html)
[9] J. Beale, A. R. Baker, B. Caswell, and M. Poor, Snort 2.1 Intrusion Detection: Syngress Media Inc, 2004.
[10] B. C. S. Ryu and J Kim, "design of packet detection system for high-speed network environment," in The 6th International Conference Advanced Communication Technology, pp. 496-498, 2004.