A study of Intrusion Discovery Method Using Genetic Neural Network

Brajendra Pratap Singh[1], Dr. Brij Bhusan[2]

[1]Research Scholar, Mewar University, Gangarar Chittorgarh, Rajasthan
[2]Professor, Mewar University, Gangarar, Chittorgarh, Rajasthan

Abstract

An Intrusion detection method is broadly classified as Anomaly based and Rule based detection methods. Anomaly based systems look for strange system behavior by observing the deviation from a baseline of normal behavior. Hence the anomaly based system has to be trained for the normal behavior. The training results in an ‘activity profile’ which represents the normal usage for a particular user over definite period of time. This acts as the baseline for the anomaly based IDS and any event that deviates from this baseline is reported as anomalous. Statistics based anomaly detection is best suited for Wireless Adhoc Networks. On other hand rule based IDS looks for a malicious event based on the rule set that is already available and customized. Wireless ad-hoc networks are increasingly being used in the tactical battlefield, emergency search and rescue missions, as well as civilian ad-hoc situations like conferences and classrooms due to the ease and speed in setting up such networks. As wireless ad-hoc networks have different characteristics from a wired network, the intrusion detection techniques used for wired networks may no longer be sufficient and effective when adapted directly to a wireless ad-hoc network. Existing methods of intrusion detection have to be modified and new methods have to be defined in order for intrusion detection to work effectively in this new network architecture. In this paper, we will first provide an introduction to wireless ad-hoc networks and thereafter an introduction to intrusion detection. We will then present various existing intrusion detection techniques that can be adapted to wireless ad-hoc networks and finally propose a hybrid intrusion detection system for wireless ad-hoc networks.

Keywords: *Intrusion, detection method, behavior, Wireless Adhoc Networks, Genetic Neural Network.*

1. INTRODUCTION:

Network intrusion detection systems monitor the traffic from the network for any leery activity and alert the network administrator. With the development of gigabit networks, current generation networking components for NIDS will soon be insufficient for numerous reasons, because the existing methods cannot meet the high performance demands of scanning the enormous data traffic. On the advent of Multicore processors a solution to handle the overwhelming data traffic by a multicore/multithreaded processor architectures using software parallelism has arrived. Hence the need of the hour would be to investigate the possibilities of parallelizing the anomaly detection algorithm to achieve software parallelism for its deployment in a Multicore processor so that it can make use of the potential of Multicore processors and could efficiently handle the task of scanning the enormous amount of data packets for intrusion.

An Anomaly based Intrusion Detection System is a one which monitors the network traffic searching for anomalous behaviour rather than matching the user behaviour pattern alone. Hence the anomaly based intrusion detection algorithms have the capability to detect unknown attacks. A self-learning algorithm for Anomaly based Intrusion Detection model which is based on GNN is proposed. The scope of the proposed algorithm remains in identifying the malicious packet. A wireless ad-hoc network consists of a collection of mobile nodes that communicate with each other via wireless links without the aid of a pre-existing communication infrastructure. Nodes within each other’s radio range communicate directly via wireless links, while those that are far apart rely on intermediate nodes to forward their messages. Each node can function both as a router as well as a host. For this paper, the mobile nodes that we are focusing our discussion on are current day laptops that have sufficient processing capability and memory to support ad-hoc networking as well as intrusion detection applications. These laptops have limited battery life only when they are unplugged from a main power source. Such mobile nodes are used to setup wireless ad-hoc networks in situations like classrooms or conferences; temporary offices like a promotional booth; emergency search and rescue missions and possibly at command posts in the military.

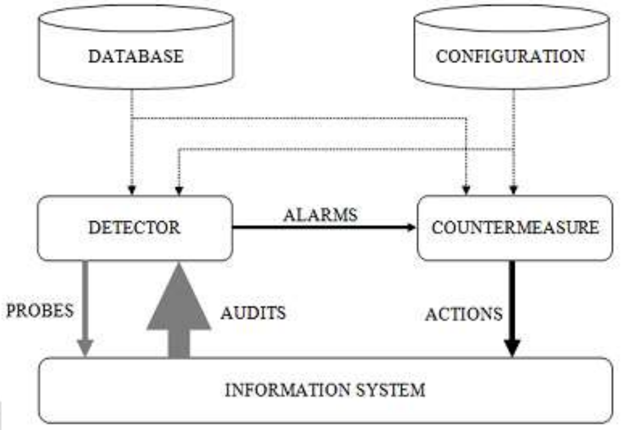

Figure 1: Simple intrusion detection system

IDSs typically record information related to observed events, notify security administrators of important observed events, and produce reports. Many IDSs can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDS stopping the attack itself, changing the security environment (e.g., reconfiguring a firewall), or changing the attack's content. A typical Intrusion Detection System is shown in figure 1. One of the major problems faced by IDS is huge number of false positive alerts, i.e. alerts that are mistakenly classified normal traffic as security violations. A perfect IDS does not generate false or irrelevant alarms. In practice, signature based IDS found to produce more false alarms than expected. This is because of the very general signatures and lack of built in verification tool to validate the success of the attack.

2. REVIEW OF LITERATURE:

Intrusion detection is designed to monitor the malicious activities occurring in a computer system or network inside or outside and analyzing them for signs of possible incidents, which are violations or forthcoming threats of violation of computer security policies, acceptable utilized policies, or standard security practices. Intrusion incidents to computer systems are increasing because of the commercialization of the internet and local networks and new automated hacking tools. Computer systems are turning out to be more and more susceptible to attack, due to its extended network connectivity. Nowadays, networked computer systems play an increasingly important role in our society and its economy. They have become the targets of a wide array of malicious attacks that invariably turn into actual intrusions. This is the reason computer security has become an essential concern for network administrators. Too often, intrusions cause havoc inside LANs and the time and cost to repair the damage can grow to extreme proportions. Instead of using passive measures to fix and patch security holes once they have been exploited, it is more effective to adopt a proactive approach to intrusions. Intrusion Detection Systems (IDS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators in real-time, or near real-time, and those that process audit data with some delay (non-real-time). The latter approach would in turn delay the time of detection. In addition, organizations use IDSs for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDSs have become a necessary addition to the security infrastructure of nearly every organization.

As mentioned by Mahoney (2003), SPADE, Audit Data Analysis and Mining (ADAM), and Next Generation Intrusion Discovery Expert System (NIDES) utilize recurrence based models, in which an occasion's likelihood is evaluated by its normal recurrence amid preparing. Lower probabilities result in higher irregularity scores, since these are apparently more inclined to be antagonistic. The model proposed by Mahoney (2003) is Network Traffic Anomaly Detector (NETAD) which computes an adjusted inconsistency score to distinguish vindictive information. The factual NETAD display has detailed 89 % exactness in distinguishing Probe attacks and in particular 93 % precision in identifying port scan attacks and 68 % exactness in recognizing DoS attacks.

According to Staniford et al (2002), port outputs can be of four sorts: vertical, level, strobe and piece. A vertical output comprises of a port sweep of a few or all ports on a solitary PC. The other three sorts of outputs are utilized over various IP addresses. An even sweep is an output of a solitary port over different IP addresses. On the off chance that the port sweep is of various ports over different IP addresses, it is known as a strobe check. A square output is a port sweep against all ports on various IP addresses. Yegneswaran et al (2003) additionally measured vertical sweep as comprising of at least six ports on a solitary PC, and a flat output as comprising of at least five IP addresses inside a subnet.

Leckie & Kotagiri (2002) present an algorithm in view of a probabilistic model. For every IP address in the checked system, the calculation creates a likelihood P(d|s) that speaks to how likely a source will contact that specific goal IP, where 'd' is the goal IP and 's' is the source, in view of how usually that goal IP is reached by different sources, P(d). Thus, it likewise registers a likelihood for each port that speaks to how likely a source will contact a specific goal port, P(p|s) where 'p' is the goal port. An impediment of this approach is that P(d) depends on the earlier conveyance of sources that have gotten to that IP address. From this it can be induced that if the probabilities for this approach are produced in view of an example of system information, and if the checked system is filtered, the subsequent circulations may incorporate sweeps and in addition typical movement. Another confinement of this approach is that it expect that an aggressor gets to the goals aimlessly; however this may not be constantly valid and the assailant may filter the goal in a specific request or pattern.

Kato et al (1999) examined this approach which aims to detect scans over large networks and is similar to GrIDS. However, it is further refined to evaluate only those connection attempts that result in a Reset Acknowledgement (RST-ACK) packet from the destination, indicating that the TCP service does not exist on the target IP address. During experiments in a 15-minute window, the method is able to identify a scan consisting four or more destinations returning RST-ACK packets to a single source. It is not suitable to detect those scans that are not TCP-based.

Robertson et al (2003) purported this method which is based on network return traffic, reconstructs sessions, and it flags any source IP that is found to contact a destination for which no response is returned. An anomaly score is estimated for each source IP based on the number of destinations contacted where no response is observed. It can view almost all traffic in both directions. However, it may not be possible to use it on large networks due to asymmetric routing policies. The authors present a second method, called peering center surveillance Discovery which has additional heuristics for analyzing traffic where there is the possibility that traffic for one direction is available and hence, no response does not necessarily indicate a scan.

Ertoz et al (2003) developed a system called MINDS (Minnesota Intrusion Discovery System) that can analyze network traffic and can also detect port scan attacks. It reads ‘Net Flow’ data and generates data characteristics, including flow level information; e.g., source IP, source port, number of bytes, etc. It then derives information such as the number of connections from a single source, the number of connections to a single destination, the number of connections from a single source to the same port, and the number of connections from a single destination to the same source port. These four features are counted over a time window and over a connection window. An anomaly score is estimated based on the flow data and derived data for each network traffic record. A report is generated ordered by anomaly score. The authors also claim that it can detect both fast and slow scanning.

Gates et al (2006) devised a method which analyzes Cisco Net Flow data for port scan attacks. The method extracts the events for each source and the flows in each event are then sorted according to destination IP and destination port. It attempts to calculate six characteristics for each event based on statistical analysis of port scans. It estimates a probability using logistic regression with these six characteristics as input variables to predict whether the events contain a scan or not. The main disadvantage of this technique is that it is non-real time.

Porras & Valdes (1998) suggested a method which is based on the EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances) system, and is used to detect port scan attacks. EMERALD considers each source IP address communicating with the monitored network as a subject. It constructs statistical profiles for subjects, and matches a short term weighted profile of subject behavior to a long term weighted profile. When the short term profile goes far enough into the tails of the distribution for the long term profile, EMERALD views it as suspicious.

Gyorgy et al (2005) proposed a model known as off-the-shelf classifier based on the data mining approach. Initially, it transforms network trace data into feature dataset with label information. Then, it selects Ripper, a fast rule based classifier, which is capable of learning rules from multi-model datasets and the results provided by it are easy to interpret. The authors successfully demonstrate that data mining models can enclose expert knowledge to create an adaptive algorithm which can outperform the heuristic based scan Discovery in both precision and recall. Also, this technique is capable of detecting the scanners at an early stage.

Rong-sheng et al (2004) proposed this approach which uses a new mechanism termed Port Scan Discovery (PSD) and is based on TCP packet anomaly evaluation. By learning the port distribution and flags of TCP packets arriving at the protected hosts, PSD can compute the anomaly score of each packet and effectively detect port scans including the slow scans and stealthy scans. It shows that PSD has high Discovery accuracy and low Discovery latency.

3. INTRUSION DETECTION:

Intrusion detection is defined as the method to identify "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource". It is pertaining to techniques that attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Hence in the context of wireless ad-hoc network, we need to identify any malicious nodes either from outside the network trying to break into or nodes that have turned bad. Bad nodes can easily disrupt or partition the network using the various forms of attacks as seen from the previous section. Detection of break-ins or attempts is done either manually or via software expert systems that operate on logs or other information available on the network. Humans can detect much more types of intrusions manually but we are interested in using automated systems that can study the audit data via certain mechanisms or rules. When working on intrusion detection, there are some primary assumptions to be made. Firstly, user and program activities are observable, that is the information regarding the usage of a system by a user or program must be recordable and analyzable. Secondly and more importantly, normal and intrusive behaviors must have distinct characteristics. Why is there a need for intrusion detection in wireless ad-hoc network? Isn't intrusion prevention enough? Intrusion preventive measures such as encryption and authentication can reduce intrusion but not eliminate them. Encryption and authentication cannot defend against compromised nodes and the fact that such nodes already carry private keys, which makes the network more vulnerable. The dynamic nature of the Adhoc network also means that trust between nodes in the network is virtually non-existent. Without trust, preventive measures are unproductive and measures that rely on a certain level of trust between nodes are susceptible attacks themselves. Another reason for not just having intrusion prevention is that it is often an after-thought during the design and development stages of computer systems. This makes room for loopholes in the system which people can exploit. As systems grow more and more complex, they become increasingly difficult to design and develop as well as maintain. The intrusion preventive measures will be inadequate as there will be more programming errors or bugs. According to Evans' Law, security risk is the product of the vulnerabilities and the number of malicious users. This works out to be about a quadrillion times worse today than in a few decades ago in terms of security problems. Hence there is the need for intrusion detection as it provides a second line of defense. As a wireless computing device is usually of limited electrical power and intensive processing drains any stored electrical power, we have to avoid the situation whereby the device has to do more routing than other devices on the network. Hence an optimal routing algorithm has to be employed. This is made even critical as power consumption increases tremendously when the wireless transceiver is active. We do not want a device to be exhaust of electrical power faster than it is necessary, especially when it is part of an optimum or even critical routing path where such a device is not operating results in the network needing route repairs or worse, segregated. Therefore, a good intrusion detection system should not only conduct intensive processing for detecting intrusion, it will be better if the system rides on an intelligent routing protocol.

In order to detect an intrusion attack, one needs to make use of a model of intrusion. That is, we need to know what an Intrusion Detection System (IDS) should look out for. There are basically two types of models employed in current IDS: anomaly detection (figure 2) and misuse detection (figure 3).

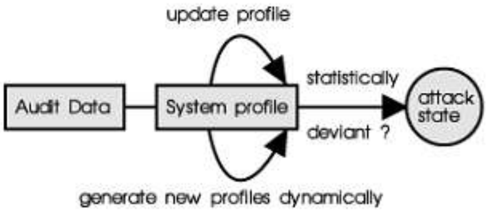

Figure – 2- A typical anomaly detection system

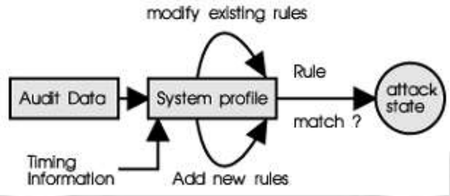

Figure – 2- A typical misuse detection system

The first model studies its detection upon the profile of a user's (or a group of users') normal behavior. It analyzes the user's current session and compares them to the profile representing the user's normal behavior statistically. It then reports any significant deviations to a designated system administrator. As it catches sessions which are not normal, this model is hence referred to as an "anomaly' detection model. Anomaly detection bases its idea on statistical behavior modeling and anomaly detectors look for behavior that deviates from normal system use. A typical anomaly detection system takes in audit data for analysis. The audit data is transformed to a format statistically comparable to the profile of a user. The user's profile is generated dynamically by the system (usually using a baseline rule laid by the system administrator) initially and subsequently updated based on the user's usage. Thresholds are normally always associated to all the profiles. If any comparison between the audit data and the user's profile resulted in deviation crossing a threshold set, an alarm of intrusion is declared. This type of detection systems is well suited to detect unknown or previously not encountered attacks.

4. INTRUSION DETECTION TECHNIQUES

Problems of current intrusion detection techniques: It is difficult to apply intrusion detection techniques developed for the wired network to the wireless ad-hoc network due to the vast difference between the two networks. The main difference is that wireless ad-hoc networks do not have fixed infrastructures, and existing network-based IDSs, which rely on real-time traffic analysis, can no longer function well in the new environment. In wired networks, traffic monitoring is usually done at switches, routers and gateways. The wireless ad-hoc environment does not have such traffic concentration points where the IDS can collect audit data for the entire network and can only rely on partial, localized audit data collected from the host and from communication activities taking place within the radio range. Besides having different network infrastructures, there is also a big difference in the communication pattern of users in the wireless mobile environment. Due to the bandwidth limitations, battery constraints and frequent disconnects, users often adopt new operations modes such as disconnected operations. This suggest that existing anomaly detection models may not be able to determine that such new operations are certified and identify them as intrusions.

Reasons for choice of intrusion detection techniques: The intrusion detection techniques that will be presented in the following sections are chosen due to the suitability of the technique for anomaly detection. Anomaly detection should be the main approach for intrusion detection in the wireless ad-hoc network because it is conceivable that intrusion in this new environment will come in the form of new attacks types that are yet to be defined. These techniques can also be adapted for local and cooperative detection. The techniques can either process partial and local data on the host as well as gather more information from the neighboring hosts to perform cooperative intrusion detection.

Haystack: This algorithm is a statistical anomaly detection algorithm. It works by first assuming that the audit trail generated from a host has been converted to a canonical audit trail (CAT) format. It then uses a CAT file to generate session vectors representing the activities of the users' sessions. These session vectors are then analyzed against specific types of intrusive activities to calculate "anomaly scores". If the scores cross some thresholds, warnings reports are generated. The algorithm analyzes a session vector in three steps: 1) it calculates a Bernoulli vector, 2) it calculates the weighted intrusion score, and 3) it calculates the suspicion quotient. The Haystack algorithm gets its name by being the algorithm implemented in the IDS called Haystack. Haystack is a host-based system which attempts to detect several types of intrusions: attempted break-ins, masquerade attacks, penetration of the security system, leakage of information, denial of service, and malicious use. It was initially developed for use in the US military network.

Mobile agents: A global distributed and modular architecture where the intrusion detection scheme is provided by local IDS (LIDS) entities, located on each node of the mobile ad hoc network (MANET) and collaborating with other LIDes through the use of mobile agents. As the lack of the centralization in MANET, some of the tasks required for the intrusion detection processes should be executed in a distributed and cooperative manner. Mobile agents are an alternative to the client-sever distribution model. Mobile agents can provide a first element of response to the problem of the scalability of the global intrusion detection process. When a node joins the network, it does so with running LIDS and a mobile agent platform. It can therefore, immediately take part in the global cooperative intrusion detection process.

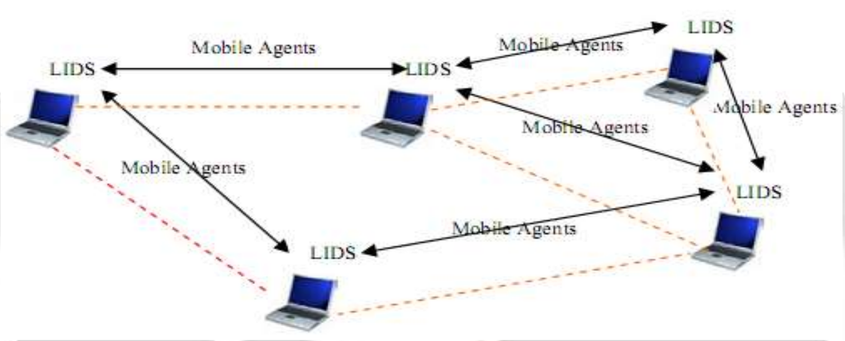

Figure 3- Intrusion detection system using mobile agents

Data mining: Data mining algorithms implemented on each mobile node can be used to analyze audit data and thereafter generate intrusion detection models. Data mining generally refers to the process of extracting useful models from large repositories of data. Below are several algorithms that are particularly useful for mining audit data for anomaly detection. Classification is the process by which a data item is mapped into one of several predefined categories. The classification algorithms normally produce "classifiers" that can be in the form of decision trees or rules. Sufficient "normal" and "abnormal" audit data must be gathered before a classification algorithm can be applied to learn a classifier that can categorize new unseen audit data as belonging to the normal class or the abnormal class. Link analysis is used to determine relations between fields in an operating system audit record. Normal usage profile can be constructed from determining the correlation between command and argument in the shell command history data of a user. A programmer, for example, may have iMac's highly associated with C files. Sequence analysis involves the analysis of frequent sequential patterns of audit data in order to gain insight into the temporal and statistical nature of many attacks as well as the normal behavior of users and programs. The statistical information collected can then be incorporated into intrusion detection models.

5. CONCLUSION

Wireless ad-hoc networks have brought about a paradigm shift in the way we think about intrusion detection. We need to rethink methods for these new networks based on the characteristics that these networks have. In this paper, we have provided an introduction to wireless ad-hoc networks. We then proceeded to provide an introduction to intrusion detection in the context of wireless ad-hoc networking. Having understood the implications and problems in performing intrusion detection in this new environment, we performed a survey on the existing methods for intrusion detection and listed four techniques that we deemed are suitable for the wireless ad-hoc environment. We ended by proposing a hybrid intrusion detection system that allows the different techniques that we have identified to be incorporated into the system and is most suited for wireless ad-hoc networking.

6. REFERENCES:

1. Mahoney, MV (2003), 'Network Traffic Anomaly Discovery Based on Packet Bytes', Proceedings of the eighteenth ACM symposium on Applied Computing (SAC), pp. 346–350.
2. Staniford, S, Hoagland, J A & McAlerney, J M (2002), 'Practical automated Discovery of stealthy portscans', Journal of Computer Security', vol. 10, pp. 105-136.
3. Yegneswaran, V, Barford, P & Ullrich, J (2003), 'Internet Intrusions: global characteristics and prevalence', SIGMETRICS Performance Evaluation Review, vol. 31, pg. 138 -147.
4. Leckie, C & Kotagiri, R (2002), 'A probabilistic approach to detecting network scans', Proceedings of Network Operations and Management Symposium (NOMS'02), pp. 359-372.
5. Kato, N, Nitou, H, Ohta, K, Mansfield, G & Nemoto, Y (1999), 'A realtime intrusion Discovery system (ids) for large scale networks and its evaluations', Institute of Electronics, Information and Communication Engineers Transactions on Communications, vol. E82-B, no.11, pp. 1817-1825.
6. Robertson, S, Siegel, EV, Miller, M & Stolfo, SJ (2003), 'Surveillance Discovery in high bandwidth environments', Proceedings of DARPA third conference on DARPA Information Survivability Conference and Exposition, pp. 130 – 139.
7. Ertoz, L, Eilertson, E, Lazarevic, A, Tan, PN, Dokas, P, Kumar, V & Srivastava, J (2003), 'Discovery of novel network attacks using data mining', Proceedings of ICDM WDMCS'03, pp. 30-39.
8. Gates, C, McNutt, JJ, Kadane, JB & Kellner, M (2006), 'Scan Discovery on very large networks using logistic regression modeling', Proceedings of IEEE Symposium on Computers and Communication, pp. 402–408.
9. Porras, P & Valdes, A (1998), 'Live traffic analysis of TCP/IP gateways', Proceedings of ISOC Symposium on Network and Distributed System Security, pp. 1-13.
10. Gyorgy, JS, Hui, X, Eric, E & Vipin, K (2005), 'Scan Discovery: A data mining approach', Proceedings of SIAM International Conference on Data Mining, pp. 118-129.
11. Rong-sheng, S, Xiao-yong, L & Jian-hua, L (2004), 'An adaptive algorithm to detect port scans', Journal of Shangai University (English Edition), vol. 8, no. 3, pp. 328-332.