Advances in Mechanical Engineering and its Applications
Vol. 1, No. 2, 2012

www.worldsciencepublisher.org

Intrusion Detection and Remedial Action

[1]Manoj Kumar Tyagi, [2]Kalyan Chavali, [3]Bakka Lidiya

1. Associate Professor, Electronics and Computers Engineering, K L University, Vijayawada, India
2. Student, Electronics and Computers Engineering, K L University, Vijayawada, India
3. Student, Electronics and Computers Engineering, K L University, Vijayawada, India

***Abstract*-** 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 the proposed hybrid intrusion detection system for wireless ad-hoc networks.

Keywords- Intrusions, Intrusion Detection Systems, Wireless networks, wireless ad-hoc networks, anomaly detection, misuse detection and data mining.

1. Introduction

Wireless has opened a new and exciting world for many of us. Its technology is advancing and changing every day and its popularity is increasing. The biggest concern with wireless, however, has been security. For some time wireless has had very poor, if any, security on a wide open medium.

Wireless network refers to any type of computer network that is not connected by cables of any kind. It is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using a transmission system called radio waves. This implementation takes place at the physical level (layer) of the network structure.

A wireless ad-hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. It often contains mobile devices called as nodes. Each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. Each node can function both as a router as well as a host. In addition to the classic routing, ad-hoc networks can use flooding for forwarding the data.

Mobile devices can be anything from a smart-phone to a mainframe. Here we consider the mobile devices as laptops for easy generalization of nodes. As these have limited battery life and highly reduced performance, the classic intrusion detection systems that use intensive processing have limited uses.

The very nature of wireless ad-hoc networks makes them vulnerable to numerous attacks. They can range from a passive eavesdropping (traffic analysis) to active interference (Masquerade) attacks. Unlike wired networks where the hacker must gain physical access to the network wires or must pass through several levels of defense, wireless ad-hoc networks are susceptible to various attacks from all directions. Moreover, in large-scale wireless ad-hoc networks tracking down a single mobile node is very difficult. Therefore each node must be prepared for attacks from every direction.

Not only in the upper level of nodes are the attacks performed, but also in inner levels like routing and MAC protocols of the ad-hoc. They are vulnerable to attacks but only difference is that these attacks can be lethal to the whole network. For example by intruding into the ad-hoc the adversary can paralyze the whole ad-hoc system.

In summary wireless ad-hoc networks have vulnerabilities that are not easily preventable. To employ a

high security wireless ad-hoc networks we need to introduce intrusion detection systems and response techniques. Intrusion detection by definition would detect any kind of attack because an adversary must intrude into a network first before he performs any networks.

2. Intrusion Detection and Intrusion Detection System

Intrusion detection is the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource. When Intrusion detection takes a preventive measure without direct human intervention, then it becomes an Intrusion-prevention system.

Intrusion detection can be performed manually or automatically. Manual intrusion detection might take place by examining log files or other evidence for signs of intrusions, including network traffic. A system that performs automated intrusion detection is called an Intrusion Detection System (IDS). An IDS can be either host-based, if it monitors system calls or logs, or network-based if it monitors the flow of network packets. Modern IDSs are usually a combination of these two approaches. Another important distinction is between systems that identify patterns of traffic or application data presumed to be malicious (misuse detection systems), and systems that compare activities against a 'normal' baseline (anomaly detection systems).

Determining what the probable intrusion actually is and taking some form of action to stop it or prevent it from happening again are usually outside the scope of intrusion detection. However, some forms of automatic reaction can be implemented through the interaction of Intrusion Detection Systems and access control systems such as firewalls.

Some authors classify the identification of attack attempts at the source system as extrusion detection (also known as outbound intrusion detection) techniques.

There are certain types of intrusion detection. Some of them include the following:

2.1 Signature based detection

An Intrusion Detection System can use signature-based detection, relying on known traffic data to analyze potentially unwanted traffic. This type of detection is very fast and easy to configure. However, an attacker can slightly modify an attack to render it undetectable by a signature based Intrusion Detection System. Still, signature-based detection, although limited in its detection capability, can be very accurate.

2.2 Anomaly based detection

An Intrusion Detection System that looks at network traffic and detects data that is incorrect, not valid, or generally abnormal is called anomaly-based detection. This method is useful for detecting unwanted traffic that is not specifically known. For instance, an anomaly-based Intrusion Detection System will detect that an Internet protocol (IP) packet is malformed. It does not detect that it is malformed in a specific way, but indicates that it is anomalous.

2.3 Stateful Protocol Inspection

Stateful protocol inspection is similar to anomaly based detection, but it can also analyze traffic at the network and transport layer and vendor-specific traffic at the application layer, which anomaly-based detection cannot do.

Intrusion Detection System is a combination of software and hardware that attempts to perform intrusion detection. Its main functionality is to raise the alarm when a possible intrusion occurs. It is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station.

The various types of Intrusion Detection System include:

2.4 Network-based IDS:

It is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts. Network intrusion detection systems gain access to network traffic by connecting to a network hub, network switch configured for port mirroring, or network tap. In a NIDS, sensors are located at choke points in the network to be monitored, often in the demilitarized zone (DMZ) or at network borders. Sensors capture all network traffic and analyze the content of individual packets for malicious traffic.

2.5 Host-based IDS:

It consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability databases, Access control lists, etc.) and other host

activities and state. In a HIDS, sensors usually consist of a software agent. Some application-based IDS are also part of this category.

Almost every IDS today is at least in part signature-based. Attacks and their tools usually have a unique signature that can be detected and/or found. This means that known attacks can be detected by looking for these signatures. The downside to these is that they are easy to fool and can only detect attacks for which it has a signature.

The other approach is anomaly-based systems. These are not often implemented, mostly because of the high amount of false alarms. An anomaly-based system develops a baseline of what it considers normal traffic. Any time it detects traffic which deviates from what it considers normal an alert is generated. The advantage is that it can catch many attacks that are new or unknown and that would never be seen by signature-based IDS. The drawbacks consist mainly of large amounts of time being spent to train and retrain the IDS system, as well as the large amount of false alerts that have to be examined. As a note, hybrid systems have also been evolving that use both signature-based and anomaly-based techniques.

3. Data Mining

Data Mining (the analysis step of the Knowledge Discovery in Databases process, or KDD), a relatively young and interdisciplinary field of computer science, is the process of discovering new patterns from large data sets involving methods from statistics and artificial intelligence but also database management. In contrast to machine learning, the emphasis lies on the discovery of previously unknown patterns as opposed to generalizing known patterns to new data.

The term is a buzzword, and is frequently misused to mean any form of large scale data or information processing (collection, extraction, warehousing, analysis and statistics) but also generalized to any kind of computer decision support system including artificial intelligence, machine learning and business intelligence. In the proper use of the word, the key term is discovery, commonly defined as "detecting something new". Even the popular book "Data mining: Practical machine learning tools and techniques with Java" (which covers mostly machine learning material) was originally to be named just "Practical machine learning", and the term "data mining" was only added for marketing reasons. Often the more general terms "(large scale) data analysis" or "analytics" are more appropriate.

4. Data mining for Intrusion Detection

The concept of data mining can be applied to the intrusion detection system in order to develop a new and hybrid Intrusion detection system. The basic idea of implementing data mining techniques to intrusion detection system is to detect new types of intrusions by learning from old signatures. This would be a valuable functionality that would be of large help to the IDS as newer attacks invented by the hackers can also be detected.

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.

In data mining we can use two techniques to detect intrusions – Anomaly detection and misuse detection. The detectors using former method look for deviations in normal behavior while the detectors using the latter approach look for behavior that matches the known attack state. Obviously anomaly detection scheme is better and like a virus detection system, misuse detection is only as good as the database of attack signatures that it uses to compare with.

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. Problems of current Intrusion Detection Systems

The vast difference between both the types of networks make the existing intrusion detection systems made for wired networks not applicable to wireless ad-hoc networks. The most significant difference is, obviously, the lack of fixed infrastructure in the latter. In ad-hoc networks there are no specific routers, switches and gateways like in wired

networks so that the IDS located at such a location would collect data to detect intrusions. Therefore for the IDS to perform properly it must monitor the traffic in the communication devices.

The existing IDSs cannot detect new types of intrusion as most of them are conventional signature based. They detect intrusions based on already present signatures or attacks which were already performed. They cannot possibly determine the new attacks that adversaries invent every day. The implementation of adaptive, signature-based IDS in a wireless network would be impossible because it is vulnerable to attack even more than wired networks.

To be effective, IDS must be run online, in real time. Offline, or after-the-event-IDS, is useful for audit trail but will not prevent an attack from taking place. Real time IDS needs to be able to stream data across a network from sensors to a central point where it can be stored and analyzed, sometimes known as a correlation server. This additional network traffic running concurrently can significantly impact network performance so sufficient bandwidth is a prerequisite, though certain tools such as Air Defense Guard allow you to set rate throttles on each sensor to bring transfer rates to the server as low as 9.6 Kbps.

Some IDSs like Snort which verify the content of each packet would detect intrusions based only on the previously known attacks. Moreover, it would also require a lot of CPU processing and thus use another resource to perform the intrusion detection.

To overcome such limitations we can employ the concept of data mining to design a new intrusion detection system which is better than the conventional IDS.

In wireless ad-hoc networks there is no cleardifference between normal and anomalous behaviors. So anomaly detection (previously pointed as a better method) is not really apt.

In summary we must take care of following things in developing a better intrusion detection system for wireless ad-hoc networks:

1. Ideal system architecture for building the IDS and response systems in wireless environment.
2. Audit data sources that provide basis for anomaly detection
3. Separation of the affected and affecter from other systems in the network

These things are taken care of in the rest of this paper.

6. Proposed System: Intrusion Detection and Remedial Action

6.1 Architecture

For effective working, both the intrusion detection system and remedial system must be distributed in nature. Therefore, in the proposed system every node participates in intrusion detection and response. Here response activity depends on neighboring nodes which are collaborative enough to do the task.

Basically IDS agents will be present at each and every node of the network. If an anomaly is detected, neighboring agents will collaborate in global intrusion detection acts. These individual IDSs collectively form the IDS of the whole network.

The internal structure of an IDS agent can be complex as it should collaborate with neighboring IDSs and work. There can be 5 parts to each Intrusion Detection System.

Data collector: The data collector collects data at the link layer, the network layer and the application layer. Information is needed from these three different layers to perform multi-layered intrusion detection. Multi-layered intrusion detection is needed as certain attacks that target the upper layer may seem perfectly legitimate to the lower layers.

Detection optimizer: Due to the limited battery life that the mobile node has, we deem that intrusion detection should be done on the basis of different levels of escalation starting from the simplest and least battery consuming intrusion detection operation to more complex and CPU intensive operation. The detection optimizer preprocesses all the audit data collected from the different layers and send the most relevant audit data to the detection engine based on the mode that the mobile node is currently operating in.

Detection engine: The detection engine performs both misuse and anomaly detection. Either the Haystack or data mining algorithms can be implemented in the detection engine.

Response engine: When an intrusion is detected, the system needs to respond appropriately. It can either sound a local alarm on the host or a global alarm on the network. The nodes can then respond to the intrusion either locally or cooperatively.

Secure communication module: The secure communication module is needed when the node needs to perform cooperatively intrusion detection as well as when sounding a global alarm.

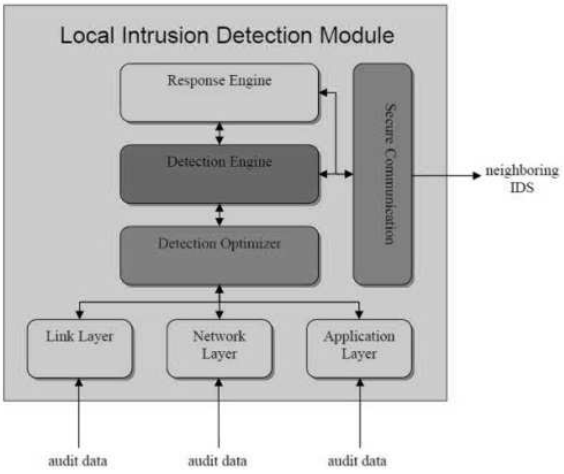

Figure 1: Architecture of INDRA

6.2 Anomaly Detection

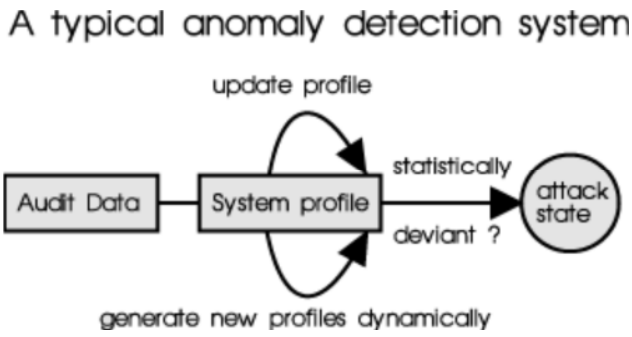

Figure 2: Anomaly Detection

Anomaly detection hypothesizes 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.

The main aim of anomaly detection is low false positive rates, detected as deviations from normal states. In ad-hoc networks the main concern is the false routing information generated by a compromised node will be disseminating to and used by other nodes. Therefore a routing table is employed to detect abnormal updates.

The routing table should at least contain the next hop to destination node and the distance. A noticeable change in the routing table can be caused by physical movement of nodes or by network membership changes. We use data's physical movements and the corresponding change in its routing as the basis for tracing.The physical movement is measured by speed, direction and distance. This can be obtained by a built in GPS device.

6.3 Response module

Response module or remedial part of the IDS is an important part as detection only is not enough. When an intrusion is detected, the system needs to respond appropriately. It can either sound a local alarm on the host or a global alarm on the network. The nodes can then respond to the intrusion either locally or cooperatively.

As mentioned above the basic idea of INtrusion detection and remedial action is cooperation between nodes. That is very useful and advantageous functionality which helps nodes to respond very effectively to an intrusion.

In wired networks were firewalls are present it is easy to detect and prevent intrusions that arise from application layer as IDSs usually accept data only from lower layers. But in wireless ad-hoc networks, there are no firewalls apart from ones present in devices. So an IDS is mandatory to the network as some networks like "back-door" attacks may seem perfectly safe to lower layers but are based on MAC protocols.

The following steps are followed to correct the loophole involving layers:

- If a node detects an intrusion that affects entire network, it initiates the re-authentication process to exclude the compromised nodes from the network.
- If an intrusion of higher layer is detected, the lower layers are notified. The data acquisition part there can then can verify the sources and then investigate on the ad-hoc routing protocols.

With these two steps and this approach the lower layers now need more than just one anomaly detection model. Such model relies on data from one layer and indirectly uses evidence from other layers. With this layered approach we can achieve both higher true positive and lower false positive rates. Thus, we can achieve higher rates of performances in response module.

In addition to the above approach, we can also implement the following steps for effective response:

- Preparation
- Identification
- Initial response
- Formulation of response strategy
- Investigation of the incident
- Reporting
- Resolution

Preparation involves setting up systems to detect threats, creating policies, and organizing a response team that can respond when needed. Setting up your WIDS would be part of this first step. Identification of an incident (a threat which poses a risk and requires action) can also be provided in part by a WIDS that logs and alerts to potential threats. Often these alerts come from other sources as well, for example, staff members reporting unusual activity.

Initial Response consist of recording what is taking place along with bringing in necessary staff or teams to start investigating and responding to the alert, as well as informing any higher authorities necessary. Formulating the response strategy is strait forward; determine the best plan of action, get approval and proceed with plan. Investigating the incident includes collecting a complete record of what happened including any data involved, what was done and by whom, along with when it happened and how to prevent it. This may include gathering logs stored from the WIDS system, as well as determining any settings that may be modified to help prevent the threat in the future.

Reporting and documenting every step and action taken, down to any command entered and by whom, is perhaps one of the most important steps involved in an incident response. A dressed up version of the report is also usually made for upper staff, while a complete record like what was created in the previous investigation phase may be kept for in-depth analysis at a later time. Finally resolution involves trying to prevent this from happening again.

Tightening up the firewall and servers and adding/changing signatures and settings on the IDS systems are all typical changes during the resolution phase. It also involves looking over what happened and how it was handled so that the process can be improved. What tools, procedures, and people, did or didn't work as planned and how or what can be done to improve the process.

7. Conclusion

Any secure network will have vulnerabilities that an adversary can exploit. For wireless ad-hoc networks this is especially true. Intrusion detection systems alone are not enough to eliminate attacks on wireless networks. They must be complimented with proper response mechanisms to act accordingly to the attacks.

One main disadvantage that traditional signature-based intrusion detection systems have is that they cannot detect intrusions that are newly formed and depend largely on old known attacks. We have introduced the concept of data mining to Intrusion detection to detect new attacks that are spawning daily in the hands of malicious hackers.

After that we have showed the need for new types of intrusion detection systems in wireless ad-hoc networks.Due to the wireless environment many detection techniques that worked perfectly well in wired networks fail to work here. Therefore a new system with many changes is proposed in this paper.

The new system proposed has intrusion detection as one part and response engine as another. The intrusion detection uses data mining concept to detect new attacks and has a new architecture to suit for the wireless environment. We have stated how the anomaly detection is done in the new architecture.

Finally we have presented the second part that is response part of the system. This system cannot be chosen as the perfect solution for the problems in wireless ad-hoc networks but is, we believe, a little better over the rest.

References

1. **Intrusion Detection in Wireless Ad-Hoc Networks** by Foong Heng Wai, Yin Nwe Aye and Ng Hian James.
2. **Intrusion Detection in Wireless Ad-Hoc Networks** by Yong Guang Zhang and Wenke Lee.
3. **MINDS** by Levent Ertoz, Eric Eilertson, Aleksandar Lazarevicy, Pang-Ning, Vipin Kumar, Jaideep Srivastava, Paul Dokas.
4. **Data Mining for Network Intrusion Detection: How to Get Started** by Eric Bloedorn, Alan D. Christiansen, William Hill, Clement Skorupka, Lisa M. Talbot, Jonathan Tivel.
5. **Ensemble-based Adaptive Intrusion Detection** by Wei Fan and Salvatore J. Stolfo.
6. **Wireless Intrusion Detection Systems Including Incident Response & Wireless Policy** by Jeff Dixon.