Volume 3, Issue 4, April 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Intrusion Detection and Prevention in Wireless Adhoc Networks

G.Naga Satish*
Research Scholar
Department of Computer Science
Adikavi Nannaya University
Rajahmundry. A.P., India

Ch.V.Raghavendran
Research Scholar
Department of Computer Science
Adikavi Nannaya University
Rajahmundry. A.P., India

Prof.P.Suresh Varma
Professor
Department of Computer Science
Adikavi Nannaya University
Rajahmundry. A.P., India

Abstract-Intrusion detection over the last few years, assumed top importance in the world of network security and as in the case of wireless adhoc networks also. These are the networks that do not have an underlying infrastructure, network topology which are constantly changing. Because of increased vulnerabilities, Threats and Illegal Access intrusion prevention alone does not solve the problem. Intrusion detection for wireless adhoc networks is a complex and difficult task mainly due to the dynamic nature, their highly constrained nodes, and the lack of central monitoring points. Intrusion prevention systems are considered as extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected.In this paper we present outlines of the issues of intrusion detection and prevention for wireless adhoc networks.

Keywords–Adhoc networks, Intrusion detection, Intrusion prevention.

I. INTRODUCTION

An adhoc network is a self-configuring network that is formed automatically by a collection of nodes without the help of a fixed infrastructure or centralized management. Each node is equipped with a wireless transmitter and receiver, which allow it to communicate with other nodes in its radio communication range. In order for a node to forward a packet to a node that is out of its radio range, the cooperation of other nodes in the network is needed; this is known as multi-hop communication. Therefore, each node must act as both a host and a router at the same time. The network topology frequently changes due to the mobility of nodes as they move within, move into, or move out of the network [4]. A wireless adhoc network with the was originally developed for military purposes, as nodes are scattered across a battle field and there is no infrastructure to help them form a network. In recent years, wireless adhoc networks have been developing rapidly and are increasingly being used in many applications, ranging from military to civilian and commercial uses, since setting up such networks can be done without the help of any infrastructure or interaction with a human. As wireless networks become widely used, the security issue has become one of the primary concerns. Intrusion detection can be defined as a process of monitoring activities in a system, which can be a computer or network system [5]. The mechanism by which this is achieved is called an intrusion detection system (IDS). An IDS collects activity information and then analyzes it to determine whether there are any activities that violate the security rules. Once an IDS determines that an unusual activity or an activity that is known to be an attack occurs, it then generates an alarm to alert the security administrator. In addition, IDS can also initiate a proper response to the malicious activity. Although there are several intrusion detection techniques developed for wired networks today, they are not suitable for wireless adhoc networks due to the differences in their characteristics [7]. Therefore, those techniques must be modified or new techniques must be developed to make intrusion detection work effectively in wireless adhoc networks.

II. Intrusion Detection in Wireless Adhoc Networks

Intrusion detection can be defined as the automated detection and subsequent generation of an alarm to alert the security apparatus at a location if intrusions have taken place or are taking place [12]. An intrusion detection system is a defense system, which detects hostile activities in a network and then tries to prevent such activities that may compromise system security. Intrusion detection systems achieve detection by continuously monitoring the network for unusual activity. The prevention part may involve issuing alerts as well as taking direct preventive measures, such as blocking a suspected connection. In other words, intrusion detection is a process of identifying and responding to malicious activity targeted at computing and networking resources [14]. In addition, IDS tools are capable of distinguishing between insider attacks originating from inside the network and external ones. Unlike firewalls, which are the first line of defense, intrusion detection systems come into the picture only after an intrusion has occurred and a node or a network has been compromised [2]. That is why intrusion detection systems are aptly called the second line of defense .
The following are features which are not a part of Intrusion detection systems

- is NOT an anti-virus system, designed to detect malicious software, such as viruses, Trojans, worms, etc.
- is NOT a network logging system used, for example, to detect complete vulnerability to any denial-of-service (DoS) attack across a congested network. These are network traffic monitoring systems.
- is NOT a vulnerability assessment tool that checks for bugs and flaws in operating systems and network services. Such an activity would fall under the purview of security scanners.

Intrusion detection can be classified into three broad categories: anomaly detection, signature or misuse detection, and compound detection.

1) Anomaly detection:

In an anomaly detection system, a baseline profile of normal system activity is created. Any system activity that is a deviation from the baseline is treated as a possible intrusion. The problems with strict anomaly detection are that anomalous activities that are not intrusive are flagged as intrusive and intrusive activities that are not anomalous result in false negatives. One disadvantage of anomaly detection for mobile computing is that the normal profile must be periodically updated and deviations from the normal profile must be computed. The periodic calculations can impose a heavy load on some resource constrained mobile devices and perhaps a lightweight approach that involves comparatively less computation might be better suited.

2).Misuse detection:

In this decision are made on the basis of knowledge of a model of the intrusive process and what traces it ought to leave in the observed system. Legal or illegal behavior can be defined and observed behavior can be compared accordingly. Such a system tries to detect evidence of intrusive activity irrespective of any knowledge regarding the background traffic, i.e., the normal behavior of the system.

3).Specification-based detection:

This defines a set of constraints that describe the correct operation of a program or protocol, and monitors the execution of the program with respect to the defined constraints. This technique may provide the capability to detect previously unknown attacks, whileexhibiting a low false positive rate.

A. Requirements for Intrusion Detection Systems

There are two key requirements that any IDS needs to fulfill. These are effectiveness i.e how to make the intrusion detection system activity correctly and efficiency i.e how to run the intrusion detection system in a cost-effective manner as far as possible. In other words, these two requirements in essence suggest that an IDS should detect a substantial percentage of intrusions into the supervised system, while still keeping the false alarm rate at an acceptable level at a lower cost. It is expected that an ideal IDS is likely to support several of the following requirements:

- The intrusion detection system should not introduce a new weakness in the wireless adhoc networks. That is, the IDS itself should not make a node any weaker than it already is.
- An intrusion detection system should run continuously and remain transparent to the system and the users.
- The intrusion detection system should use as little of the system resources as posible to detect and prevent intrusions. Intrusion detection systems that require excessive communication among nodes or run complex algorithms are not desirable.
- It must be fault tolerant in the sense that it must be able to recover from system crashes, hopefully recover to the previous state, and resume the operations before the crash.
- A part from detecting and responding to intrusions, IDS should also resist subversion. It should monitor itself and detect whether it has been compromised by an attacker.
- An intrusion detection system should have a proper response. In other words, an IDS should not only detect but should also respond to the detected intrusions, preferably without human intervention.
- Accuracy of the intrusion detection system is another major factor. Fewer false positives and false negatives are desired.
- It should inter-operate with other intrusion detection systems collaboratively to detect intrusions.

B. Security Vulnerabilities

The lack of centralized control and infrastructure of an ad hoc network increases its vulnerability and exposure to attacks. Unlike its fixed wired counter part where an attacker must gain physical access through several lines of defense at firewalls and gateways, attacks on a wireless network can come from all directions including nodes thought to be participating in the network, as the absence of authorization facilities impedes the usual practice of distinguishing nodes as trusted and nontrusted. Since the nodes are often mobile, the topology of the network may be constantly changing as nodes join in and move out of the network as they move in and out of radio range. Also, nodes may operate in a disconnected state to preserve a limited power supply, which also affects the network topology. This dynamically changing topology makes it difficult for nodes in a network to recognize a malicious node.

C.Attacks against wireless Adhoc Networks

Attacks against wireless Adhoc networks fall into two categories: passive attacks and active attacks. Passive attacks, such as eavesdropping, can be devastating to security critical areas such as military applications. Active attacks, on the other hand, involve replication, modification, and deletion of data and since nodes without adequate protection in a wireless ad hoc network are prone to being captured, compromised, or hijacked, these networks are particularly vulnerable to attacks that come from inside. Internal attacks are far more damaging and difficult to detect. A malicious node can disrupt the network by deleting or modifying messages or even attacking the routing protocol by refusing to forward messages or advertising incorrect paths. This can be difficult to detect, because false routing messages could be benificial, just the

result of an outdated routing table. Other active attacks include energy exhaustion attacks and denial-of-service (DoS) attacks. DoS attacks can be launched by a rogue node by sending a large number of route requests or by a node spoofing its IP and sending route requests with a fake ID to the same destination, causing a DoS at the destination node.

III. ANOMALY DETECTION FOR WIRELESS ADHOC NETWORKS

In this scheme every node in the adhoc network participates in intrusion detection and response. Every node is responsible for detecting signs of intrusion locally and independently by monitoring activities such as user and system activities and the communication activities within the radio range, but neighboring nodes can investigate a broader range collaboratively. The internal structure of the detection scheme is shown conceptually in the following Figure 1. Information-theoretic measures [17] such as entropy and conditional entropy are used to describe the characteristics of normal information flows and classification algorithms are used to build anomaly detection models. For example, a classifier trained using normal data can be used to predict the next event, given the previous n events. In monitoring, when the actual event is not what the classifier has predicted, there is an anomaly [16]. When constructing a classifier, features with high information gain (or reduction in entropy) are needed. That is, a classifier needs feature value tests to partition the original (mixed and high entropy) dataset into pure (and low entropy) subsets, each ideally with one (correct) class of data.

The following procedure is used for anomaly detection.

- Select (or partition) audit data so that the normal dataset has low entropy.
- Perform appropriate data transformation according to the entropy measures.
- Compute classifier using training data.
- Apply the classifier to test data
- Post-process alarms to produce intrusion reports.

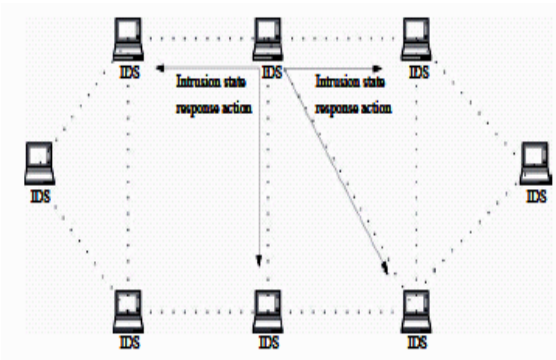


Fig1: Intrusion detection system (IDS) architecture for gíreles adhoc networks

IV. INTRUSION PREVENTION FOR WIRELESS ADHOC NETWORKS

Intrusion prevention systems (IPS) are network security appliances that monitor network and/or system activities for malicious activity [15]. The main functions of intrusion prevention systems are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity. Intrusion prevention systems can be classified into different types and they are

A. Network-based intrusion prevention system (NIPS):

The network based intrusion system is designed to passively monitor traffic and raise alarms when suspicious traffic is detected where as network based intrusion prevention system is designed to go one step further actually try to prevent the attack from succeeding. This is achieved by inserting the NIPS device inline with the traffic it is monitoring. Each network packet is inspected and passed only if it does not trigger some sort of alert based on a signature match or anomaly threshold. Suspicious packets are discarded and an alert is generated.

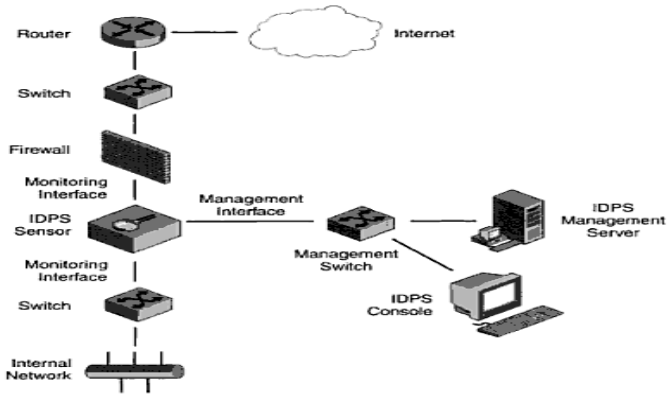
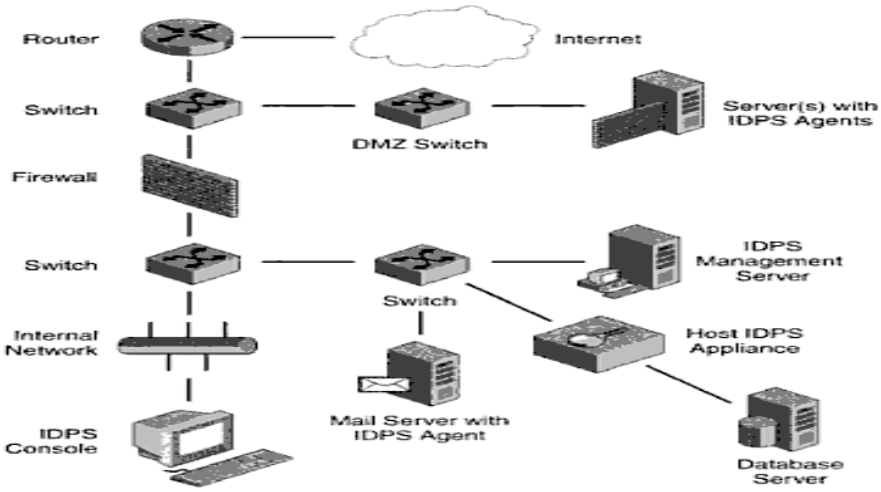


Fig 2: Network Based Intrusion Prevention Configuration

B. Host-based intrusion prevention system (HIPS):

In Host Based Intrusion prevention system installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host. The advantage of HIPS is that encrypted network traffic can be analyzed after the decryption process thus providing an opportunity to detect an attack that would have been hidden from NIPS device moni



C. Wireless intrusion prevention systems (WIPS)

This monitors a wireless network for suspicious traffic for the presence of unauthorized access points and can automatically take counter measures. These are typically implemented as an overlay to an existing wireless LAN infrastructure although they may be deployed standalone to enforce no wireless policies with in an organization. The types of threats can be prevented by a good WIPS are Client Mis-association, Unauthorized association, Man in the Middle Attack, Ad-hoc Networks, Mac-Spoofing, Denial of Service (DoS) Attack.

V CONCLUSIONS

As the use of adhoc networks has increased, the security has also become more important accordingly.Historical events show that prevention alone, i.e., cryptography and authentication are not enough; therefore, the intrusion detection systems are brought into consideration. Since most of the current techniques were originally designed for wired networks, many researchers are engaged in improving old techniques or finding and developing new techniques that are suitable. With the nature of adhoc networks, almost all of the intrusion detection systems (IDSs) are structured to be distributed and have a cooperative architecture. The number of new attacks is likely to increase quickly and those attacks should be detected before they can do any harm to the systems or data. Hence, IDS's in adhoc networks prefer using anomaly detection to misuse detection. An intrusion detection system aims to detect attacks on nodes or intrusions into the networks. The main functions of intrusion prevention systems are to identify malicious activity. However, attackers may try to attack the IDS system itself.

REFERENCES

[1] Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

[2] A. Mishra, K. Nadkarni, and A. Patcha, \Intrusion Detection in Wireless Ad Hoc Networks," IEEE Wireless Communications, Vol. 11, Issue 1, pp. 48-60, 2004.

[3] Anantvalee T, Wu J (2006) A Survey on Intrusion Detection in Mobile Ad Hoc Networks. Wirel/Mobil Netw Secur, Springer:170-196

[4] C. Endorf, E. Schultz and J. Mellander, "Intrusion Detection & Prevention", McGraw-Hill, ISBN: 0072229543

[5] Y. Zhang, W. Lee, "Intrusion detection in wireless ad-hoc networks", The 6th Annual International Conference on Mobile Computing and Networking, pp. 275–283, 2000

[6] Kejun Liu, Jing Deng, Member, IEEE, Pramod K. Varshney, Fellow, IEEE, and Kashyap Balakrishnan, Member, IEEE, "An Acknowledgment-Based Approach for the Detection of Routing Misbehaviour in MANETs", IEEE Transactions on mobile computing, Vol. 6, NO. 5, May 2007.

[7] S.Madhavi and Dr. Tai Hoon Kim "An Intrusion Detection System in Mobile Ad hoc Networks" International Journal of Security and its Application, 2, No 3, 2008.

[8] Asmaa Shaker Ashoor and Prof. Sharad Gore "Importance of Intrusion Detection System (IDS)" International Journal of Scientific & Engineering Research, January-2011

[9] E. Y. K. Chan et al., \IDR: An Intrusion Detection Router for De-fending against Distributed Denial-of-Service (DDoS) Attacks," Pro-ceedings of the 7th International Symposium on Parallel Architectures,Algorithms and Networks (ISPAN'04), pp. 581-586, May 2004.

[10] S. Bo, W. Kui, U.W. Pooch. "Towards adaptive intrusion detection in mobile ad hoc networks". IEEE Global Telecommunications Conference, pp. 3551–3555, 2004

[11] C.M. Chlamtac, J.J.-N. Liu, "Mobile ad hoc networking: imperatives and challenges", Ad Hoc Networks 1, 2003
[12] D. Sterne, P. Balasubramanyam, et al. "A General Cooperative Intrusion Detection Architecture for MANETs". In Proceedings of the 3rd IEEE International Workshop on Information Assurance (IWIA'05), pp. 57-70, 2005
[13] Burtch, P. and Ko, C., Challenges in intrusion detection for wireless ad-hoc networks, Symposium on pplications and the InternetWorkshops (SAINT'03 Workshops), 2003.
[14] Marti, S., Giuli, T., Lai, K. and Baker, M., Mitigating routing misbehavior in mobile ad hoc networks, in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, pp. 255–265, August2000.
[15] Zhou, L. and Hass, Z.J., Securing ad hoc Networks, IEEE Network, 13(6):24–30, 1999.
[16] Amitabh Mishra " Security and Quality of Service in Adhoc Wireless Networks" 2008
[17] Y. Okazaki, I. Sato, and S. Goto, ''A new intrusion detection method based on process profiling,'' Symposium on Applications and the Internet, 28 Jan.–1 Feb. 2002, pp. 82–90.

