Exploring Intrusion Detection Schemes and their Comparison in MANETs

Ankita Chaturvedi
M.Tech. Scholar
Department of CS/IT
M.I.T.S Gwalior, India

Sanjiv Sharma
Assistant Professor
Department of CS/IT
M.I.T.S Gwalior, India

ABSTRACT

The feasibility of mobile ad hoc networks (MANETs) is gaining popularity widely. Due to its fundamental characteristics like dynamic topology, open medium, absence of infrastructure, limited power and limited bandwidth, these networks are more prone to malicious attacks. The prevention methods like encryption and cryptography are not sufficient to make them secure. The reason behind this is that these techniques focus on how to protect the data but do not take any action against the intruder. Therefore some detection mechanism must be deployed to facilitate the identification and isolation of attacks before an attacker breaches the system. This paper presents the existing architectures for intrusion detection systems (IDS) along with intrusion detection techniques in MANETs and their comparison.

GENERAL TERMS

Mobile Ad hoc Networks, Intrusion detection Techniques, Malicious Nodes

Keywords

Mobile ad hoc network, intrusion detection system, malicious attack, encryption, cryptography

1. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of wireless mobile nodes that can dynamically be setup anywhere at any time without using any pre-existing network infrastructure. It is an autonomous system in which mobile nodes connected through wireless links are free to move randomly and also act as routers at the same time. This feature extends the limited wireless transmission range of the mobile nodes by multihop packet forwarding. In the situations where mobile computing devices require networking applications but a fixed network infrastructure is not available or not preferred to be used, ad hoc networks can be formed quickly and easily. The typical features of ad hoc networks are unreliable links, frequent changes in topology and lack of incorporation of security features in statically configured wireless routing protocols [1]. These features make mobile ad-hoc networks more prone to suffer from the malicious behaviors than the traditional wired networks. So, there is a need to pay more attention towards the malicious activities in the mobile ad hoc networks. In most of the routing protocols such as DSR, AODV etc., it is assumed that every node in the network is cooperative and not malicious [2]. Therefore, only one compromised node can cause the failure of the entire network. However prevention methods such as cryptography and authentication [3, 4, 5, 6] are available. Many other techniques have also been proposed and implemented but these applications are not sufficient. If we pay attention towards the detection of attack once it comes into the network, any damage to the system or data can be stopped. This thought made intrusion detection system (IDS) to come into existence.

Intrusion detection is a process of monitoring activities in a system, which can be a computer or network system. The mechanism by which this is achieved is known as intrusion detection system (IDS). An IDS collects the activity information, analyzes it and determine if there are any activities that violate the security rules. If IDS founds that an unusual activity or an attack is occurred, it generates an alarm to alert the security administrator which then initiates a proper response against the malicious activity.

2. BACKGROUND OF IDS

Intrusion prevention techniques are well known for applying encryption and authentication that aids in preventing the data from being intruded. Though prevention schemes have been successfully applied by the analysts but the scheme lacks in performing appropriate action against the intruder, if noticed. That is, intruder is allowed to do anything whatever he can do to break the security. Hence, only these techniques are not sufficient. Intrusion detection techniques can be used to protect the network from such problems. In IDS, if the intrusion is detected, a proper response is initiated to prevent or minimize damage to the system.

There are some assumptions that are made for intrusion detection systems to work [2]. The first is that user and program activities are observable. The second and more important is that normal and intrusive activities must have distinct behaviors. On the basis of these behaviors, IDS captures and analyze system activity to determine if the system is under attack. For achieving this, IDS uses three detection techniques as follows [7]:

1) Signature or misuse based IDS: In it, the system keeps patterns (or signatures) of pre-known attack scenarios and uses them to compare with the captured data. If any matched pattern is found, it is treated as intrusion.

2) Anomaly-based IDS: The normal expected behaviors of the user are kept in the system. Any activity that is found deviated from the expected behavior is treated as intrusion.

3) Specification-based IDS: The system keeps some pre-defined specifications that describe desired functionality for security-critical entities. It then monitors the current behaviors of system according to these specifications and any mismatch is reported as an attack.

3. ARCHITECTURES FOR IDS IN MANET

The network infrastructure of MANET can be either flat or multi-layer. Therefore, the optimal IDS architecture for a MANET may depend on the network infrastructure. There are mainly four IDS architectures for MANET [8] as follows:

- In the stand-alone architecture, IDS runs on each node independently to determine intrusions. In this architecture, there is no cooperation among nodes so no data is exchanged. This architecture suits better for flat network infrastructure than multi-layered network infrastructure.
- The distributed and cooperative architecture also have an IDS agent at each node. The local events and data are collected locally by an IDS agent to identify possible intrusions and to initiate a response independently. However, neighboring IDS agents also cooperate in global intrusion detection when the evidence on a single node is not conclusive. This architecture is also more suitable for flat network infrastructure.
- The hierarchical architecture is an extended version of distributed and cooperative architecture and has been proposed for multi-layered network infrastructures in which the network is divided into clusters. Here also, IDS agent runs on every node and is responsible locally for its node while the cluster-head is responsible locally for its node as well as globally for its cluster.
- IDS architecture with mobile agent uses mobile agents that are able to move through the large network. Each mobile agent is assigned to perform a specific task and then one or more agents are distributed into each node in the network. This architecture allows the distribution of the intrusion detection tasks.

4. INTRUSION DETECTION TECHNIQUES IN MANET

In mobile ad hoc networks, nodes rely on each other for routing and forwarding packets to the destination. If an intermediate node is malicious then it may drop or modify the packets and thus only a few misbehaving nodes can degrade the performance of the entire system. There are several proposed techniques and protocols to detect such misbehavior, some of them are discussed here:

4.1 Watchdog and Pathrater

WATCHDOG AND PATHRATER was proposed by Marti, Giuli, and Baker [9] and the standard was Dynamic source routing protocol (DSR). A watchdog identifies the misbehaving nodes by copying the packets to be forwarded into a buffer and then promiscuously snoops on the transmission of the next hop. If the packets that are snooped differ from the observing node's buffer then the node responsible for forwarding the packet is noted as being suspicious. When violations become greater than some predetermined threshold, the violating node is marked as malicious. This information is then passed to the pathrater for path rating evaluation. Pathrater works on an individual node and maintains a "path metric" for each path. It then rates all of the known nodes in the network on the basis of their reliabilities, which is collected from the past experiences. After obtaining the path metric, the pathrater can choose the path with the highest metric.

4.2 Confidant

Buchegger and LeBoudec proposed CONFIDANT (**C**ooperation **O**f **N**odes, **F**airness **I**n **D**ynamic **A**d-ho **N**e**T**works) [10]. It is an extension to DSR protocol and very much similar to Watchdog and Pathrater. It has four components, which are Monitor, Trust Manager, Reputation System, and Path Manager. Initially, monitor keeps a "neighborhood watch" within its radio range to detect the malicious behavior like a watchdog. If a malicious activity is detected, the monitor immediately reports to the reputation system. After several checks, the reputation system updates the rating of the reported node. If the rating becomes unacceptable, the path manager is informed which then removes all the paths containing the malicious node. An ALARM message is also generated by the trust manager to warn all the friend nodes (which are decided on the basis of trusted relationships). On receiving the ALARM message, all ALARM messages of the reported node are combined to see if there is enough evidence to report it as malicious. In CONFIDANT, nodes are also punished by not including them in routing and packet forwarding.

4.3 CORE

Michiardi and Molva presented a technique CORE (**CO**llaborative **RE**putation) [11] to detect and isolate selfish nodes. This technique also forces the selfish nodes to cooperate. Selfish nodes are those which do not intentionally misbehave but may behave in a selfish manner when it finds that battery condition is poor or just to save its battery even when it has enough power. This technique uses a watchdog and a reputation system. Watchdog works in the same way as in previous two schemes. The difference is that, in it the reputation system rates the nodes on the basis of their participation in the network. Each node may participate in different activities at different time like routing discovery or packet forwarding that has different level of effects on the network; e.g., packet forwarding has more effect on the performance of the network than routing discovery. Reputation system maintains several reputation tables, one for each function and one for accumulated values of each node. Hence, if a request comes from a node with bad reputation then that node will be rejected and not be able to use the network anymore.

4.4 OCEAN

OCEAN (**O**bservation-based **C**ooperation **E**nforcement in **A**d hoc **N**etworks) is an extension to the DSR protocol and was proposed by Bansal and Baker [12]. It is also based on the monitoring and reputation system. However, it only relies on its own observation for judging the other nodes. Therefore, OCEAN is considered as a stand-alone architecture. It categorizes the node misbehavior into two types: misleading and selfish. The node that participates in the route discovery but does not forward the packets is considered as misleading while the node that does not even participate in the route discovery is considered as selfish. The detection of misleading nodes is done by buffering the packet checksum into the node that forwards the packet and monitors the neighbor to know whether it forwards the packet or not within a given time. Based on this the rating is done and if it falls below the faulty

threshold, the neighbor is added to a faulty list and all the traffic from that neighbor are rejected. This scheme uses the faulty timeout which is used to allow the faulty node to join the network again in case that it might be false accused or it behaves better. To mitigate the selfish behavior, it uses chipcounts. A neighbor node earns chips if it forwards a packet otherwise it loses chips. If the chipcount becomes below the threshold, packets coming from neighbor will be denied.

4.5 Cooperative IDS

Cooperative Intrusion Detection System is a cluster-based approach presented by Huang and Lee [13]. In this, an IDS is able to detect an intrusion as well as to identify the attack type and attacker through statistical anomaly detection. Various types of statistics [14] like the basic view of network topology, routing operations and traffic patterns are evaluated. If the statistics deviates from the pre-computed ones then the attacks could be identified. There is a set of predefined identification rules for known attacks. Once an anomaly is detected, the IDS perform further investigation with the help of these identification rules for detailed information of the attack. These rules help the system to identify the type of the attack and also the attacking node sometimes.

4.6 Ex Watchdog

Nasser and Chen proposed an intrusion detection system called ExWatchdog [15], an extension of the watchdog. This technique was proposed to overcome the problem of false misbehavior that is one of the big weaknesses in watchdog. In false misbehavior, a malicious node falsely reports other nodes as misbehaving while actually it is the real offender. This can cause the serious impact on network performance. In this scheme, each node maintains a table that contains the entry <source, destination, sum, path>. When an intermediate node on the path reports to the source that its next hop is malicious, the source will not decrease the rating of the reported node immediately. Instead it will send a message <source, destination, sum, malicious_node_address> to the destination using an alternate path either by finding it in the route table or by launching a route discovery. The destination node on receiving the message will check if the sum field of the message sent and that of its table are equal. If they are equal then the node that is reporting other nodes as misbehaving will be declared as malicious. Otherwise, the node that is being reported malicious is actually malicious.

5. CONCLUSION AND FUTURE WORK

As the use of mobile ad hoc networks has increased widely, the security in MANETs has been considered of paramount importance. The prevention techniques alone, i.e., cryptography and authentication are not sufficient; therefore the intrusion detection systems came into limelight. An intrusion detection system aims to detect malicious nodes into the network. Although the basic idea behind all of the above discussed IDSs is the watchdog. However watchdog is considered as the most effective technique but it has several limitations. It has been noticed that watchdog cannot work properly in the presence of collisions, limited transmission power, false misbehavior, collusion and partial dropping. Hence in order to cope up with these limitations, other techniques improve it and solve some of the problems that were faced with watchdog. In this context, comparison between the discussed intrusion detection techniques is shown in Table 1. However, IDS system itself may be attacked by the attackers [9] and the study of the defense to such attacks should also be explored. In this survey paper, the brief introduction of various available intrusion detection techniques is presented. It has been noticed that there is also a need of supporting activities that can able intrusion detection system to adapt dynamic network conditions. These activities include detecting all types of attacks in MANET; collecting and correlating intrusion events; responding to intrusion; and managing intrusion detection and all related function to cater for a secure communication [16].

Table 1: Comparison among IDSs

ID Techniques		Watchdog/ Pathrater	CONFIDANT	CORE	ExWatchdog	OCEAN	Cooperative IDS
Architecture		Distributed and Cooperative				Stand-alone	Hierarchical
Type of Data Collection		Reputation					Statistics
Observation	Self to neighbor	Yes	Yes	Yes	Yes	Yes	Yes
	Neighbor to neighbor	No	Yes	No	No	Yes	Yes
Misbehavior Detection	Selfish -routing	No	Yes	Yes	No	Yes	Yes
	Selfish-packet forwarding	Yes	Yes	Yes	Yes	Yes	Yes
	Malicious-routing	No	Yes	No	Yes	No	Yes
	Malicious-packet forwarding	Yes	Yes	No	Yes	No	Yes
Punishment		No	Yes	Yes	No	Yes	n/a

6. REFERENCES

[1] A. Mishra and K. M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book "The Handbook of Ad Hoc Wireless Networks (Chapter 30)", CRC Press LLC, 2003.

[2] 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, 2003.

[3] M. G. Zapata, "Secure Ad Hoc On-demand Distance Vector (SAODV) Routing", ACM Mobile Computing and Communication Review (MC2R), Vol. 6, No. 3, pp. 106-107, 2002.

[4] Y. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", Proceedings of the 4th IEEE Workshop On Mobile Computing Systems And Applications (WMCSA'02), pp. 3-13, 2002.

[5] Y. Hu, A. Perrig and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol For Ad Hoc Networks, "Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (Mobicom'02), pp. 12-23, 2002.

[6] A. Perrig, R. Canetti, D. Tygar, and D.Song, "The TESLA Broadcast Authentication Protocol," RSA CryptoBytes, 5 (summer), 2002.

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

[8] T. Anantvalee and J. Wu, " A survey on Intrusion Detection in Mobile ad Hoc Networks", Book Series Wireless Network Security, Springer, pp. 170-196, ISBN: 978-0-387-28040-0, 2006.

[9] S.Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proceedings of the 6th Annual International Conference on Mobile Computing And Networking (Mobicom'00), pp. 255-265, 2000.

[10] S. Buchegger and J. Le Boudec, "Performance Analysis of the CONFIDANT protocol (Cooperation of Nodes-Fairness In Dynamic Ad Hoc networks)", Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02), pp. 226-336, 2002.

[11] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc networks", Communication and Multimedia Security Conference (CMS'02), 2002.

[12] S. Bansal and M. Baker, "Observation-Based Cooperation Enforcement in Ad hoc Networks", Research Report cs. NI/0307012, Stanford University, 2003.

[13] Y. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks", Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN'03), pp. 135-147, 2003.

[14] Y. Huang, W. Fan, W. Lee, and P. Yu, "Cross-Feature Analysis for Detecting Ad Hoc routing Anomalies", Proceedings of the 23rd IEEE International Conference on Distributed Computing Systems (ICDCS'03), 2003.

[15] N. Nasser and Y. Chen, "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad Hoc Networks", Proceedings of the ICC, 2007.

[16] S. Sahu and S.K. Shandilya, "A Comprehensive Survey on Intrusion Detection in MANET", International Journal of Information Technology and Knowledge Management, Vol. 2, No. 2, pp. 305-310, 2010.