World Academy of Science, Engineering and Technology
International Journal of Humanities and Social Sciences
Vol:1, No:11, 2007

Hybrid Intelligent Intrusion Detection System

Norbik Bashah, Idris Bharanidharan Shanmugam, and Abdul Manan Ahmed

Abstract**—**Intrusion Detection Systems are increasingly a key part of systems defense. Various approaches to Intrusion Detection are currently being used, but they are relatively ineffective. Artificial Intelligence plays a driving role in security services. This paper proposes a dynamic model Intelligent Intrusion Detection System, based on specific AI approach for intrusion detection. The techniques that are being investigated includes neural networks and fuzzy logic with network profiling, that uses simple data mining techniques to process the network data. The proposed system is a hybrid system that combines anomaly, misuse and host based detection. Simple Fuzzy rules allow us to construct if-then rules that reflect common ways of describing security attacks. For host based intrusion detection we use neural-networks along with self organizing maps. Suspicious intrusions can be traced back to its original source path and any traffic from that particular source will be redirected back to them in future. Both network traffic and system audit data are used as inputs for both.

Keywords**—**Intrusion Detection, Network Security, Data mining, Fuzzy Logic**.**

I. Introduction

INFORMATION has become an organization's most precious asset. Organizations have become increasingly dependent on the information since more information is being stored and processed on network-based systems. The wide spread use of e-commerce, has increased the necessity of protecting the system to a very high extend. Intrusion detection has become an integral part of the information security process. But it is not technically feasible to build a system with no vulnerabilities; intrusion detection continues to be an important area of research.

The remaining part of this paper is organized as follows: Section 2 gives an overview of current Intrusion Detection Systems; Section 3 elucidates the overview of system architecture and our goals. Section 4 describes about the usage of Fuzzy and data mining techniques. Section 5 explains about the usage of Self Organized Maps in our model and Section 6 summarizes the work and points out what we will do in future

Manuscript received May 20, 2005.

Dr. Norbik Bashah Idris, is with Centre for Advanced Software Engineering, University Teknologi Malaysia , Jalan Semarak , Kualalumpur Malaysia 54100.

Bharanidharan Shanmugam, is with Centre for Advanced Software Engineering University Teknologi Malaysia , Jalan Semarak , Kualalumpur Malaysia 54100 (phone: 00-60-16-2473454; e-mail: s.bharani@gmail.com).

Assoc. Prof. Abdul Manan Ahmed, is with Faculty of computer science and Information systems, Universiti Teknologi Malaysia, Johor, Malaysia.

II. Overview of Current Intrusion Detection Systems

Intrusion detection is defined [1] as the process of intelligently monitoring the events occurring in a computer system or network, analyzing them for signs of violations of the security policy. The primary aim of Intrusion Detection Systems (IDS) is to protect the availability, confidentiality and integrity of critical networked information systems. Intrusion Detection Systems (IDS) are defined by both the method used to detect attacks and the placement of the IDS on the network. IDS may perform either misuse detection or anomaly detection and may be deployed as either a network-based system or a host-based system. This result in four general groups: misuse-host, misuse-network, anomaly-host and anomaly-network. Misuse detection relies on matching known patterns of hostile activity against databases of past attacks. They are highly effective at identifying known attack and vulnerabilities, but rather poor in identifying new security threats. Anomaly detection will search for something rare or unusual by applying statistical measures or artificial intelligence to compare current activity against historical knowledge. Common problems with anomaly-based systems are that, they often require extensive training data for artificial learning algorithms, and they tend to be more computationally expensive, because several metrics are often maintained, and these need to be updated against every systems activity. Some IDS combine qualities from all these categories (usually implementing both misuse and anomaly detection) and are known as hybrid systems. Artificial Intelligence techniques have been applied both to misuse detection and also for anomaly detection. SRI's Intrusion Detection Expert System (IDES) [2] encode an expert's knowledge of known patterns of attack and system vulnerabilities as if-then rules. Time-based Inductive Machine (TIM) for intrusion detection [3] learns sequential patterns. Recently, techniques from data mining area have been used to mine normal patterns from audit data [4,5,6]. Several approaches apply artificial neural networks in the intrusion detection system have been proposed [7, 8, 9]. NeGPAIM [10] based on trend analysis, fuzzy logic and neural networks to minimize and control intrusion. Existing intrusion detection especially commercial intrusion detection systems that must resist intrusion attacks are based on misuse detection approach, which means these systems will only be able to detect known attack types and in most cases they tend to be ineffective due to various reasons like non-availability of attack patterns, time consumption for developing new attack patterns, insufficient attack data etc,

The performance of the current intrusion detection systems can be improved by utilizing a hybrid intrusion detection which combines anomaly and misuse analysis. The strategy

will be discussed in more detail in the subsequent sections.

III. Goals and Proposed Architecture

Our aim is to design and develop an Intelligent Intrusion Detection System (IIDS) that would be accurate, low in false alarms, not easily cheated by small variations in patterns, adaptive and be of real time.

In our model we use SNORT [11], a leading and famous open source packet sniffer. The data processor and classifier summarizes and tabulates the data into carefully selected categories i.e. the attack types are carefully correlated. This is the stage where a kind of data mining is performed on the collected data. In the next stage, the current data is compared with the historical mined data to create values that reflect how new data differs from the past observed data. The inference engine is MySQL based and is bi-directional. Its inference speed is faster than any other text-oriented inference. Based on the facts from the analyzer, the decision will be taken whether to activate the detection phase or not. If the detection phase is activated then an alert will be issued and the tracer phase will be initiated. This phase will trace back to the intruders original source address location. Based on the initial research work we conclude Sleepy watermark [12] tracing method by has proved to be very efficient with in tracing the original source. This tends to be the most tedious phase of the project. Once the original path has been identified and verified then all the attacks from that particular host will be redirected to their source. SNORT_INLINE [13] has proved to be the best in changing the appropriate packet values.

The architecture shown in Fig 1 is now under construction. Our preliminary research work demonstrates that fuzzy network profiling with data mining can and will provide efficient solution for Intrusion problems. In this paper we have focused about the usage of fuzzy, Data mining and Self Organized Maps in our proposed model.

IV. Intrusion Detection via Fuzzy Logic and Data Mining

Data mining is one of the hot topics in the field of knowledge extraction from database. Data mining is used to automatically learn patterns from large quantities of data. Mining can efficiently discover useful and interesting rules from large collection of data. Fuzzy logic provides a powerful way to categorize a concept in an abstract way. The advantage of fuzzy logic is that it allows representation of overlapping categories. We are combining techniques from fuzzy logic and data mining for anomaly detection and it helps us to create more abstract patterns.

A. Fuzzy Logic

Fuzzy concepts derive from fuzzy phenomena that commonly occur in the natural world. For instance "rain" is a fuzzy statement of "Today raining heavily" since there is no clear boundary between "rain" and "heavy rain". In intrusion detection suppose we want to write a rule as given below we need a reason about a quantity such as the number of different destination IP addresses in the last 2 seconds.

IF *the number of different destination addresses during the last n seconds was high*
THEN *an unusual situation exists.*

Fuzzy logic, which is utilized, is a superset of conventional logic that has been extended to handle the concept of partial truth, which lies between completely true and completely false.

B. Data Mining Methods

Data mining methods are used to automatically discover new patters from a large amount of data. Association rules have been successfully used to mine audit data to find normal patterns for anomaly intrusion detection [14].

C. Association Rules

The association rule mechanism proposed by Agrawal is a most popular tool. Agrawal and Srikant [14] developed the Apriori Algorithm for mining association rules. The Apriori Algorithm needs confidence (to represent minimum confidence) and support (to represent minimum support). These two values determine the degree of association that must hold.

D. Fuzzy Association Rules

To efficiently use the Apriori algorithm of Agrawal and Srikant [15] for mining association rules, quantitative variables should be partitioned into discrete categories. This leads to "sharp boundary problem" in which a very small change in value causes an abrupt change in category. To address this problem fuzzy association rules was developed by Kuok, Fu and Wong [16]. We modify the algorithm [16] by introducing a normalization factor to ensure that every transaction is counted only one time.

V. Host Based Intrusion Detection

Previous researches have proved that usage of SOM [17] is very efficient in unsupervised learning. In order to fulfill our aim for automating the process of Intrusion detection actions, we first will try to identify the behavior/ characteristic of common user. This information is stored for later usage to find out if any user has unusual or different characteristics labels.

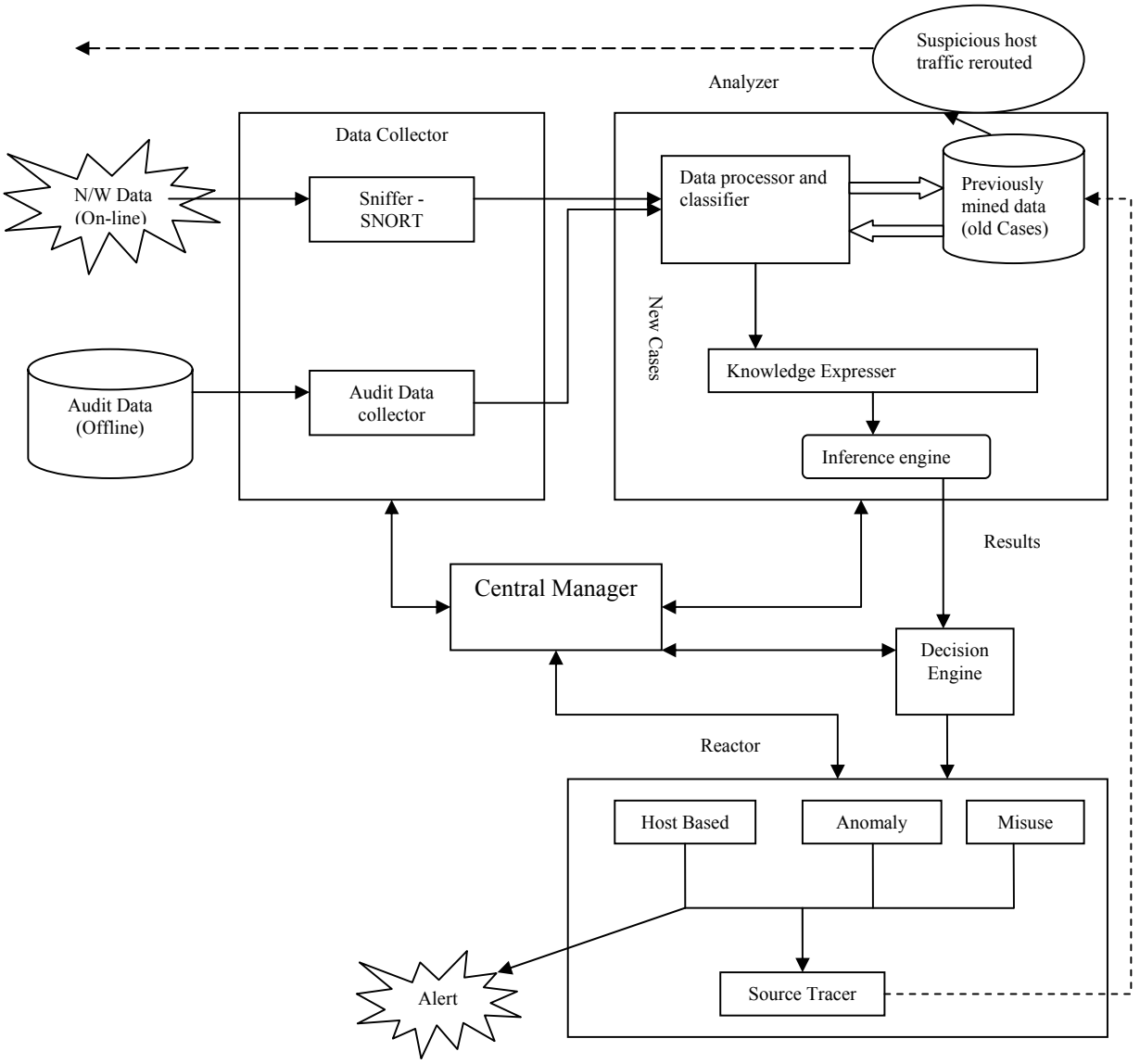

Fig. 1 Proposed IIDS

VI. Summary and Future Work

We have combined fuzzy logic with data mining to provide efficient technique for anomaly based intrusion detection and used SOM for host based intrusion detection. This model is now at infant stage of development. Our long term goal is to make this system to implement with Artificial Immune systems. More results could be obtained once we finish deploying the system.

References

[1] Bace R.G Intrusion Detection, *Technical Publishing* (ISBN 1-57870-185-6).

[2] Lunt. T. "Detecting intruders in computer systems". *Conference on auditing and computer technology*, 1993.

[3] Teng, H., K.Chen and S.Lu "Adaptive real time anomaly detection using inductively generated sequential patters". *IEEE computer society symposium on research in security and privacy, California*, IEEE Computer Society 278-84 1990.

[4] Lee, S.Stolfo and K.Mok "Mining audit data to build data to build intrusion detection models". Fourth international conference on knowledge discovery and data mining, New York, AAAI Press 66-72, 1998.

[5] Mukkamala, R., J.Gagnon and S.Jaiodia Integrating data mining techniques with intrusion detection methods. *Research Advances in Database and Information systems security*, 33-46, 2000.

[6] S Stolfo, Lee, Chan. "Data mining-based Intrusion detectors : An overview of the Columbia IDS Project" *SIGMOD Record* Vol 30, No 4, 200.

[7] Debar, M. Becker, D.Siboni. "A neural network component for an intrusion detection system". *IEEE Computer Society Symposium on Research in Computer Security and Privacy*, 240-250 1992.

[8] Tan.K "The Application of Neural Networks to UNIX Computer security". *IEEE International conference on Neural Networks* Vol 1, 476-481 1995

[9] Wang J, Wang Z, Dai K, "A Network intrusion detection system based on ANN", *InfoSecu04, ACM* 2004(ISBN1-58113-955-1)

[10] Botha.M, Solms R, Perry K, Loubser E, Yamoyany G "The utilization of Artificial Intelligence in a Hybrid Intrusion Detection System", *SAICSIT*, 149-155 2002

[11] www.snort.org

[12] Xinyuan Wang, Douglas S. Reeves, S. Felix and Jim Yuill, " Sleepy Watermark Tracing : An active Network Based Intrusion Response Framework" *IEEE Information Survivability Workshop*, October 2003

[13] http://snort-inline.sourceforge.net/

[14] Lee, W.,S Stolfo and K. Mok 1998 "Mining audit data to build intrusion detection models". *Fourth international conference on knowledge discovery and data mining*, New York August 1998

[15] Agrawal, R., and R.Srikant 1994 "Fast algorithms for mining association *rules 20"h international conference on very large databases* September 1994

[16] Kuok, C., A.Fu and M. Wong "Mining fuzzy association rules in databases" *SIGMOD* Record 17 (1) 41-46.

[17] Peter Lichodzijewski A.Nur Zincir-Heywood, Malcolm I. Heywood "Host-based Intrusion Detection using Self-Organizing maps" *IEEE Communications* 2002.