Intrusion Detection in Mobile Ad-hoc Networks: A Survey

Parth Bhatiya

P.G Student, L.D.R.P College of Engineering, Gandhinagar
parthbhatiya@ymail.com

ABSTRACT

With the progression of computer networks extending boundaries, Mobile ad hoc network (MANET) has more easy technology to provide anywhere, anytime communication. Due to its deployment nature, MANETs are easier to malicious attack. The absolute security in the mobile ad hoc network is very hard to achieve because of its fundamental characteristics, such as dynamic topology, open medium, limited power and limited bandwidth. The Prevention methods like authentication techniques and cryptography techniques and algorithms alone are not able to provide the security to these types of networks. so, efficient intrusion detection must be made to facilitate the identification and isolation of attacks. In this paper, we have surveyed several techniques for intrusion detection in MANET

1. Introduction

In MANET, a set of interacting nodes should cooperatively implement routing functions to enable end-to-end communication along dynamic paths composed by multi-hop wireless links. Several multi-hop routing protocols have been proposed for MANET, and most popular ones include: Dynamic Source Routing (DSR), Optimized Link-State Routing (OLSR), Destination-Sequenced Distance-Vector (DSDV) and Ad Hoc On-Demand Distance Vector (AODV). Most these protocols rely on the assumption of a trustworthy cooperation among all participating devices; unfortunately, this may not be a realistic assumption in real systems.

Malicious nodes could exploit the weakness of MANET to launch various kinds of attacks.

A mobile ad hoc network is comprised of mobile hosts that can communicate with each other using wireless links. Some scenarios where an ad hoc network can be used are business associates sharing information during a meeting, emergency disaster relief personnel coordinating efforts after a natural disaster such as a hurricane, earthquake, or flooding, and military personnel relaying tactical and other types of information in a battlefield. In this environment a route between two hosts may consist of hops through one or more nodes in the MANET. An important problem in a mobile ad hoc network is finding and maintaining routes since host mobility can cause topology changes. Node mobility on MANET cannot be restricted. As results, many IDS solutions have been proposed for wired network, which they are defined on strategic points such as switches, gateways, and routers, can not be implemented on the MANET. *Thus, the wired network IDS characteristics must be modified prior to be implemented in the MANET.*

Data communication in a MANET differs from that of wired networks in different aspects. The bandwidth availability and computing resources (e.g., hardware and battery power) are restricted in mobile ad hoc networks. Algorithms and protocols need to save both bandwidth and energy and must take into account the low capacity and limited processing power of wireless devices. An important challenge in the design of algorithms for a mobile ad hoc network is the fact that its topology is dynamic. Since the nodes are mobile, the network topology may change rapidly and unexpectedly, thereby affecting the availability of routing paths. Figure 1 depicts a snapshot of a MANET topology.

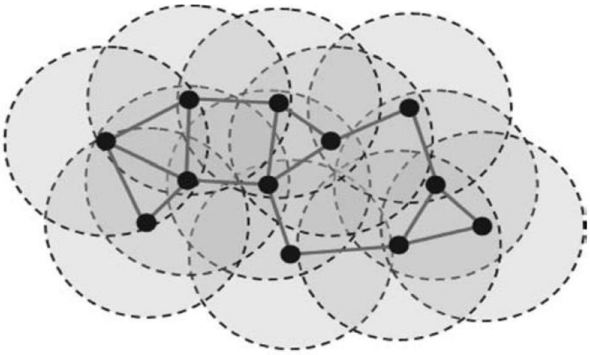

Fig. 1 MANET Topology

Given all theses differences, the design of algorithms for ad hoc networks are more complex than their wired counterpart.

2. Attacks on MANET

There are various types of attacks on mobile ad hoc network which are described as follow:

(1) Wormhole

A malicious node can eavesdrop or receive data packets at a point and transfer them to another malicious node, which is at another part of the network, through an out-of-band channel. The second malicious node then replays the packets. This makes all the nodes that can hear the transmissions by the second malicious node believe that the node that sent the packets to the first malicious node is their single-hop neighbour and they are receiving the packets directly from it.

(2) Denial of Service

Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network. Specific instance of denial of service attacks is the routing table overflow.

(3) Distributed Denial of Service

A DDoS attack is a form of DoS attack but difference is that DoS attack is performed by only one node and DDoS is performed by the combination of many nodes. All nodes simultaneously attack on the victim node or network by sending them huge packets, this will totally consume the victim bandwidth and this will not allow victim to receive the important data from the network.

(4) Black hole

In a black hole attack, a malicious mode attracts traffic from various nodes by advertising that it has a shortest path to a destination. Malicious node does not forward the packets but drop all the packets.

(5) Replay

A replay attack is performed when attacker listening the conversation or transaction between two nodes and put important massage like password or authentication message from conversation and use this in future to make attack on the legitimate user pretending as real sender.

3. IDS Background

An intrusion-detection system (IDS) can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. Intrusion detection is typically one part of an overall protection system that is installed around a system or device—it is not a stand-alone protection measure. Depending on the detection techniques used, IDS can be classified into three main categories as follows:

(1) Anomaly detection systems

The normal profiles (or normal behaviors) of users are kept in the system. The system compares the captured data

With these profiles, and then treats any activity that deviates from the baseline as a possible intrusion by informing system administrators or initializing a proper response.

(2) Misuse detection systems

The system keeps patterns (or signatures) of known attacks and uses them to compare with the captured data. Any matched pattern is treated as an intrusion. Like a virus detection system, it cannot detect new kinds of attacks.

(3) Specification-based detection

The system defines a set of constraints that describe the correct operation of a program or protocol. Then, it monitors the execution of the program with respect to the defined constraints.

4. Unique IDS Challenges in MANET

Defending MANET networks is much more challenging than defending traditional enterprise networks for a variety of reasons. Characteristics such as volatility, mobility, as well as the ease of listening to wireless transmissions make the network inherently less secure. Existing tools usually assume a well-structured and static network and therefore can not be used as they are.

The nature of MANET networks makes it easier for malicious users to disrupt the network because by definition MANETs are flexible and lack a fixed infrastructure. When securing the network we cannot assume that the threat is mostly from outside the network. Therefore, the network needs to be protected from all nodes, both external and internal. Another unique challenge of MANET is the limited bandwidth.

In a MANET, nodes tend to move a lot and therefore the connectivity of nodes changes dramatically. MANET networks are also much more dynamic and unpredictable because connectivity depends on the movements of nodes, terrain, changes in the mission (e.g. for a military application or a first responder application), node failures, weather, and other factors. As a result, it is difficult to accurately characterize normal behavior. Hence, it is often difficult to distinguish malicious behavior from normal.

Unlike in wire line networks, nodes in an ad hoc network have limited energy. Hence, often only computationally simple, energy-efficient detection strategies can be used by such nodes. The detection algorithms must also be distributed as communication with a central computing unit will consume significant energy and bandwidth.

5. Related Work

Since the IDS for traditional wired systems are not well-suited to MANETs, many researchers have proposed several IDS especially for MANETs.

5.1 Distributed and Cooperative IDS

Zhang and Lee proposed [1] the model for distributed and cooperative IDS as shown in figure 3. The model for an IDS agent is structured into six modules. The *local data collection* module collects real-time audit data, which includes system and user activities within its radio range. This collected data will be analyzed by the *local detection engine* module for evidence of anomalies. If an anomaly is detected with strong evidence, the IDS agent can determine independently that the system is under attack and initiate a response through the *local response* module (i.e., alerting the local user) or the *global response* module (i.e., deciding on an action), depending on the type of intrusion, the type of network protocols and applications, and the certainty of the evidence. If an anomaly is detected with weak or inconclusive evidence, the IDS agent can request the cooperation of neighboring IDS agents through a *cooperative detection engine* module, which communicates to other agents through a *secure communication* module.

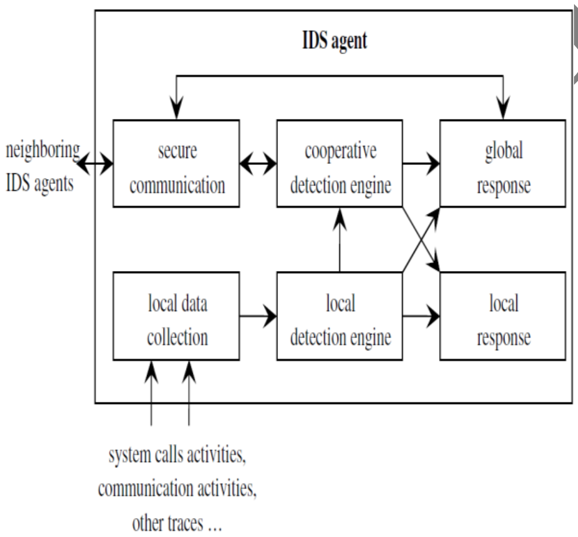

Fig. 2 A Model for an IDS Agent

5.2 Local Intrusion Detection System (LIDS)

Albers *et al.* [2] proposed a distributed and collaborative architecture of IDS by using mobile agents. A Local Intrusion Detection System (LIDS) is implemented on every node for local concern, which can be extended for global concern by cooperating with other LIDS.

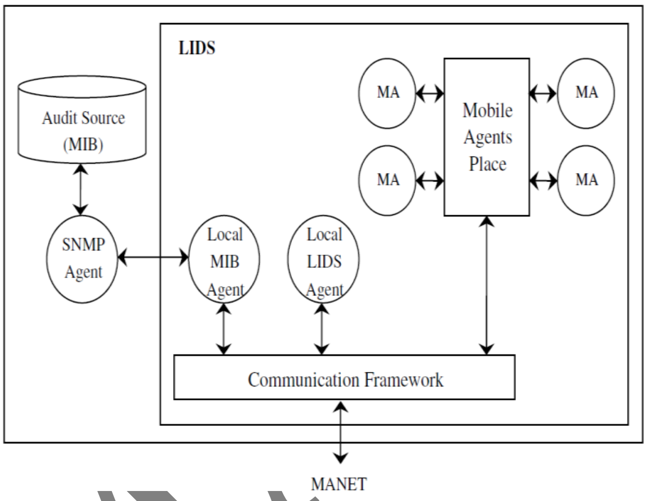

Fig. 3 LIDS architecture in a mobile node

The LIDS architecture is shown in Figure 3. Communication framework facilitate for both internal and external communication with a LIDS. Local LIDS agent is responsible for local intrusion detection and local response. Local MIB agent provides a means of collecting MIB variables for either mobile agents or the Local LIDS Agent. Mobile agents are distributed from its LID to collect and process data on other nodes. Mobile agents place is used to provide a security control to mobile agents.

5.3 Distributed Intrusion Detection System Using Multiple Sensors

Kachirski and Guha [3] proposed a multi-sensor intrusion detection system based on mobile agent technology. The system can be divided into three main modules, each of which represents a mobile agent with certain functionality: monitoring, decision making or initiating a response.

The network is logically divided into clusters with a single cluster head for each cluster. This cluster head will monitor the packets within the cluster and only packets whose originators are in the same cluster are captured and investigated. This means that the network monitoring agent (with network monitoring sensor) and the decision agent are run on the cluster head. In this mechanism, the decision agent performs the decision-making based on its own collected information from its network-monitoring sensor; thus, other nodes have no influence on its decision. This way, spoofing attacks and false accusations can be prevented.

5.4 Dynamic Hierarchical Intrusion Detection Architecture

Since nodes move arbitrarily across the network, a static hierarchy is not suitable for such dynamic network topology. Sterne *et al*. [4] proposed a dynamic intrusion detection hierarchy that is potentially scalable to large networks However; it can be structured in more than two levels: the first level cluster heads and the second level cluster heads and so on. Members of the first level of the cluster are called leaf nodes.

Every node has the responsibilities of monitoring logging, analyzing (i.e., attack signature matching or checking on packet headers and payloads), responding to intrusions detected if there is enough evidence, and alerting or reporting to cluster heads.

Cluster heads aggregate and correlate reports from members of the cluster and data of their own. Besides, cluster heads may send the requests to their children for additional information in order to correlate reports correctly. The uppermost levels of the hierarchy have the authority and responsibility for managing the detection and response capabilities of the clusters and cluster heads below them. They may send the signatures update, or directives and policies to alter the configurations for intrusion detection and response. These update and directives will flow from the top of the hierarchy to the bottom.

5.5 IDS based on Finite State Machine

Tseng *et al*. [5] proposed a solution using specification based technique to detect attacks on AODV. Specification based monitoring capture the correct behavior by comparing the behavior of objects with their associated security specifications. Thus, intrusions which cause incorrect behavior can be detected without exact knowledge about them. The proposed approach uses finite state machines for describing the valid flow of AODV routing behavior. Violations in the specifications are detected by the distributed network monitors. The IDS is built on the monitoring architecture that traces AODV request-reply flow.

5.6 IDS based on State Transition Analysis

The proposed method [6] is based on the State Transition Analysis Technique (STAT). AODVSTAT sensors are deployed either on stand alone or distributed basis on a subset of the nodes of the network. The sensors perform real-time stateful analysis on the packet stream to detect signs of intrusions.

5.7 IDS for AODV based network

Viswanatham and Chari [7] proposed using My-AODV agent for detecting and analyzing various attacks on MANET. The My-AODV agent is utilized to introduce various attacks against the network. The proposed system works in two levels, it initially detects nodes which drop data packets, divert routes or consume extra resources. After detection, the recovery process is started where the malicious node is isolated from the network.

6. Conclusion

Most of the MANET IDSes tend to have the distributed architectures and their variants. The IDS architecture may depend on the network infrastructure and networks techniques. We need to search for new architecture and mechanisms to protect the mobile ad hoc networks. 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. Accordingly, the study of the defense to such attacks should be explored as well.

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] P. Albers, O. Camp, J. Percher, B. Jouga, L. M・ and R. Puttini, “Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches,” *Proceedings of the 1st International Workshop on Wireless Information Systems (WIS-2002)*, pp. 1-12, April 2002.

[3] O. Kachirski and R. Guha, “Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks,” *Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS’03)*, p. 57.1, January 2003.

[4] D. Sterne, P. Balasubramanyam, D. Carman, B.Wilson, R. Talpade, C. Ko, R. Balupari, C.-Y. Tseng, T. Bowen, K. Levitt, and J. Rowe, “AGeneral Cooperative Intrusion Detection Architecture for MANETs,” *Proceedings of the 3rd IEEE International Workshop on Information Assurance (IWIA’05)*, pp. 57-70, March 2005.

[5] Tseng, C.Y., P. Balasubramanyam, C. Ko, R. Limprasittiporn and J. Rowe *et al.*, 2003. A specification-based intrusion detection system for AODV. Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, Oct. 27- 30, ACM Press, Washington, DC, USA., pp: 125- 134. DOI: 10.1145/986858.986876

[6] Vigna, G., S. Gwalani, K. Srinivasan, E.M. Belding-Royer and R.A. Kemmerer, 2004. An intrusion detection tool for AODV-based ad hoc wireless networks. Proceedings of the 20th Annual Computer Security Applications Conference, Dec. 6-10, IEEE Xplore Press, pp: 16-27. DOI: 10.1109/CSAC.2004.6

[7] Viswanatham, V.M. and A.A. Chari, 2008. An approach for detecting attacks in mobile adhoc networks. J. Comput. Sci., 4: 245-251. DOI: 10.3844/jcssp.2008.245.251