모바일 에드혹네트워크를 위한 효과적인 침입 탐지 시스템

Rakesh Shrestha[*], 박규진[*], 박광채[**], 최동유[*], 한승조[1*]
조선대학교

An Effective Intrusion Detection System for MobileAdHocNetwork

Rakesh Shrestha[*], Kyu-jin Park[*], Kwang-chae Park[**], Dong-you Choi[*], Seung-jo Han[1*]
Department of Information and Communication Engineering[*]
Department of Electronics Engineering[**]
Chosun University
[1*]Corresponding author. E-mail : sjbhan@chosun.ac.kr

ABSTRACT

The intrusion detection system is one of the active fields of research in wireless networks. Intrusion detection in wireless mobile Ad hoc network is challenging because the network topologies is dynamic, lack centralization and are vulnerable to attacks. This paper is about the effective enhancement of the IDS technique that is being implemented in the mobile ad hoc network and deals with security and vulnerabilities issues which results in the better performance and detection of the intrusion.

Keywords
Intrusion detection, mobile ad-hoc network, IDS technique

1. Introduction

The intrusion detection system is one of the active fields of research in wireless networks. Intrusion detection in wireless mobile Ad hoc network is challenging because the network topologies is dynamic, lack centralization and are vulnerable to attacks. This paper is about the effective enhancement of the IDS technique that is being implemented in the mobile ad hoc network and deals with security and vulnerabilities issues which results in the better performance and detection of the intrusion.

MANETis the abbreviation of mobile ad-hoc network which is a kind of wireless ad-hoc network, and is a self-configuring network of mobile nodes and associated hosts connected by wireless links. Some of the characteristic features of MANET are the nodes are free to move randomly i.e. they have high mobility, organize themselves arbitrarily, dynamic network topology and hence they have decentralized network control. Such a network may operate in a standalone fashion, or may be connected to the larger network and consume very low power and resources. One of the differences between fixed wired and mobile wireless networks is that mobile nodes have a very limited bandwidth and battery power because efficient host-based monitoring requires large amounts of CPU processing power, and hence is energy consuming.

A wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure. Nodes within each other's radio range communicate directly via wireless links, while those that are out of range use other nodes as relays. Various protocols are designed to manage the new distributed communication platform on different layers. Nodes usually share the same physical media; they transmit and acquire signals at the same frequency band, and follow the same hopping sequence or spreading code. The data-link-layer functions manage the wireless link resources and coordinate medium access among neighboring nodes. The medium access control (MAC) protocol allows mobile nodes to share a common broadcast channel. The network-layer maintains the multi-hop communication paths across the network; all nodes must function as routers that discover and maintain routes to other nodes in the network. Mobility and volatility are hidden from the applications so that any node can communicate with any other node as if everyone were in a fixed wired network. There are various applications of ad-hoc networks like emergency search-and-rescue missions, military, data collection etc.

1.1 Vulnerabilities in MANET

The very advantage of mobility in MANET leads to its vulnerabilities. Wireless networks have become an important aspect in our daily lives as they are increasingly used in numerous applications. But the inherent nature of the wireless medium makes it susceptible to variety of security attacks ranging from passive eavesdropping to active interference. The wireless intrusion detection system is more complex than wired systems. Intrusion prevention mechanisms such as secret key and encryption are used in the presence of malicious nodes. However, these authentication mechanisms are not sufficient and effective against internal attacks as the secret key is compromised when its node is compromised. In order to secure MANET, we need a second line of defense to detect the intrusions [4]. For this purpose, Intrusion Detection Systems (IDS) are deployed to identify any set of actions that compromise the integrity, confidentiality and availability of resources. Misuse and anomaly detection are common IDS techniques that are used to study the abnormalities in the system to detect if an intrusion has occurred.

The lack of centralized authority and management results some wireless network to rely on the cooperative participation of all nodes and the infrastructure. So, the adversaries can exploit this vulnerability and new types of attacks break the cooperative algorithm. In addition to this, wired networks is less prone to denial of service as the physical network and the MAC layer are isolated from the external world by the firewall and the layer 3 gateways where as the MANET are vulnerable to these attacks due to open medium, limited bandwidth, slower links, higher costs, battery constrains and disconnected operations.

1.2 Challenges faced by MANET

Intrusion prevention techniques such as encryption, using password or biometrics are the first line of defense and are not sufficient in MANET due to its wireless mobile structure. In case of DoS attacks, the goal of the attacker is to weaken the resources of the networks and cause it to malfunction. In this, an attacker can damage and replace a node by stealing or replacing the information or cryptographic keys. In short, the DoS attacks cause disabling of service, exhaustion, service degradation and sometimes non-availability of the network infrastructure. In order to detect DoS attacks, conventional systems use a network IDS that resides in a gateway node and monitors the network for abnormal network behavior. In a wireless ad hoc network, a dedicated gateway node cannot be assumed because of the fugacious nature of the network. Intrusion detection can be used as second wall of defense to protect the network systems as once the intrusion is detected in the early stage of the DoS attack, response can be put into place to minimize damages, gather evidence for prosecution and even lunch counter-attacks.

2. Intrusion Detection System (Background)

An Intrusion Detection System (IDS) is a software or hardware tool used to detect unauthorized access of a computer system or network. An intrusion attempt or a threat to be the potential possibility of a deliberate unauthorized attempt to access information, manipulate information, or render a system unreliable or unusable. Intrusion detection involves capturing audit data and reasoning about the evidence in the data to determine if the system is under attack or not. Depending on the scope of protection or deployment and according to audit data used, IDSs can be classified as network-based or host-based. Normally a network based IDS runs at the gateway of a network which inspect network traffic that identifies and captures the abnormal network packets. But a host-based IDS relies on the operating system audit data to monitor and analyze the events generated by the execution of system programs, various system logs or users activities on the local host. Again, depending upon the detection model IDS is usually classified in one of two ways, with either signature-based or anomaly based detection.

2.1 Intrusion Detection Models:

2.1.1 Anomaly Detection: The anomaly detection observes the flag activities and if it is deviated from the normal activity profile then an anomaly alarm will be raised indicating possible intrusion and can identify the statically significant amounts of intrusion attempts. It assumes that all intrusive activities are inevitably anomalous. The main advantage of anomaly detection is that it does not require prior knowledge of intrusion and hence can detect new intrusions. Some of the disadvantages of anomaly detection are that it may not be able to describe what the attack is and may have high false positive rate. Anomaly detection systems are also computationally expensive because of the overhead of keeping track of, and possibly updating several system profile metrics. The approaches used in this model are Statistical approaches, and Predictive pattern generation.

2.1.2 Misuse Detection: The basic idea behind this detection strategy is that the attacks are represented in the form of a pattern or a signature so that even variations of the same attack can be detected. Misuse detection system use weak spot of the system or patterns of the well known attacks to match and identify known intrusions and recognize the "bad" behavior. The main advantage of misuse detection is that it can accurately an efficiently detect instances of known attacks and the disadvantage is that it lacks the ability to detect the new attacks whose signature has not been written. The approaches used in this model are Expert systems, Keystroke monitoring, Model based Intrusion detection and State Transition Analysis.

2.2 Difficulties Faced by current IDS Techniques

The intrusion detection technique which is developed for wired network environment has to face many problems when implementing these techniques in the MANET because of the vast difference between these two network structures.

Further, the available audit trace will be limited within the radio range and it often adopts disconnected operations. In the mobile environment, there may perhaps not be clear separation between normalcy and anomaly. A node that has been compromised or that has been temporarily out of sync due to volatile physical movement may send out false routing information as a consequence it may be difficult for the intrusion detection to distinguish false alarms from real intrusions. So for developing a good intrusion detection system for MANET one should focus on the appropriate audit data sources and system architecture that fits the feature of mobile ad-hoc networks.

3. Intrusion Detection System Architecture

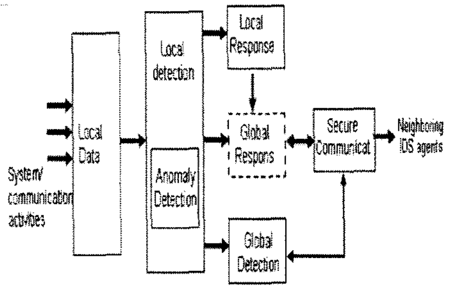

FIG.1 Intrusion Detection System Architecture

The intrusion detection and response system used in the mobile ad-hoc network should be both distributive and cooperative for better performance [6]. The presented IDS architecture consists of six modules. The individual IDS agents are placed on each and every node which detects intrusions from local traces and initiates response.

3.1 Local Data Collection: The real time audit data from various sources is collected at the local level in a distributed manner. Each node IDS component will gather relevant data from listening to network traffic, these data includes the user and system activities within the mobile node as well as the communication activities within the radio range of the node.

3.2 Local Detection: The local detection engine examines the local data traces gathered by the local data collection module for evidence of anomalies. It can include both misuse detections and anomaly detections. Anomaly detection engine plays a greater role for newly created attacks on MANET networks.

3.3 Local Response: According to the Local Detection, appropriate response should be made such as reinitializing communication channels between nodes, identifying compromised nodes and reorganizing the network to omit the promised nodes. It can also send a re-authentication request to all the nodes in the network to prompt the end users to authenticate themselves and those nodes which negotiate new communication channels is regarded as legitimate node.

3.4 Co operative or Global Detection: If local data cannot fully support a decision and needs broader investigation then global or co operative detection is initiated. If anomaly detected is inconclusive then neighboring IDS agents will cooperatively participate in global intrusion detection action.

In distributed intrusion detection procedure, each node sends an intrusion state request to its neighboring node and these nodes again sends state information to its immediate neighbors indicating probability of intrusion. Depending upon the majority of received reports from the neighboring nodes, it is concluded that the network is under attack and response procedure is initiated.

3.5 Global Response: Once a global response is recommended for a detected intrusion, each node IDS components must communicate with other nodes to initiate and follow-through with action.

3.6 Secure Communication: In some cases, we may need to exchanged between node IDS in a secure manner. We plan to determine times when this may not be required to reduce overhead in the system.

4. DoS attacks in different Protocol layers

It is difficult to identify intrusions in the networks as nodes may fail to provide services due to genuine reasons such as network congestion, link failure or topology changes, thus causing high false positives. DoS attacks could be launched at multiple layers of the protocol suite [5]. By detecting abnormal behavior at different layers and using information across layers, we can detect malicious nodes with increasing accuracy.

4.1 Collision: An adversary node can induce a collision in the wireless channel by transmitting when another node in its range is already in transmission. The purpose of this attack is to either prevent access to a certain node or to exhaust the transmitting node's resources by continuous retransmissions.

4.2 Packet drop: At the network layer, the adversary node can randomly drop the control or data packets. This results in denial of service to the destination node, hence affecting the availability of the node.

4.3 Misdirection: Misdirection attack is a routing protocol DoS attack which occurs when the adversary node forwards the data packet to the wrong destination node also the adversary node can deny the availability of an existing route to the destination by sending false Route Error (RERR) messages.

5. Cross Layer Intrusion Detection System

The vulnerabilities of multiple layers in the wireless ad-hoc network have necessitated the need for an integrated intrusion detection module that runs across the different layers of the protocol stack. A cross-layer based IDS architecture using anomaly detection results for efficient intrusion detection by learning behavioral information from two or more layers used in detection. Multiple levels of detection are performed across different layers of the protocol stack before confirming the malicious behavior of the nodes, thus reducing false positives.

5.1 Integration Scheme

The following integration schemes are used:

-If a node detects an intrusion that affects the entire network, e.g., when it detects an attack on the ad hoc routing protocols, it initiates the re-authentication process to exclude the compromised/malicious nodes from the network.

-If a node detects a local intrusion at a higher layer, e.g., when it detects attacks to one of its services, lower layers are notified. The detection modules there can then be further investigated.

5.2 Cross layer design Configuration

There are two main configurations in cross layer design [1]. They are:

a.) Multiple data collection and multiple data analysis (MCMA): In this type of analysis, every chosen layer has its own data collection and analysis module and their detections are performed independent of other layers. However, for the final decision, the predictions from individual layers are weighed and correlated. It is similar to having individual IDS at each chosen layer.

b.) Multiple data Collection and a Single data Analysis (MCSA): A single data analysis module is located in an optimal layer in case of MCSA. A data collection module is designated for every chosen layer. These collection modules collect behavioral information consisting of layer-specific features and forward it to the data analysis module. The features from different layers are processed at the single data analysis module for a decision about the uncategorized behavior. MCSA reduces the overhead by using a single data analysis component in a convenient location. Also correlating and combining features from different layers is most vital to cross layer based intrusion detection. Therefore, attacks targeted at or sourced from any layer can be detected promptly. This paper mainly focuses on MCSA analysis.

The selection of the right combination of layers in cross layer IDS design is crucial as different combination of layers helps to detect different kinds of attacks. For illustration, attacks on the application layer can be detected by combining application and transport layers whereas for behavior information physical layer and network layer is essential.

The proposed intrusion detection mechanism is enabled by triggering detection across the protocol layers. There are two levels of intrusion detection- Level 1 detection and Level 2 detection. The two levels of detection occur at the same layer of the protocol stack. The level 1 detection is only passive monitoring of nodes to obtain information about the network. Based on the first level of detection, a level 2 detection is triggered but within the same layer. This detection often obtains the information from different protocol layers thus exploiting the cross-layer interactions. The advantage of this approach is that the nodes do not have to spend energy in performing the first level of detection hence it is energy efficient which is essential in MANET.

Each layer consists of a data collection model which collects all the relevant data regarding the intrusion occurs in each layer. The collision attacks are detected using a link layer monitoring mechanism. A monitoring node is used which have sufficient power to monitor and report the detection but the compromised node should not be chosen as the monitor node. On the basis of monitor node's decision, it can classify and detect the malicious node. The node that occurs repeatedly in more than one list is grouped into a Hit list to narrow down the suspicious node list. These are collected by the data collection model present in the link layer and these specific information is again transmitted to the next layer. The data collection module present in the network layer collects all the relevant data regarding DoS attacks such as packet drop and misrouting in this layer. For this, the DSR routing protocol can be used for detecting intrusions. The packet drop may occur due to several reasons like network congestion, lack of energy resources, poor channel conditions, or malicious behavior and these behaviors are regarded as misbehavior.

Misdirection is another DoS attack which frequently occurs in the routing protocol of the network layer. To prevent this attack the monitoring node algorithm is extended to check whether the packet transmitted by next hop is sent to the required destination or not. If it behaves maliciously then it is assumed as intrusion. All these information are collected in the data collection module and then it is send to the data analysis module for further analysis. According to the result of the data analysis module, the node which is suspected is considered to be malicious.

6. Conclusion

Hence, a better intrusion detection mechanism based on anomaly detection in distributive and cooperative environment is presented in this paper. A cross-layer based intrusion detection engine is designed to detect DoS attacks at different layers of the protocol stack. This cross layer approach is based on MCSA for effective intrusion detection system. Since, a single data analysis module is present which collects and analyze the data that are collected from data collection module present in each designated layer, the data analysis overhead as well as the energy consumption is reduced. Also, cross layer detection confirms the misbehavior caused by malicious node in the network, thus reducing the false positive rates and hence enhanced the accuracy in detecting attacks.

Future work will involve research into more robust and intelligent IDS system which involves the application layer in the cross layer design because attack is detected much earlier in this layer due to presence of richer semantic information.

References

[1]. John Felix Charles Joseph, Amitabha Das, Boon-Chong Seet, Bu-Sung Lee .Cross Layer versus Single Layer Approaches for Intrusion Detection in MANETs Center for Multimedia and Networks (CEMNET) School of Computer Engineering, Nanyang Technological University, Singapore.

[2]. Zheng Yan. Security in Ad Hoc Networks Networking Laboratory Helsinki University of Technology.

[3]. D. Sterne1, P. Balasubramanyam2, D. Carman1, B. Wilson1, R. Talpade3, C. Ko1, R. Balupari1, C-Y. Tseng2, T. Bowen3, K.Levitt2 and J. Rowe2. A General Cooperative Intrusion Detection Architecture for MANETs

[4]. Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in Mobile Computing and Networking, pp. 275 - 283, 2000.

[5]. Thamilarasu, G., et al. A cross-layer based intrusion detection approach for wireless ad hoc networks. in Mobile Ad hoc and Sensor Systems Conference, 2005. IEEE International Conference on 2005.

[6]. Yongguang Zhang Wenke Lee and Yi-an Huang. "Intrusion Detection Techniques for Mobile Wireless Networks". Wireless Networks. Kluwer. 2003. ACM/Kluwer Wireless Networks Journal, Sept; 9(5):545-56 (2003)

[7]. Jeff Dixon. Wireless Intrusion Detection Systems Including Incident Response & Wireless Policy.

[8]. Slobodan Petrovic. Vulnerabilities in wireless networks and intrusion detection.

[9]. Christopher Besemann, Satoshi Kawamura, Florent Rizzo. Intrusion Detection System in Wireless Ad-Hoc Networks:Sybil Attack Detection and Others Department of Computer Science, North Dakota State University.

[10]. Yi-an Huang. Anomaly Detection for Wireless Ad-Hoc Routing Protocols. A thesis submitted to the Graduate Faculty of North Carolina State University in partial fulfillment of the requirements for the Degree of Master of Science COMPUTER SCIENCE Raleigh 2001.

※This work was supported in part by MIC & IITA
<08-Infra-13, IT Research Infrastructure Program>