Modified Network Intrusion Protection System Using Knowledge Base

S. Jeya[1] Dr. K. Ramar[2]

ABSTRACT

Quickly increased complexity, openness, interconnection and interdependence have made computer systems more vulnerable and difficult to protect from malicious attacks. Network intrusion detection system plays a vital role in today's network. The attacks detection can be classified into either misuse or anomaly detection. The misuse detection cannot detect unknown intrusions whereas the anomaly detection can give false positive. Combining the best feature of misuse and anomaly detection one intelligent intrusion detection system (IIDS) is proposed which is able to detect not only the known intrusions but also the unknown intrusions. For detecting the unknown intrusions the proper knowledge base is to be formed after preprocessing the packets captured from the network. The preprocessing is the combination of partitioning and feature extraction. The partitioning of packets is based on the network services and extraction of attack feature is added to the knowledge base. The preprocessed attacks can be classified by using mining classification which will be given to rule builder. Once the unknown intrusions are detected that information's can be added to misuse detector for further detection. The network intrusion detection system should be adaptable to all type of critical situations arise in network.

[1]K.S.R. College of Engineering, Thiruchengode, Namakkal, Tamil Nadu, India, Email: mayej_s@yahoo.co.in

[2]Professor & HOD/CSE Dept., National Engineering College, Kovilpatti, Tamil Nadu, India.
E-mail: kramar_nec@rediffmail.com

Key words: Genetic Algorithm, Artificial Intelligence, Network Sniffer, local response and global response.

1. INTRODUCTION

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network. Intrusions are caused by attackers accessing the systems from the Internet, authorized users of the systems who attempt to gain additional privileges for which they are not authorized, and authorized users who misuse the privileges given them. Intrusion Detection Systems (IDSs) are software or hardware products that automate this monitoring and analysis process. Intrusion detection allows organizations to protect their systems from the threats that come with increasing network connectivity and reliance on information systems. Intrusion Detection Systems (IDS) attempts to detect intrusion through analyzing observed system or network activities. Based on the type of observed activities, IDS can be classified as network-based or host-based. IDS will raise alarms when it has detected misuse or anomaly. It may also report intrusions by emailing or paging system administrator and even disconnect intrusion connection locally.

There are three fundamental functions of IDS: Monitoring, Analysis, Response, and Generating Reports. The different sources of event information can be drawn from different levels of the system, with network, host, and

application monitoring system. Analysis makes sense of the events derived from the information sources, deciding when those events indicate that intrusions are occurring or have already taken place. The most common analysis approaches are misuse detection and anomaly detection. Misuse based systems can detect known attacks like virus detection systems, but they cannot detect unknown attacks [12& 11]. Misuse detection usually has highest detection rate and lower false positive rate than anomaly detection. Anomaly detection can detect unknown intrusions but its computational complexity is very high. The critical technique is to build profiles of normal usage. The advantages of these two can be combined to build intelligent IDS to cope up with the new unknown attacks. Responses can be generated involving some automated intervention on the part of the system, and involving reporting IDS findings to humans, who are then expected to take action based on those reports. Semi automation is required because in a large or busy network the network-based IDSs may fail to recognize an attack launched during periods of high traffic. The proposed technique is the combination of online and offline computation where online detection can be done using misuse detector and offline analysis can be done using anomaly detection using preprocessing and classification of unknown attacks depending on their impact to form the rules for future misuse detection. Here the computational complexity can be reduced when unknown intrusions are converted to known to make the intrusion detection system more intelligent and attack resistant.

2. Related work

A developmental view of system security [4] is an online network based IDS which uses association rules algorithm in detection. This technique has two phases: one is training phase and another is online phase. In training phase the attack free data is fed into the module whose output is rule based profile or normal activities. The training data, which contains attacks, are then fed to the other module for online detection using association rule mining. Though this technique overcomes the general problem of rule-based approach to update the rules for new attacks but there is no offline analysis to build the knowledge base for new attacking features and here the attack free training data is also analyzed which just wastes time. Also there is the possibility of false positive. Issue of high speed internet security and designing an integrated architecture for network content security gateways [5, 15] are able to detect unknown intrusions which overcome new intrusion attack rules. But, there is a possibility of false positives as no intelligent knowledge base is built offline.

Behavior based network security goes mainstream [2] perform real time monitoring of user activity on multiple target systems connected on a network. It consists of a misuse detection component as well as an anomaly detection component. The rule base misuse component employs expert rules to define known intrusive activities. The anomaly component is based on statistical approach, and it flags activities as attacks if they are largely deviant from the expected behaviors. By combing a statistical component and an expert system component, IDS increases the chances to detect intrusions. As no offline analysis is there to build patterns for unknown attacks, which can be used to build knowledge base for, future can degrade the intelligence of the IDS.

3. Intrusion protection system

There are two generally accepted categories of intrusion detection techniques: misuse detection and anomaly detection [14]. Misuse detection refers to techniques that characterize known methods to penetrate a system. These

penetrations are characterized as a 'pattern' or a 'signature' that the IDS look for. The pattern/signature might be a static string or a set sequence of actions. System responses are based on identified penetrations. Anomaly detection refers to techniques that define and characterize normal or acceptable behaviors of the system.

IDSs can also be divided into two groups depending on where they look for intrusive behavior: Network-based IDS (NIDS) and Host-based IDS. The former refers to systems that identify intrusions by monitoring traffic through network devices [13, 7]. A host-based IDS monitors file and process activities related to a software environment associated with a specific host. Some host-based IDSs also listen to network traffic to identify attacks against a host.

3.1. Knowledge Base

We need to collect enough historical data that includes both normal and anomalous network connections. This is the first part inside the Knowledge Base. The network sniffers analyze this data set and results are fed into GA. The final goal of applying GA is to generate rules that match only the anomalous connections. These rules are tested on historical connections and are used to filter new connections to find suspicious network traffic. In this implementation, the network traffic used for GA is a pre-classified data set that differentiates normal network connections from anomalous ones.

GA can be used to evolve simple rules for network traffic. These rules are used to differentiate normal network connections from anomalous connections. These anomalous connections refer to events with probability of intrusions. GA can be viewed as a tool to help generate knowledge for the knowledge base system. In order to detect such intrusions, both temporal and spatial information of network traffic should be included in the rule set. Then the Genetic Algorithm (GA) is executed and Artificial Intelligent (AI) is selecting the best rule, the rule set is generated. The rules stored in the rule set are usually in the following form:

if { condition } then { act }

Example

if {the connection has following information: source IP address 209.11.??.??; destination IP address: 130.18.176+?.??; source port number: 42335; destination port number: 80; connection time: 482 seconds; the connection is stopped by the originator; the protocol used is TCP; the originator sent 7320 bytes of data; and the responder sent 38891 bytes of data } then {stop the connection}

These rules are stored in a knowledge base to be used by the network intrusion detection system.

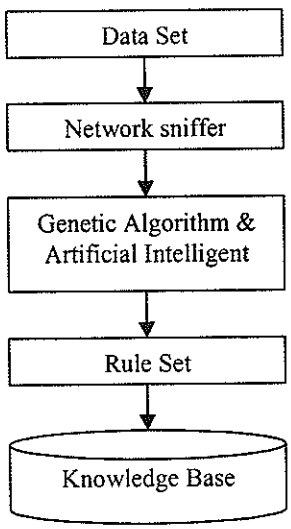

Figure 1: Knowledge Base

Knowledge base IDS analyze the traffic data passing through it and differentiate the traffic behaviors to be intrusive or normal [1]. The knowledge base system use

the rules stored in its knowledge base to detect and take actions when anomaly occurs in the traffic and/or undergoing some unauthorized activities. In brief, the rule set is applied to compare the patters in the traffic data with the patters customarily found during attack attempts. The IDS will alert the network administrator or security officer if the network is, or probably will be, under attack [6]. The alerts are usually sent together with detail information of the suspected intrusion. In general, the domain experts define the rules used in the rule-based system by their experiences and observations. They observe the behavior of individual attack and define the corresponding rules to detect the attack. Moreover, the subsequence actions of network administrator to deal with the attack are also defined. In some cases, the action may be taken by the IDS automatically [9].

4. System Architecture

This intrusion detection system is designed as shown in Figure 2 using two components: one is IDS host and another is the IDS server. IDS host components are network misuse detector and anomaly sensor. The misuse detector can detect known intrusion using well-known snort based technique [10]. The unknown attacks a re sensed using anomaly sensor. These sensed unknown attacked packets are sent to IDS server for further analysis. The detected known intrusions will generate alarm to all the hosts on the network. IDS hosts are responsible for local response. The IDS server components are anomaly detector, feature extractor, knowledge base and mining classifier. The feature extractor is used to extract attacking features from packets which can be upgraded to the knowledgebase. Depending on the attacking features the packets are classified according to their proximities [8]. The patterns are built for those attacking features. IDS server is responsible for global response.

4.1. Performance Measures

The performance of the system can be evaluated using two parameters: detection rate and false positive rate. The detection rate will be higher than the existing technique as both online and offline phases are there and depending on the extracted features the efficient knowledge base is constructed to make the system more adaptable to available network attacks [3]. The false positive rate also will be low as the knowledge up gradation is the continuation process. Knowledge-based system gets their power from the expert knowledge that has been coded into facts, rules, heuristics, and procedures. The knowledge is stored in a knowledge base separate from the control and inference components. This makes it possible to add new knowledge or refine existing knowledge without recompiling the control and inference program. Using previously stored intruder's characteristics easily recognize anomalies behavior.

5. Experiments

Network intrusion protection system using knowledge base results obtained; it is evident that the genetic algorithm designed for this experiment was

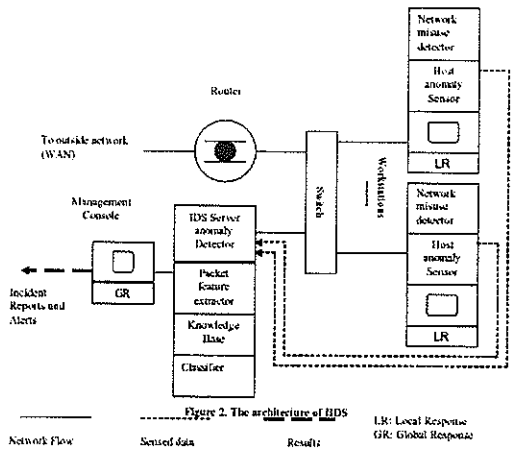

Figure 2. The architecture of IDS

over training data. The genetic algorithm was able to perform the mutation and evolution strategies according to the fitness function.

[* Filter does not support this file format | In-line.TIF *]

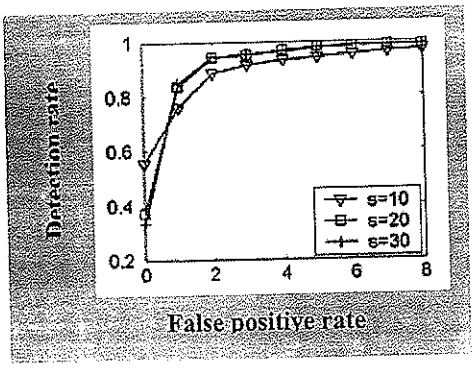

Figure 3: The best individual of each generation's correct detection rate vs. false positive rate

The genetic algorithm then successfully applied what it had learned to a real-world test case. The figure 3 shows the evolution of the best individual of each generation's correct detection rate vs. its false positive rate.

[* Filter does not support this file format | In-line.TIF *]

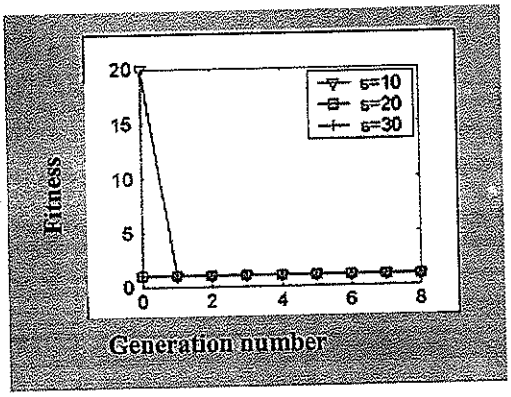

Figure 4: mean fitness value for the population vs. generation number.

The fitness value of the best individual for each generation had an approximate steady increase, at which point it is apparent that the best possible individual possible by the current methods had been created. Figure 4 shows the mean fitness value for the population. Fitness increases as evolution proceeds and the maximum fitness converges to 0.9. This shows that we can find better network intrusion by evolution and that the evolved networks can classify the training data at about 90% accuracy. However, without using knowledgebase the largest intrusion detection rate is only 0.7687% of attacks. Using network intrusion detection system based on knowledgebase the largest detection rate is 0.8734% of attacks. The results presented in this paper show that "Network intrusion protection system using knowledge base" are a promising method for the detection of malicious intrusions into computer systems.

6. Conclusions and Future Work

The network intrusion protection system using knowledge base is build an adaptive mechanism of detection by using feature extraction and classification mining. This system has significant advantage over the normal intrusion detection system for known attacks. The computational complexity is reduced as the offline analysis of unknown attacks is proposed. There is a less possibility of having false positive. This system can be implemented using distributed systems where single point of failure can be easily removed. Combining knowledge from different security sensors into a standard knowledge base is another promising area in this work.

Reference

[1] Chaker Katar, "*Combining Multiple Techniques for Intrusion Detection*", International Journal of Computer Science and Network Security, VOL.6 No.2B, February 2006.

[2] Geer D, *"Behavior based Network Security goes mainstream"*, IEEE Computer Society, Vol 39, issue 3, PP 14-17, March 2006.

[3] Huaizhi Li, Mukesh Singhal, *"Trust Management in Distributed System"*, IEEE Computer Society, Vol 40, issue 2, PP 45-53, Feb 2007.

[4] Huntley C L, *"A developmental view of System security"*, IEEE Computer Society, Vol 39, issue 1, PP 113-114, Jan 2006.

[5] Jungck P, Shim ssy, *"Issues in high speed internet security"*, IEEE Computer Society, Vol 37, issue 7, PP 36-42, July 2004.

[6] Kemmerer R A, Vigna G, *"Hi DRA: Intrusion Detection for internet Security"*, Proceedings of the IEEE, Vol 93, issue 10, PP 1848-1857, Oct 2005.

[7] Kemmerer R A, Vigna G, *"Intrusion detection: a brief history and overview"*, IEEE Computer Society, Vol 35, issue 4, PP 27-30, April 2002.

[8] Leckie T, Yasinsac A, *"Metadata for Anomaly based Security Protocol attack Detection"*, IEEE Transaction on Knowledge and Data Engineering, Vol 16, issue 9, PP 1157-1168, Sept 2004.

[9] Mishra A, Nadkarni K, *"Intrusion Detection in wireless ad-hoc Network"*, IEEE Wireless Communications, Vol 4, issue 1, PP 48-60, Feb 2004.

[10] Nong Ye, Farley T' *"A Scientific approach to cyber attack detection"*, IEEE Computer Society, Vol 38, issue 11, PP 55-61, Nov 2005

[11] Sang Long Pao T, Po Wei Wang, *"Net flow based Intrusion Detection System"*, IEEE international Conference on Networking sensing & Control, Vol-2, PP 731-736, 2004.

[12] Sang Jun Han, Sung Bae Cho, *"Evolutionary neural network for anomaly detection based on the behaviour of a program"*, IEEE Transaction on Systems, Man and Cybernetics, Part B, Vol 36, issue 3, PP 559-570, June 2006.

[13] Sarasamma S T, Zhu Q A, Huff J, *"Hierarchical Kohonenen net for anomaly detection in Network Security"*, IEEE transaction on Man and Cybernetics, Vol 35, issue 2, PP 302-312, April 2005.

[14] Vijairagavan V, Shah D, Galgali P, Shah D, Srinivasan V, *"Marking Technique to isolate boundary router and attacker"*, IEEE Computer Society, Vol 40, issue 2, PP 54-58, Feb 2007.

[15] Ying Dar Lin, Chih Wei Jan, Po Ching Lin, Yuan Cheng Lai, *"Designing an integrated Architecture for Network Content Security Gateways"*, IEEE Computer Society, Vol 39, issue 11, pp 66-72, Nov 2006.

Author's Biography

S.Jeya, has obtained her B.Sc., M.C.A., and M.Phill., degree from Manonmaniyam Sundaranar University in 1994, 1997 and 2004 respectively. She worked as Software Engineer at Bangaloor (1997-99) and Head of the MCA department at Rajaas Engineering College, Tirunelveli (1999-2006). Now she has been working as Assistant Professor in K.S.R. College of Engineering Tiruchengode, and pursuing her research work in Mother Teresa Women's University. Her interesting research area is "Network Security". Her research articles published in various International/ National journals. She is a life member of ISTE, CSI.

Dr. K. Ramar, has obtained his B.E., M.E. and PhD degree in 1986, 1991 and 2001 respectively. He is working as Professor and Head of the CSE department at National Engineering College, Kovilpatti. He has more than 20 years of experience in teaching and research. He is also a member of various scientific and professional societies. His interesting research area is "Image processing" and "Network Security". His research articles published in various International/National journals.