Intrusion Detection Techniques for Detecting Misbehaving Nodes

Farzaneh Pakzad (Corresponding author)
Tiran Branch, Islamic Azad University, Tiran, Iran
Tel: 98-91-3918-7090 E-mail: f_pakzad@iautiran.ac.ir

Marjan Kuchaki Rafsanjani
Department of Computer science, Shahid Bahonar University of Kerman, Kerman, Iran
E-mail: kuchaki@mail.uk.ac.ir

Abstract

A Mobile Ad hoc Network (MANET) consists of a group of autonomous mobile nodes with wireless transmission capability without using any existing infrastructure or centralized administration. The MANET environment is particularly vulnerable due to its dynamic topology, less powerful mobile devices and distributed environment. Current solutions for security are more geared towards wired networks. Therefore, they are not applicable for wireless ad hoc networks and cannot be applied without modifications in this environment. In this paper, we classify the techniques for intrusion detection systems (IDS) that have been introduced for MANETs, and compare some important aspects such as performance and overhead in these techniques. Finally we provide some directions for further research.

Keywords: Intrusion Detection System (IDS), Cooperative, Misbehaving, Mobile Ad Hoc Network (MANET), Security

1. Introduction

Mobile ad hoc network is a network consisting of mobile nodes (Laptop, Personal Digital Assistants (PDAs) and wireless phones) with the characteristics of self-organization and self-configuration which enable it to form a new network quickly. MANETs are highly vulnerable to several types of attacks, due to their open medium, lack of centralized monitoring, management point, and lack of strong line of defense. Therefore, deploying security in mobile ad hoc networks is important (Zhang Y, Lee W, Huang Y, 2003).

The first line of defense is to prevent attacks, using verification and encryption methods; however, past experiments have shown that encryption and authentication used as intrusion prevention are not sufficient. So, to resist against attacks, a second wall is needed which is Intrusion Detection (ID) that Monitoring activities for policy violation in mobile ad hoc networks. These two mechanisms should act together to ensure high security requirements (Mishra A, Nadkarni K, Patcha A, 2004).

An intrusion can be defined as any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource. This can be something as severe as stealing confidential data or misusing the email system for spam. Intrusion detection can be defined as a process of monitoring activities in a system whether a computer or a network. An Intrusion Detection System (IDS) is a system for detecting such intrusions (Zhang Y, Lee W, Huang Y, 2003)(Chaki R, Chaki N, 2007).

There are two basic types of intrusion detection: host-based and network-based. Each has a distinct approach to monitoring and securing data, and each has distinct advantages and disadvantages. In short, host-based IDSs examine data held on individual computers that serve as hosts, while network based IDSs examine data exchanged between computers (Beghdad R, 2008).

In this paper, the most important techniques for intrusion detection to achieve secure systems will be investigated and compared.

Intrusion detection techniques can be mapped into four classes: anomaly detection, misuse or Signature-based detection, specification-based detection, and model-based detection. Anomaly detection consists of establishing normal behavior profile for user and system activity and observing significant deviations of actual user activity with respect to the established habitual pattern. Misuse detection, refers to intrusions that follow well defined attack patterns that exploit weaknesses in system and application software (Beghdad R, 2008). Misuse detection has a low error rate (false positives rate) on known attacks but anomaly detection is the only means to catch new attacks (Zhang Y, Lee W, Huang Y, 2003). Signature-based schemes provide very good detection results for specified, well-known attacks. However, they are not capable of detecting new, unfamiliar intrusions, even if they are built as minimum variants of already known attacks. On the contrary, the main benefit of anomaly-based detection techniques is their potential to detect previously unseen intrusion events. However, despite the likely inaccuracy in formal signature specifications, the rate of false positives (or FP) in anomaly-based systems is usually higher than in signature based ones (Garcia-Teodoro P, Diaz-Verdejo J, Macia´Ferna´ndez G, Va´zquez E, 2009). In specification- based detection, the correct behaviors of critical objects are manually abstracted and crafted as security specifications, which are compared with the actual behavior of the objects. Intrusions, which usually cause object to behavior in an incorrect manner, can be detected without exact knowledge about them. Model-based intrusion detection compares a process's execution against a program model to detect intrusion attempts (Beghdad R, 2008).

A wired network under a single administrative domain allows for discovery, repair, response, and forensics of suspicious nodes. A MANET is typically not under a single administrative domain, making it difficult to perform any kind of centralized management or control (Chaki R, Chaki N, 2007).

Many intrusion detection systems proposed in the wired network were installed on the switches, routers or gateways through which all network traffic can be monitored. So intrusion detection systems can easily add and implement in these elements. MANET scenario is very different, because of the lack of any fire walls and gateways in these networks. In addition, the medium environment is wide open to the extent that allows the normal and malicious user to have access to it. Moreover, there is no clear separation between normal and unusual activity in the mobile environment. While the nodes can move arbitrarily, incorrect routing information can be sent from a compromised node or the one with outdated information. Thus, the current IDS techniques on traditional networks do not apply on Ad hoc networks. Many intrusion detection techniques for MANET have been proposed that some of which will be discussed in the next sections (Huang Y, Lee W, 2003).

2. Intrusion Detection Techniques in Mobile Ad hoc Networks

As there is no any fixed infrastructure in mobile Ad hoc networks, all nodes should cooperate with each other in routing and transmitting the packets to deliver the packets to the specified destination. Intermediate nodes may agree to forward packets, but in fact they delete or modify them, because they are malicious. Only a few misbehaving nodes (malicious nodes, selfish nodes) can decrease whole system performance. Several methods and protocols have been proposed to detect and prevent such misbehaving nodes, and some projects have also suggested punishment (Jou Y F, Gong F, Sargor C, Wu X, Wu S, Chang H, F. Wang, 2000)(Chan E Y K et al. 2004).

2.1 Watchdog

Watchdog identifies misbehaving node by eavesdropping on the transmission of the next hop. When a node forwards packets, Watchdog verifies whether the next node in the route forwards the packets or not. If the next node refuses to forward the packets, then it is known as misbehavior. Figure 1 shows how the Watchdog works. Suppose that node S wants to send a packet to node D, there is a path from S to destination D through node A, B and C (Kachirski O, Guha R, 2003).

Consider now A receives the packet from S to destination D; packet contains message and routing information. When A forwards this packet to B, A also keeps a copy of the packet in its buffer. Then, it promiscuously listens to the transmission of B to make sure that B forward the packet to C. If the packet overheard from B (represented by a dashed line) matches what is stored in the buffer, it means that B really forwards to the next hop (represented as a solid line). Then, it removes the packet from the buffer. However, if there's no matched packet after a certain time, the Watchdog increments one to failure counter of node B. If this counter exceeds the threshold, A concludes that B is misbehaving and reports to the source node S (Kachirski O, Guha R, 2003).

The advantages of Watchdog mechanism is that it can identify misbehaving nodes not in forwarding level but also in the level of connection. In other words, it identifies nodes not only in the link layer, but also in the network layer. Implementation of Watchdog is relatively easy (Kachirski O, Guha R, 2003).

Watchdog has some obvious disadvantages. For example, due to the lack of cooperation in nodes, it may be unable to identify misbehaving nodes in circumstances such as 1) ambiguous collision 2) receiver collision 3) limited transmission power 4) false misbehaving 5) collision 6) minor dropping (Kachirski O, Guha R, 2003).

Furthermore, two neighbors can collude with each other to deceive Watchdog and the node that detects the intrusion must decide about the final vote all by itself which is not appropriate for nodes with limited resources.

2.2 Pathrater

Pathrater technique calculates "path metric" for every path. Like Watchdog, each node runs Pathrater. The node maintains a degree of other nodes identified in the network. The path metric which is collected from past experience can be calculated by combining the node rating with link reliability. After calculating the path metric for all reachable paths, the path with the highest metric can be chosen by the pathrater. In addition, if the link reliability is not collected, it allows the Pathrater to estimate the shortest path algorithm as it is explained below. The path with highest metric will be chosen, if there are several identical routes to a destination. Consequently, paths containing misbehaving nodes will be avoided.

The degrees of node will be set by Pathrater according to the following path algorithm. When one node in the network is known for Pathrater (through the route discovery), the Pathrater sets a 0.5 “neutral” degree for it. A node always sets its own rate on 1.0. If all nodes are neutral (rather than misbehaving nodes) and path rates are calculated, the Pathrater certainly chooses the path with shortest length degree. Maximum amount for a neutral node is 0.08. Pathrater doesn`t alter the degree of a node which is not participating in routing (Kachirski O, Guha R, 2003).

According to the simulation result, the system with Watchdog and Pathrater is quite effective in route selection to avoid misbehaving node. However, the misbehaving nodes are not punished. In contrast, they even advantage from the network which encourages them to continue their malicious behavior. Watchdog mechanism and Pathrater with DSR increase the performance to 27% when 12% to 24% overhead appears; Watchdog itself adds very little overhead (Kachirski O, Guha R, 2003). The important advantage is that we have a route without any misbehaving node.

2.3 Routeguard

Routeguard employs a smart and smooth architecture in order to effectively discover malicious nodes and then proceeds to protect the network. Simulation results demonstrate that this scheme improves network throughput by smartly classifying the nodes into different categories depending on their current actions and previous history. This system categorizes each neighbor node by combining Watchdog and Pathrater. This categorization is as follows: Fresh, Member, Unstable, Suspect, or Malicious. Moreover, the class of each node depends on the ratings achieved from the Watchdog according to its behavior. Furthermore, each class or tag implies a different trust level which goes from trusted (Member), allowing the node to participate in the network, to completely un-trusted (Malicious), being excluded from the network. A simulation model for this system has been developed in Network Simulator (NS-2) (Hasswa A, Zulkernine M, Hassanein H, 2005).

2.4 Hop-by-hop signing

This system proposed a secure routing system which would allow intrusion detection. The different public key management protocols for MANETs are review in this paper. The public key infrastructure provides public key encryption and signatures for every node. According to the structure presented in Fig. 2, A could send signed packets to C through B, and C could authenticate that they came from A. Lastly, Watchdog technique is presented as a solution to avoid denial of service attacks such as Black and Grey Hole routers. However, this system has been thought for short paths (for one or two hops as maximum) (Caballero E J, 2006).

2.5 Patwardhan secure routing and intrusion detection system

This technique presents a proof of concept where a secure routing protocol is implemented by using public key encryption, intrusion detection, and a reaction system. The system implements a secure routing protocol, adding public key signatures to validate the ownership of the messages. In addition, it has an intrusion detection system where each node monitors its neighbors in a promiscuous mode by listening to their routing activity. When a node claiming to be a router, is detected as misbehaving, the detection system marks the node as malicious node and the reaction system isolates the node from the MANET (Caballero E J, 2006).

Some complex IDS techniques (such as Hop-by-hop signing and Patwardhan secure routing) require public key encryption operations in each node. This method improves the systems security by adding all the advantages from the public key cryptography; however, due to its efficiency, the public key cryptography implies a higher overhead for each operation. This higher overhead for the operations facilitates Resource Exhaustion attacks (Caballero E J, 2006).

2.6 ExWatchdog

Nasser and Chen (Kachirski O, Guha R, 2003) have proposed techniques to identify IDS called ExWatchdog which is actually an extension of Watchdog. ExWatchdog also detects intrusion from malicious nodes and reports this data to the response system, i.e., Pathrater or Routguard (Hasswa A, Zulkernine M, Hassanein H, 2005). Watchdog which is based on overhearing resides in each node. Each node can detect the malicious action of its neighbors through overhearing and can report this misbehaving to other nodes. However, if the node that is overhearing and reporting is malicious itself, it can make a serious impact on network performance. The main feature of the proposed system is the ability to detect malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then it proceeds to protect the network. So, ExWatchdog solves the fatal problem of Watchdog (Rafsanjani M k, Movaghar A, Koroupi F, 2008).

2.7 CONFIDANT

Buchegger and LeBoudec(Buchegger S, Le Boudec J, 2002) proposed a CONFIDANT (Cooperation Of Nodes, Fairness In Dynamic Ad hoc Networks) which is in fact an expansion of DSR protocol. This technique is similar to Watchdog and Pathrater. Each node monitors the behaviors of neighbor nodes within its radio range and learns from them. This protocol resolves the Watchdog and Pathrater problem, meaning that it does punish misbehaving nodes by not using them in routing and not forwarding packets through them. In addition, when a node detects a misbehaving node, it sends a warning to all other nodes and they do not use this node either. CONFIDANT protocol consists of Monitoring System, Reputation System, Trust Manager and Path Manager. Their tasks are divided into two sections: the process to handle their own observations and the one to handle reports from trusted nodes.

For observations, the monitoring node uses a "neighborhood watch" within its radio range to discover any malicious behaviors. If a dubitable event is detected, monitoring node then reports it to the reputation system. At that time, the reputation system accomplishes several checks and updates the rating of the reported node in the reputation table. If the rating result is dubitable, it forwards the information to the path manager, which then omits all paths containing the misbehavior node. Then the trust manager sends An ALARM to warn other nodes that consider these nodes as friends (Buchegger S, Le Boudec J, 2002).

When the monitoring node receives an ALARM message from trusted nodes, at first the trust manager evaluates the message to see if the source node is trustworthy. If so, the ALARM message with the trust level will be stored in the alarm table. All ALARM messages of the reported node will then be combined to see if there is enough evidence to identify the malicious one. In this case, the information will be sent to the reputation system, which then performs the same functions as described in the previous paragraph (Buchegger S, Le Boudec J, 2002).

2.8 CORE

A technique which is proposed by Michiardi and Molva detects selfish nodes and forces them to cooperate as well. Similar to CONFIDENT, This technique is based on monitoring system and reputation system, which includes both direct and indirect reputation from the system. Sometimes nodes do not misbehave intentionally; for example when their battery is low, they should not be considered misbehaving nodes and be fired from the network. To do so, the reputation should be rated based on past reputation, which is zero (neutral) at the beginning. In addition, participation in the network can be categorized into several functions such as routing discovery (in DSR) or forwarding packets. The difference between CORE and CONFIDANT is that CORE only allows positive reports to pass through but CONFIDANT allows the negative ones. This means that CORE prevents false reports, and thus it prevents a DOS attack which CONFIDANT cannot do. When a node cannot cooperate, it is given a negative rating and its reputation decreases. In contrast, a positive rating is given to a node from which a positive report is received and then its reputation increases (Michiardi P, Molva R, 2002).

2.9 OCEAN

Bansal and Baker also proposed a protocol called OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks) which is an extension of the DSR protocol. OCEAN like previous techniques uses a monitoring and a reputation system. However, contrary to previous approaches, OCEAN relies only on its own observation to avoid the new vulnerability of false accusation from second-hand reputation exchanges. So, OCEAN can be considered a stand-alone architecture (Bansal S, Baker M, 2003).

OCEAN classified routing misbehavior into two classes: misleading and selfish. If a node participates in the route discovery but does not forward a packet, its class is misleading as it misleads other nodes to route packets through it. But if a node does not even take part in the route discovery, it is considered to be selfish.

In order to detect the misleading routing behaviors, a node buffers the packet checksum after forwarding a packet to a neighbor, then it can monitor if the neighbor attempts to forward the packet within a given time. As a result of monitoring, either a negative or positive event is produced to update the neighbor rating. If the rating is lower than the faulty threshold, that neighbor node is added to a faulty list and then to the RREQ as an avoid-list. In addition, all the traffic from the misbehaving neighbor node will be rejected. This node is given a specific time to return to the network because it is possible that it is wrongly accused of misbehaving or if it is a misbehaving one, it must be improved in this time period. Each node has also a mechanism of maintaining chipcounts for each neighbor to discover the selfish behavior. A neighbor node increases chips when forwarding a packet for other nodes and decreases chips when requesting others to forward a packet. If the chipcount of the neighbor is below the threshold, the packets coming from that neighbor will be rejected (Bansal S, Baker M, 2003).

3. Cooperative Intrusion Detection System

Huang and Lee (Huang Y, Lee W, 2003) proposed a Cooperative Intrusion Detection System based on clustering approaches was similar to Kachirski and Guha's system (Kachirski O, Guha R, 2003). In this method, IDS not only detects an intrusion but also identifies the type of attack and the attacker. This is possible by using statistical anomaly detection. Statistical formulas can define Identification rules to discover attacks. These rules help to detect the type of attack and in some cases the attacking node itself (Huang Y, Fan W, Lee W, Yu P, 2003). In this technique, IDS architecture is hierarchical, and each node has an equal chance of becoming a cluster head. Monitoring the data obtained from the traffic would be which is analyzed for possible intrusions consume power. Therefore, instead of every node capturing all features themselves, the cluster head alone is responsible for computing traffic-related statistics. This can be done because the cluster head overhears incoming and outgoing traffic on all members of the cluster since it is one hop away (a clique: a group of nodes in which each pair of members can communicate via a direct wireless link). As a result, the energy consumption of member nodes is decreased, whereas the detection accuracy is just a little worse than that of not implementing clusters. Besides, the performance of the overall network is noticeably better decreased in CPU usage and network overhead (Xiao Y, Lin Y B, Du D Z, 2006)(Rafsanjani M k, Movaghar A, Koroupi F, 2008). One of these systems which is worked cooperatively is being as follow.

3.1 Snooping packets technique

Snooping protocols have two inherent characteristics in most of the MANET protocols. The first feature is that each node in the network keeps a list of addresses of those nodes near or on the route from source to destination. The Second one is 802.11 and MACAW link layer protocol, when a node is able to "hear" RTS / CTS transmission of its neighbors. So, in the process of intrusion detection of a neighbor, each node "snoops" on its neighbor's transference to ensure that it is not distorted or misrouted (Parker J, Undercoffer J, Pinkston J, Joshi A, 2004).

Jame parker and his colleagues (Parker J, Undercoffer J, Pinkston J, Joshi A, 2004) have introduced a technique based on the snooping packets to discover misbehavior in mobile ad hoc networks. In this plan, appropriate for DSR and other routing protocols, the Snooping nodes listen to all nodes in their proximity. This technique is in complete contrast with Watchdog and (CONFIDENT) Neighborhood watch on DSR that are only watching the next node from source to destination path. Listening to the transferring of neighbors, if a node discovers that another one is malicious then a response mechanism for isolating a malicious one will be launching.

There are two response mechanisms in this plan:

Passive response mode**:** Once a node determines that another one is malicious, unilaterally stops interacting with it. Although each node acts independently, eventually the intrusive node will be isolated from using all network resources (Such as OCEAN).

Active response mode**:** each node relies on the hierarchical categories. When a node detects a malicious neighbor, informs the cluster head which in turn initiates the voting process. If the majority of nodes decide that the suspected one is actually intrusive, a warning will be released throughout the network and intrusive node will be deprived of network resources.

This technique extend watchdog and CONFIDENT by expanding the malicious detection to cooperate with routing protocol other than DSR, and has been proposed a stronger recognition process of the destructive activities in cluster voting scheme.

4. Comparison of intrusion detection techniques

If we review all the above IDS, we can conclude that although the IDS techniques use the watchdog mechanism, they improve it and solve some of its problems. All these IDS are common in detecting selfish nodes. Table 1 represents the final comparison between discussed intrusion detection techniques.

Accordingly, the defense mechanism against such attacks should be explored as well. Also attack models must be carefully established. On the other hand, solutions must consider resource limitations such as energy (Rafsanjani M k, Movaghar A, Koroupi F, 2008).

5. Conclusion and Discussion

As the use of Mobile Ad hoc Networks (MANETs) has increased, the MANETs security has become more important accordingly. No doubt the IDS are here to keep our systems safe; however, future systems will definitely take a different form from our modern-day versions. In this survey research, we have discussed various Intrusion Detection techniques for mobile ad hoc networks. Intrusion detection techniques also should be integrated with existing MANET application. This requires an understanding of deployed applications and related attacks in using suitable intrusion detection mechanisms. An intrusion detection system aims to detect attacks on mobile nodes or intrusions into the networks. However, attackers may try to attack the IDS system itself.

In active black hole attacks on wireless networks malicious nodes advertise the shortest path between source and destination, which leads to modifications in routing table and packet loss. A grouped black hole attack security model stops grouped malicious nodes to advertise the shortest path through them to source and destination hence eliminating routing table modifications and packet loss. In our future work, we will discuss these types of attacks.

References

Bansal S, Baker M. (2003). Observation-based cooperation enforcement in ad hoc networks, *Technical Paper on Network and Internet Architecture (cs.NI / 0307012), Stanford Univ.*

Beghdad R. (2008). Critical study of neural networks in detecting intrusions, *Elsevier Computer & security,* 27, pp 168-75.

Buchegger S, Le Boudec J. (2002). Performance analysis of the CONFIDANT protocol (Cooperation of nodes – fairness in dynamic ad-hoc network) , *in Proceeding 3rd ACM International Symposium on Mobile Ad Hoc Networks and Computer (MobiHoc'02)*, pp 226–336.

Caballero E J. (2006). Vulnerabilities of intrusion detection systems in mobile ad hoc networks- the routing system, *Seminar on Network security, Helsinki University of Technol.*

Chaki R, Chaki N. (2007). IDSX: A Cluster Based Collaborative Intrusion Detection Algorithm for Mobile Ad-Hoc Network, *in Proceeding IEEE 6th International Conference on Computer Information System and Industrial Management Application (CISIM'07),* pp 179-84.

Chan E Y K et al. (2004). IDR: An Intrusion Detection Router for Defending against Distributed Denial-of-Service (DDoS) Attacks, *in Proceeding IEEE International Symposium on Parallel Architecture, Algorithms and Networks (ISPAN'04)*, pp 581-6.

Garcia-Teodoro P, Diaz-Verdejo J, Macia´Ferna´ndez G, Va´zquez E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges, *Elsevier Computer & security,* 28, pp 18–28.

Hasswa A, Zulkernine M, Hassanein H. (2005) Routeguard: an intrusion detection and response system for mobile ad hoc networks, *in Proceeding IEEE International Conference on Wireless and Mobile Computing* (WiMob'2005), 3, pp 336-43.

Huang Y, Fan W, Lee W, Yu P. (2003). Cross-feature analysis for detecting ad-hoc routing anomalies, *in Proceeding 23rd IEEE International. Conference on Distributed Computer System (ICDCS'03),* pp 478-87.

Huang Y, Lee W. (2003). A Cooperative Intrusion Detection System for Ad Hoc Networks, *in Proceeding of the ACM Workshop on security in Ad Hoc and Sensor Networks (SASN'03),* pp 135-47.

Jou Y F, Gong F, Sargor C, Wu X, Wu S, Chang H, F. Wang. (2000) Design and Implementation of a Scalable Intrusion Detection System for the Protection of Networks Infrastructure, *in Proceeding of DARPA Information Survivability Conference and Exposition*, 2, pp 69-83.

Kachirski O, Guha R. (2003). Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks, *in Proceeding IEEE Hawaii International Conference on System Science (HICSS'03),* pp 57.1.

Michiardi P, Molva R. (2002). Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks*, in Proceeding International Conference on IFIP Communications and Multimedia security (CMS'02),* pp 107 – 21.

Mishra A, Nadkarni K, Patcha A. (2004). Intrusion Detection in Wireless Ad Hoc Networks*, in Proceeding IEEE Conference on Wireless Communications*, 11, pp 48-60.

Nasser N, Chen Y. (2007). Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc network*, in Proceeding IEEE International Conference on Communication. (ICC'07),* pp 1154-9.

Parker J, Undercoffer J, Pinkston J, Joshi A. (2004). On intrusion Detection and Response for Mobil Ad Hoc Networks, *in Proceeding IEEE International Conference on Performance Computer and Communications, Workshop on Information Assurance,* pp 747-52.

Rafsanjani M k, Movaghar A, Koroupi F. (2008). Investigating Intrusion Detection Systems in MANET and Comparing IDS for Detecting Misbehaving Nodes, *in Proceeding of the World Academy of Science, Engineering and Technology.* 34, pp 351-5.

Xiao Y, Lin Y B, Du D Z. (2006). Wireless/Mobile Network Security, *EURASIP J. on Wireless Communications and Networking*, ch.7.

Zhang Y, Lee W, Huang Y. (2003). Intrusion Detection Techniques for Mobile Wireless Networks, *ACM/Kluwer Wireless Networks Journal (ACM WINET),* 9, pp 545–56.