International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
www.ijset.com, Volume No.1, Issue No.2 pg:17-21 01 April 2012

Simulation & Assessment of Network Security Based on System Dynamics

Manoj Patel, Dr.Manish Shrivastava, Kavita Deshmukh

Department of Information Technology,

Laxmi Narain College of Technology, Bhopal M.P. India

Corresponding Email: manoj.patel85@gmail.com

Abstract: Security is one of the most important aspects while designing a Computer Network, the issue is gaining more & more attention as the Network area is growing, the robust Security mechanism is required especially for the networks involving ecommerce & confidential data. Till now there are number of solutions are available to defend against attack but the defending system always consume some of system resources & security checks always imposes delays on the communication hence to overcome these problem this paper presents an parallel approach to generate alert signals which can be used as input for re-tuning the security at the desired level so the security policy could be configured dynamically on the basis of current threat type & seriousness , the proposed system monitors the system dynamics like types of packets, delay, drop rate, buffer overflow etc. to detect the threat level. The classification of the system state is done on the basis of clustering.

Keywords: Network Security, security threats, clustering.

1. Introduction

In the field of networking, the area of network security [1] consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources. Network security involves the

authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.

Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

2. Literature Review

Although different detection approaches exist for threat alarming in general terms all of them consist of the following basic modules or stages (Fig. 1)

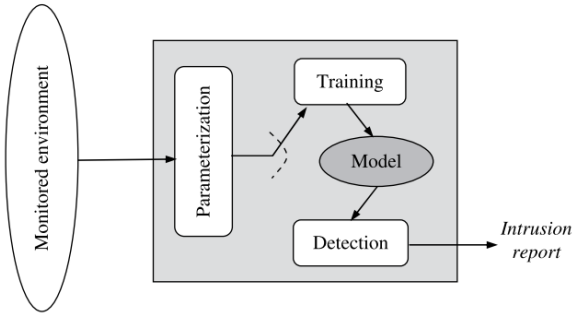

Figure 1.Basic functional architecture detection system [2].

Parameterization: In this stage, the observed instances of the target system are represented in a pre-established form.

Training stage: The normal (or abnormal) behavior of the system is characterized and a corresponding model is built. This can be done in very different ways, automatically or manually, depending on the type of classification.

According to the type of processing related to the ‘‘behavioral’’ model of the target system, anomaly detection stage: Once the model for the system is available, it is compared with the (parameterized) observed traffic. If the deviation found exceeds (or is below, in the case of abnormality models) a given threshold an alarm will be triggered.

Detection techniques can be classified into three main categories (Lazarevic et al., 2005) (see Fig. 2): statistical-based, knowledge-based, and machine learning-based. In the statistical-based case, the behavior of the system is represented from a random viewpoint. On the other hand, knowledge-based techniques try to capture the claimed behavior from available system data (protocol specifications, network traffic instances, etc.). Finally, machine learning schemes are based on the establishment of an explicit or implicit model that allows the patterns analyzed to be categorized.

Two key aspects concern the evaluation, and thus the comparison, of the performance of alternative intrusion detection approaches: these are the efficiency of the detection process, and the cost involved in the operation.

Without underestimating the importance of the cost, at this point the efficiency aspect must be emphasized. Four situations exist in this context, corresponding to the relation between the result of the detection for an analyzed event (‘‘normal’’ vs. ’’attacked’’) and its actual nature (‘‘innocuous’’ vs. ‘‘malicious’’). These situations are: false positive (FP), if the analyzed event is innocuous (or ‘‘clean’’) from the perspective of security, but it is classified as malicious; true positive (TP), if the analyzed event is correctly classified as intrusion/malicious; false negative (FN), if the analyzed event is malicious but it is classified as normal/innocuous; and true negative (TN), if the analyzed event is correctly classified as normal/innocuous. It is clear that low FP and FN rates, together with high TP and TN rates, will result in good efficiency values [2].

The fundamentals for statistical, knowledge and machine learning-based, as well as the principal subtypes of each, are described below.

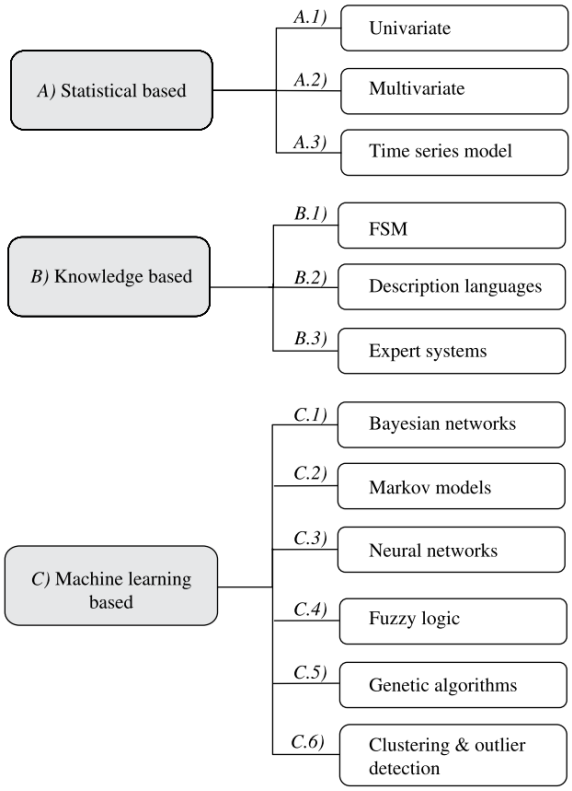

Figure 2. Classification of the anomaly detection techniques according to the nature of the processing involved in the ‘‘behavioral’’ model considered [2].

- **Expert systems**, these work on a previously defined set of rules describing an attack. All security related events incorporated in an audit trail are translated in terms of if-then-else rules. Examples are Wisdom & Sense and ComputerWatch (developed at AT&T).

- **Signature analysis** Similarly to expert System approach, this method is based on the attack knowledge. They transform the semantic description of an attack into the appropriate audit trail format. Thus, attack signatures can be found in logs or input data streams in a straightforward way. An attack scenario can be described, for example, as a sequence of audit events that a given attack generates or patterns of searchable data that are captured in the audit trail. This method uses abstract equivalents of audit trail data. Detection is accomplished by using common text string matching mechanisms. Typically, it is a very powerful technique and as such very often employed

in commercial systems (for example Stalker, Real Secure, NetRanger, Emerald eXpert-BSM).

- **State-transition analysis** here, an attack is described with a set of goals and transitions that must be achieved by an intruder to compromise a system. Transitions are represented on state-transition diagrams.

- **Statistical analysis approach** this is a frequently used method (for example SECURENET). The user or system behavior (set of attributes) is measured by a number of variables over time. Examples of such variables are: user login, logout, number of files accessed in a period of time, usage of disk space, memory, CPU etc. The frequency of updating can vary from a few minutes to, for example, one month. The system stores mean values for each variable used for detecting exceeds that of a predefined threshold. Yet, this simple approach was unable to match a typical user behavior model. Approaches that relied on matching individual user profiles with aggregated group variables also failed to be efficient. Therefore, a more sophisticated model of user behavior has been developed using short- and long-term user profiles. These profiles are regularly updated to keep up with the changes in user behaviors. Statistical methods are often used in implementations of normal user behavior profile-based Intrusion Detection Systems.

- **Neural Networks** Neural networks use their learning algorithms to learn about the relationship between input and output vectors and to generalize them to extract new input/output relationships. With the neural network approach to intrusion detection, the main purpose is to learn the behavior of actors in the system (e.g., users, daemons). It is known that statistical methods partially equate neural networks. The advantage of using neural networks over statistics resides in having a simple way to express nonlinear relationships between variables, and in learning about relationships automatically. Experiments were carried out with neural network prediction of user behaviors. From the results it has been found that the behavior of UNIX super-users (*roots*) is predictable (because of very regular functioning of automatic system processes). With few exceptions, behavior of most other users is also predictable. Neural networks are still a computationally intensive technique, and are not widely used in the intrusion detection community.

- **User intention identification** This technique (that to our knowledge has only been used in the SECURENET project) models normal behavior of users by the set of high-level tasks they have to perform on the system (in relation to the users' functions). These tasks are taken as series of actions, which in turn are matched to the appropriate audit data. The analyzer keeps a set of tasks that are acceptable for each user. Whenever a mismatch is encountered, an alarm is produced.

- **Machine learning** This is an artificial intelligence technique that stores the user-input stream of commands in a vectorial form and is used as a reference of normal user behavior profile. Profiles are then grouped in a library of user commands having certain common characteristics [3].

- **Data mining** generally refers to a set of techniques that use the process of extracting previously unknown but potentially useful data from large stores of data. Data mining method excels at processing large system logs (audit data). However they are less useful for stream analysis of network traffic. One of the fundamental data mining techniques used in intrusion detection is associated with *decision trees* [3]. Decision tree models allow one to detect anomalies in large databases. Another technique refers to segmentation, allowing extraction of patterns of unknown attacks [3]. This is done by matching patterns extracted from a simple audit set with those referred to warehoused unknown attacks [3]. A typical data mining technique is associated with finding *association rules*. It allows one to extract previously unknown knowledge on new attacks [3] or built on normal behavior patterns. Anomaly detection often generates false alarms. With data mining it is easy to correlate data related to alarms with mined audit data, thereby considerably reducing the rate of false alarms [3].

3. Proposed Algorithm

Since there is no data available about the network characteristics on attacked situation, hence it is needed to simulate the network for such condition and to collect the data, for this purpose a network simulator (OPNET) is used here, and after simulating the network for different scenario the raw data is collected. Now this data is classified into different group based on the data type (delay, drop rate, conjunction, packet type, bandwidth utilization, process status, services running, and processor utilization), then each data set it normalized by detecting its maximum and minimum values by the following formula

$$V_{norm} = \frac{V - V_{min}}{V_{max} - V_{\min}}$$

The normalized values set are arranged in an array to represent system condition by a vector this vector can be represented by

$$Trn_{vect} = [V_{norm1}, V_{norm2}, V_{norm3}, \ldots . V_{normn}]$$

Hence the system states can be projected into a hyper space of n dimensions.

According to the system states, vectors of that states are grouped and the centre for that group is calculated after that the maximum radius is also calculated (by measuring the distance from centre point to the point of maximum distance).

These processes provide the m centers for m different states (under attack, serious attack, ok etc.) of network and their maximum movement.

Now for detecting the system status any time the system data is collected and converted in to the vector as stated above and then the distance of current vector from all m centre points are calculated and the alarm is generated for the nearest point from the present vector.

4. Simulation Results

The simulation of the proposed algorithm is performed using MATLAB 7.5 on IBM P4 PC with windows XP operating system. Before that the raw data is collected using OPNET Network Simulator.

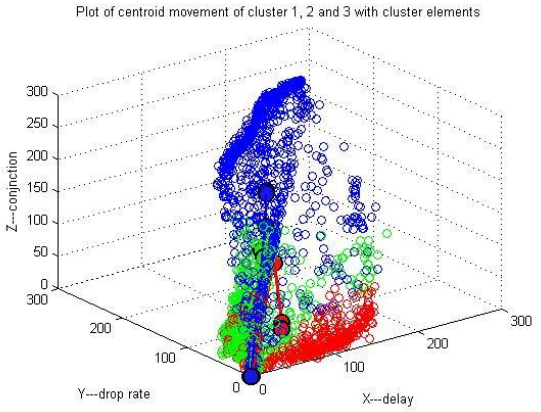

Figure 3. Plot of the system states on different conditions (worm holes, IP spoofing, DoS) for only three dimensional vector (higher dimensions are eliminated only for representation since plotting of more than three dimension is not possible).

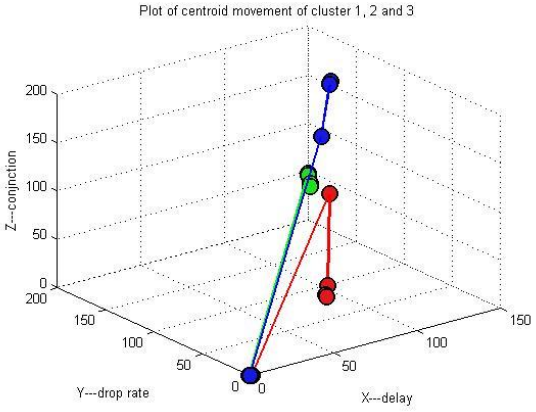

Figure 4. Plot of the cluster centers for above data mentioned in figure 3.

Table: showing the predicted results by the proposed algorithm.

Training States	Attack Type	TPR	TNR	FPR	FNR	Accu--racy
100	1	0.70	0.72	0.35	0.28	0.73
100	2	0.65	0.69	0.38	0.41	0.62
100	3	0.76	0.74	0.33	0.50	0.71
200	1	0.78	0.62	0.38	0.03	0.72
200	2	0.77	0.61	0.32	0.26	0.70
200	3	0.70	0.75	0.29	0.24	0.73
400	1	0.74	0.67	0.39	0.20	0.67
400	2	0.65	0.63	0.51	0.38	0.64
400	3	0.71	0.68	0.38	0.24	0.67

5. Conclusion

The Cyber Attack detector presented in this paper is capable of generating alert and the individual attack detection accuracy of the system is up to 73% which is above average also the algorithm does not requires too much of resources because its simplicity further it could achieve much better performance for only binary detections like attack and non attack conditions in future it can also be modified with different classification techniques to get much better results.

References

[1] Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285: 317–323.

[2] P. Garcı´a-Teodoroa, J. Dı´az-Verdejo, G. Macia´-Erna´ndeza, E. Va´zquezb "Anomaly-based network intrusion detection Techniques, systems and challenges " published on computers & security 28 (2009) 18 – 28".

[3]http://www.windowsecurity.com/articles/ids-part2-classification-methods-techniques.html

[4] Axelsson S.: Intrusion Detection Systems: A Taxomomy and Survey. Technical Report No 99-15, Dept. of Computer Engineering, Chalmers University of Technology, Sweden, March 2000, http://www.ce.chalmers.se/staff/sax/taxonomy.ps

[5] Bass T.: Intrusion Detection Systems Multisensor Data Fusion: Creating Cyberspace Situational Awareness. Communication of the ACM, Vol. 43, Number 1, January 2000, pp. 99-105,http://www.silkroad.com/papers/acm.fusion.ids.ps.

[6] Debar H., Dacier M., Wespi A.: Towards a taxonomy of intrusion-detection systems. Computer Networks, 31, 1999, pp. 805-822.

[7] Dorosz P., Kazienko P.: Omijanie intrusion detection systems. Software 2.0 no 9 (93), September 2002, pages 48-54. (In Polish only)

[8] Dorosz P., Kazienko P. Systems wykrywania intruzów. VI Krajowa Konferencja Zastosowan Kryptografii ENIGMA 2002, Warsaw 14-17 May 2002 , p. TIV 47-78, (In Polish only) http://www.enigma.com.pl/konferencje/vi_kkzk/index.htm