GA based Network Security System for Medical Image Transmission Through Web

K.A.Mohamed Junaid[1]

Professor and Head, Department of EIE, RMK Engineering College, Kavaraipettai – 601206, Tamilnadu, INDIA

Summary
Intrusion Detection System (IDS) has been developed using genetic algorithm, in which new anomalies are detected to have intrusion free network for secure medical image transmission. The aim of this work is to block unauthorized users / hackers to protect the medical images during transmission through web. The genetic algorithm starts with a population that has randomly selected rules (Goldberg 1989). The population will be evolved by using the crossover and mutations. Due to the effectiveness of the evaluation function, the succeeding populations are biased towards the rules that match with the intruders behaviours At the end of the execution of algorithm , new intruder's data are generated and added into the IDS rule base as new intruder data. In the IDS developed, generation of new rules is obtained using GA, which tend to incorporate improved network security system. In the case of Data Encryption and water marking techniques, the image data content can be protected from the unauthorized users. But, they can not be prevented from altering the data. By using GA, unauthorized users / hackers are not allowed in the network to visualize the medical images transmitted thro' the web.

Key words:
Intrusion Detection System, Genetic Algorithm, Network Security, Medical Image.

1. Introduction

Intrusion is an act of unauthorized entry into the system by the intruder. Intruders can be classified into two categories, namely Outside intruders and Inside intruders. Intruders from outside the network, attack through web servers, forward spam through e-mail servers, etc. These outside intruders may also attempt to go around the firewall to attack machines on the internal network. Outside intruders may come from the Internet, dial-up lines, physical break-ins, or from partner network that is linked to corporate network like vendor, customer, reseller, etc., Intruders who legitimately use the internal network is known as inside intruders. These include users who misuse privileges or who impersonate higher privileged users like usage of others terminal. A frequently quoted statistic is that 80% of security breaches are committed by inside intruders (Stephen Northcutt et al 2002).

1.1 Need for Network Security System using Intrusion Detection system (IDS)

Security has been a vital concern in many areas since computers have been networked together with a very large user source and with multivariate intentions. With the rapid growth of internet communication and availability of tools to intrude the network, network security has become indispensable. Security threat comes not only from external intruder but also from internal misuse (Anderson 1980). Current security policies do not sufficiently guard data stored in an information system against privileged users.
Intruders who have gained super-user privileges can perform malicious operations and disable many resources in the information system. Many other mechanisms and technologies like firewalls (Bellovin 1994), encryption (Naccache 2007), authorization (Gal and Atluri 2000,), vulnerability checking and access control policies (Ryutov et al 2003) can offer security but they are still susceptible for attacks from hackers who take advantage of system flaws and social engineering tricks. In addition, computer systems with no connection to public networks remain vulnerable to disgruntled employees (Zhang et al 2010) who misuse their privileges. These observations result in the fact that much more emphasis has to be placed on Intrusion Detection System (IDS) to protect the system from intruders (Lunt 1993).
An IDS (Denning 1987, McHugh 2001, Qin et al 2002, Esponda et al 2004) is a security system that monitors all activities on the network and detects any attempts to compromise the security policy. This is in contrast to technologies like firewalls that contain fixed set of rules that determine an attacker's behaviour (Joshi et al 2001) since it analyses the user behaviors dynamically.

1.2 GENETIC ALGORITHM (GA)

Among various heuristic methods, Genetic Algorithms (GA) is more promising since it differs in many ways from other heuristics. First, GA works on population of possible solutions, while other heuristic methods use a single solution in their iterations.
Second, most heuristics are probabilistic or stochastic, in nature and hence they are not deterministic. On the other

Manuscript received September 5, 2013
Manuscript revised September 20, 2013

hand, each individual in the GA population contributes well to obtain a possible solution to the problem.

In GA, the algorithm starts with a set of possible solutions represented by chromosomes called population. Potential solution to specific problem is encoded in the form of chromosome. Solutions from one population are taken and used to form a new population. Solutions which are selected to form new solutions called offs.pring and are selected according to their fitness value. The more suitable they are the more chances they have to reproduce. Finally, GAs are more suitable in reducing the search space. Therefore, the convergence of the algorithm is faster when GA is employed.

1.2.1 Properties of GA

- GA works with a coding of the parameter set and does not work with the parameters themselves.
- GA search from a population of points and does not search from a single point.
- GA use a objective function information and does not use derivatives.
- GA use probabilistic transition rules and does not use deterministic rules (Melanie Mitchel 1998).

1.2.2 Parameters in GA

There are many parameters to consider for the application of GA. Each of these parameters heavily influences the effectiveness of the genetic algorithm. Evaluation parameters and crossover mutation parameters are the important parameters.

1.2.3 Crossover and Mutation

Traditional genetic algorithms have been used to identify and converge populations of candidate hypotheses to a single global optimum. For this problem, a set of rules is needed as a basis for the IDS. As mentioned earlier, there is no way to clearly identity whether a network connection is normal or anomalous just using one rule. Multiple rules are needed to identify unrelated anomalies, which mean that, several good rules are more effective than a single best rule. Another reason of finding multiple rules is because there are so many network connection possibilities. Using the genetic algorithm, local maxima, a set of 'good enough' solutions is found as opposed to the global maximum the best solution. The niching techniques are used to find multiple local maxima. It is based on the analogy to nature in that within each environment, there are different subspaces or niches that can support different types of life. In a similar manner, genetic algorithm can maintain the diversity of each population in a multimodal domain, which refers to domains requiring the identification of multiple optima.

2. GA BASED NETWORK SECURITY SYSTEM USING IDS

The different machine learning techniques, such as finite state machine, decision trees and GA can be used to generate artificial intelligence rules for IDS. One network connection and its related behavior can be translated to represent a rule which is used to find whether a real-time connection is considered as an intrusion. These rules can be modeled as chromosomes inside the population. The population evolves until the evaluation criteria are met. The generated rule set can be used as knowledge inside the IDS for judging whether the network connection and related behaviors are potential intrusions. Using autonomous agents like security sensors and applied Artificial Intelligence (AI) techniques, genetic algorithms can be evolved. Agents are modeled as chromosomes and an internal evaluator is used inside the every agent.

In the approaches described above, the IDS can be viewed as a Rule-Based System (RBS) and GA can be viewed as a tool to help generate knowledge for the RBS. These approaches have some disadvantages. In order to detect intrusive behaviors for a local network, network connections should be used to define normal and anomalous behaviors. Sometimes an attack can be as simple as scanning for available ports in a server or a password guessing. But typically they are complex and are generated by automated tools that are freely available from the internet. An example can be a Trojan horse or a backdoor that can run for a period of time, or can be initiated from different locations. In order to detect such intrusions, both temporal and spatial information of network traffic should be included in the rule set. The current GA applications do not address these issues extensively. This research work is implemented to model network connection information as chromosomes and the parameters in genetic algorithm are defined. In this, both temporal and spatial information of network traffic is included in the rule set to detect intrusions initiated from different locations.

2.1 System Architecture

The system architecture for the implementation of this research work is shown in Figure 1

The Information Systems Technology Group (IST) of Lincoln Laboratory, under Defense Advanced Research Projects Agency (DARPA) and Air Force Research Laboratory (AFRL) sponsorship has collected and distributed the first standard corpora for evaluation of

computer network intrusion detection systems. Such evaluation efforts have been carried out in 1998 and 1999.

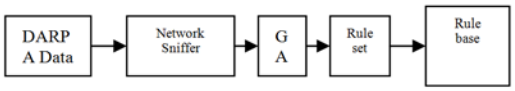

Figure 1. Architecture of applying GA into intrusion detection

These evaluations measured probability of detection and probability of false alarm for each system under test. These evaluations contributed significantly to the intrusion detection research field by providing direction for research efforts and an objective calibration of the technical state of the art. They are of interest to all researchers working on the general problem of workstation and network intrusion detection. The evaluation was designed to be simple, to focus on core technology issues, and to encourage the widest possible participation by eliminating security and privacy concerns, and by providing data types that were used commonly by the majority of intrusion detection systems. Off-line data sets are available to provide researchers with extensive examples of attacks and background traffic. Two data sets (1998 and 1999) are the result of the DARPA Intrusion Detection Evaluations are available and can be downloaded from Lincoln laboratory web portal.
The historical data that includes both normal and anomalous network connections are collected and dataset is formed. The dataset for testing IDS is represented in the TCP dump in binary format. This is the first part inside the system architecture (Dimittris Pendarakis et al 2001). The network sniffers analyze this data set and results are fed into GA for fitness evaluation. Then the GA is executed and the rule set is generated. These rules are stored into a database to be used by the IDS.

2.2 Rule Formation Parameters

The following information is used to formulate the chromosome structure. Each chromosome is encoded as a possible parameter. Using these parameters, the possible IDS can be created that would try to detect the anomaly occurring in the network.

1) Source and Destination IP Address.
2) Source and Destination Port Number.
3) Action: “Allow or Deny / Forward or Drop” Packets
4) Protocol Selection
5) Payload of the originator and responder
6) Time duration of the transaction etc.

2.3 REALIZATION

Genetic algorithms 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. The rules stored in the rule base in the following form

if { condition } then { act }

For the problem shown above, the condition usually refers to a match between current network connection and the rules in IDS to indicate the probability of an intrusion. This is achieved by using the source and destination IP addresses and port numbers used in TCP/IP network protocols, duration of the connection and protocol used. The act field usually refers to an action defined by the security policies within an organization, such as reporting an alert to the system administrator, stopping the connection, logging a message into system audit files.
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.

2.4 Methodology

The genetic algorithm starts with a population that has randomly selected rules. The population will be evolved by using the crossover and mutations operators. Due to the effectiveness of the evaluation function, the succeeding populations are biased toward rules that match intrusive connections. Ultimately as the algorithm stops, rules are selected and added into the IDS rule base.
The design methodology used in this research work is described as follows:

- The historical data that includes both normal and anomalous network connections are collected and dataset is formed. The dataset for testing IDS is represented in the Tcp dump in binary format.
- The Network sniffers analyze this data set and results are fed into GA for fitness evaluation.
- Then the GA is executed using crossover and mutation selecting the best rule, the rule set is generated. These rules are stored in a database to be used by the IDS.
- The rule based expert system in ‘if- then’ structure is used to monitor the network and system parameters continuously and important abnormalities are identified.
- Identification of abnormalities are clearly defined by set of rules with various attributes.

- The chromosome structure with 57 genes for the corresponding connection is generated and mutation and evolution strategies are performed by GA.
- Since attributes in a rule includes IP addresses and port numbers, the spatial information is included in the rules. The inclusion of the duration time of a network connection in the chromosome ensures incorporation of temporal information for network connections.

2.5 Simulation Output Results

In this work, example value attributes with source address 172.16.36.4 and destination IP address 172.16.36.18 are considered as potential intrusion within the local network. The chromosome structure is obtained for these attributes and included in the rule set. The output screen shows the output obtained by running the IDS algorithm in which the connection is stopped. This is illustrated as Drop action in the simulation output for these Source and destination IP address. Similarly, for various Source and destination IP addresses are taken into consideration and the same Drop action is performed by the system to stop the connection for simulated potential intrusions. The following Figure2 shows the simulated output for various IP addresses.

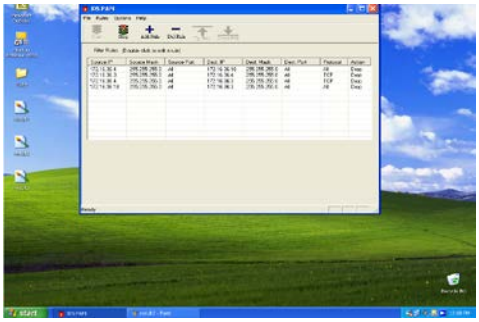

Figure2. Source and destination IP address simulation output

Similarly, attributes of smurf attack are simulated and identified by the system as intrusion and the new rules are generated to stop the connection after identifying the attack. Figure3 shows the output screen for detecting such anomalies. Figure 4 shows the output screen for creating new rules for detection new anomalies after identifying the anomalies.

3. Discussion

Medical Image Transmission Network Intrusion Detection System (IDS) has been developed using genetic algorithm, in which new anomalies are detected to have intrusion free network for secure image transmission. In these IDS, new rules will be generated due to the time evolving nature of the GA, which ensure a secure network system. Creation of new rules will enable the IDS to detect new anomalies without enhancing the system configuration or the algorithm.

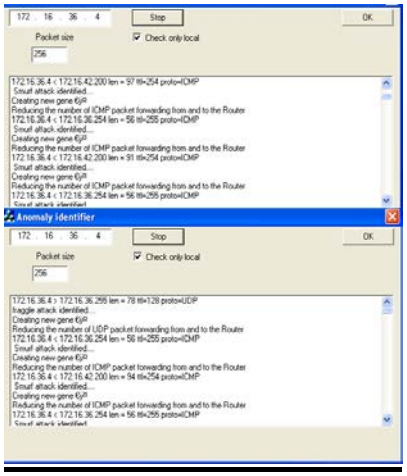

Figure 3. Smurf attack identification

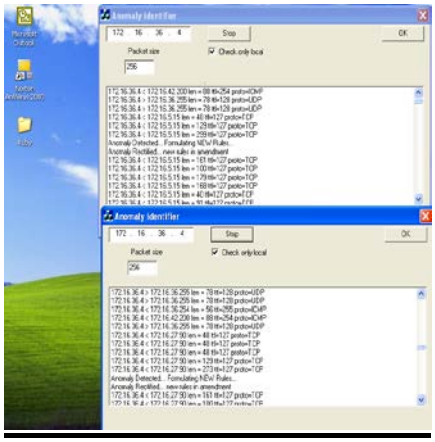

Figure 4 Creation of new rules output

Asymmetric encryption algorithm is developed to provide secured access by the user (Sergey Khludov et al 2000). However the intrusion detection system is not incorporated for improved security. Independent Component analysis method for secure image transmission is developed (Sungjin Park et al 2003). In that work, unique user ID, server and client IP addresses are not provided for enhanced security for image transmission.

Intrusion Detection and Prevention to provide internet security has been developed various attacks (Tront and Marchany 2004). Methodology for multi-stage network attack analysis has been developed in which applications related to network security management is discussed (Jerald Dawkins et al 2004). Network anomaly detection

with few attacks has also been developed (Gonzalez et al 2003). However, in these methods, the identification of new anomalies are not developed. The feasibility of the present method is compared with the existing methods and the present method yield with better results.

REFERENCES

[1] Bellovin, S.M.(1994)"Network firewalls", IEEE Communications Magazine, Vol.32, pp. 50-57.

[2] Bezroukov and Nikolai (2003), 'Intrusion Detection (general Issues)', Softpanorama: Open Source Software Educational Society, Mississippi.

[3] Brian Nutter and Sunanda Mitra (2007), 'Secure Medical Image Retrieval Over the Internet', IEEE International conference on Multimedia, Beijing, pp. 691-694.

[4] Gal, A. and Atluri, V. (2000) "An Authorization model for temporal data," in Proceedings of the Seventh ACM Conference on Computer and Communication Security, Athens, Greece, pp 144-153.

[5] Gonzalez F., Gomez J., Madhavi Kaniganti and Dipankar Dasgupta (2003), 'An Evolutionary Approach to Generate Fuzzy Anomaly (Attack) Signatures', Information Assurance Workshop, IEEE Systems, Man and Cybernetics Society, New York, pp. 251-259.

[6] Jerald Dawkins and John Hale (2004), 'A Systematic Approach to Multi-Stage Network Attack Analysis', Proceedings of the 2nd IEEE International Information Assurance Workshop, Charlotte, NC, pp.48-56.

[7] Lunt, T. (1987) "Detecting intruders in computer systems," in Proceedings of Conference on Auditing and Computer Technology, pp. 1-17, 1993. Denning, D.E. "An intrusion-detection model", IEEE Transaction on Software Engineering, Vol.13, pp. 222-232.

[8] Sergey Khludov, Lutz Vorwerk and Christoph Meinel (2000), 'Internet-Orientated Medical Information System for Dicom-Data Tranfer, Visualization and Revision', IEEE International Workshop on Biomedical Circuit and Systems, Pacific Grove, CA, pp. s3.3-s3.12.

[9] Tront J.G. and Marchany R.C. (2004), 'Internet Security: Intrusion Detection and Prevention', IEEE Proceedings of the 37th International Conference on System Sciences, Hawaii. P.2491.

[10] Zebbiche (2008) "An efficient watermarking technique for protection of finger print images". EURASIP Journal on Information Security, Vol.2008, pp1-21.

[11] Zhang, N., Yu, W., Fu, X. and Das, S.K. (2010) "Maintaining defender's reputation in anomaly detection against insider attacks", IEEE Transactions on Systems, Man, and Cybernetics. Part B, Cybernetics, Vol.40, No.3, pp.597-611.

Mohamed Junaid received the B.E. degree in Electronics and Communication Engineering from Bharathiar University in 1988 and M.E. and PhD. degrees from Anna University in 1991 and 2011 respectively. He now with RMK Engineering College, Tamilnadu, India as Professor and Head Electronics and Instrumentation Engineering Department.