INTRUSION DETECTION METHODS IN MOBILE AD-HOC NETWORKS

K. K. Singh

ABSTRACT

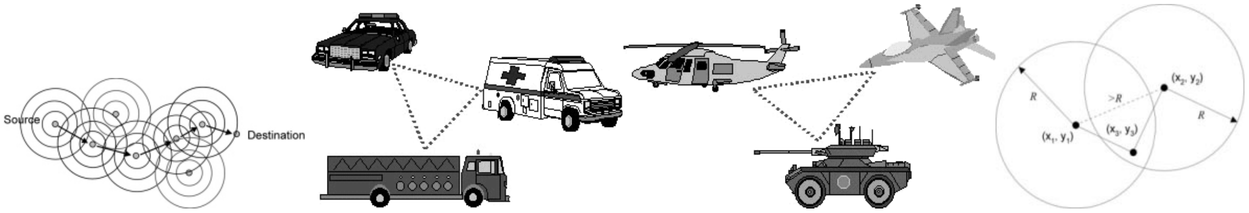
Instruction detection in MANETs is a challenging task because these networks dynamically change their topologies; lack concentration points where aggregated traffic can be analyzed; utilize infrastructure less protocols that are susceptible to manipulation; and rely on noisy, intermittent wireless communications. Due to infrastructure less network secure communication and maintaining the connectivity in the presence of adversaries is major issue; therefore, identify the attack types and selecting an efficient intrusion detection methods are especially important for MANET applications. The purpose of this paper is to guidelines on selecting intrusion detection methods in MANET. To clearly describe the intrusion detection methods in ad-hoc networks, I attempt to present an approach, with which some existing intrusion detection techniques can be integrated and more advanced intrusion detection techniques can be developed that can be adopted to wireless ad-hoc networks.

1. INTRODUCTION

In recent years, considerable interest has developed in creating new kinds of network applications that fully exploit distributed mobile computing, particularly for military uses. The key underlying technology for such applications is mobile ad hoc network (MANET) technology. Flexibility and adaptability, which are the strengths of MANETs, are unfortunately accompanied in MANETs by increased security risks. This is because radio-based mobile communications among the components of distributed applications, and the infrastructure protocols that enable these communications, are exposed new threats, yet must remain available continuously, even in harsh environments. Intrusion detection technology will undoubtedly be a crucial ingredient in any comprehensive security solution to address these threats.

Ad-hoc networks are a new paradigm of wireless communication for mobile host as shown in figure 1.1. An ad-hoc network is a collection of wireless mobile nodes,

Figure 1.1 Wireless communication systems



* *Senior Lecturer, Department of Information Technology, Delhi Business School, New Delhi.*

dynamically forming a network without any infrastructure. Security in mobile ad-hoc networks is a hard to achieve due to dynamically changing and fully decentralized topology as well as the vulnerabilities and limitations of wireless data transmissions. Existing solutions that are applied in wired networks can be used to obtain a certain level of security. These solutions are not always be suitable to wireless networks. Therefore ad-hoc networks have their own vulnerabilities that cannot be always tackled by these wired network security solutions.

Once of the main challenges that ad-hoc networking faces is related to the use of wireless links. Due to the use of wireless medium an ad-hoc network is vulnerable to link attacks ranking from passive eavesdropping to active impersonation, message replay and message corruption. An adversary can easily eavesdrop network traffic by placing a wireless enabled device within the range of the ad-hoc network and capture routing and application packets. By eavesdropping the malicious node can gain access to secret information and violate the confidentially requirement. Passive attacks like eavesdropping are very hard to detect since they do not present any significant pattern or impact in the performance of the network. Active attacks may allow a malicious node to delete or inject to the network traffic erroneous messages, modify messages and impersonate as another node, hence violating availability, integrity, authentication and non-repudiation. As opposed to passive attacks, active attacks can be detected and limited with the utilization of various schemes.

2. MANET

In 1996, the Internet Engineering Task Force (IETF) set down a MANET workgroup and its goal is to standardize IP routing protocol functionality suitable for wireless routing applications within both static and dynamic topologies.

A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways and interface with a fixed network. Its nodes are equipped with wireless transmitters/ receivers using antennas which may be omni-directional (broadcast), highly-directional (point-to-point), or some combination thereof. At a given time, the system can be viewed as a random graph due to the movement of the nodes, their transmitters/ receiver coverage patterns, the transmission power levels, and the co-channel interference levels. The network topology may change with time as the nodes move or adjust their transmission and reception parameters. The characteristics of MANET are identified as follows (Rafique, 2002; Albers and Camp, 2003; Smith, 2001):

- Autonomous terminal: Each node in MANET is autonomous and is both router and host.
- Distributed: MANET is distributed in its operation and functionalities, such as routing, host configuration and security. For instance, unlike wired network, MANET can not have a centralized firewall (Albers and Camp, 2003).
- Multi-hop routing: If the source and destination of a message is out of the radio range of one node, a multi-hop routing is necessary.
- Dynamic network topology: Nodes are mobile and can join or leave the network at any time; therefore, the topology is dynamic.
- Fluctuating link bandwidth: The stability, capacity and reliability of wireless link is always inferior to wired links.

- Thin terminal: The mobile nodes are often light weight, with less powerful CPU, memory and power.
- Spontaneous and mobile: minimum intervention is needed in configuration of the network. The routing protocol should be an adapted one that allows users to communicate in the network. It should also support security.

4. INTRUSION DETECTION SYSTEM IN MANET

Intrusion is defined as "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource".

Mobile ad hoc networks (MANETs) present a number of unique problems for Intrusion Detection Systems (IDS). Network traffic can be monitored on a wired network segment, but ad hoc nodes can only monitor network traffic within their observable radio transmission range. A wired network under a single administrative domain allows for discovery, repair, response, and forensics of suspicious nodes. A MANET is most likely not under a single administrative domain, making it difficult to perform any kind of centralized management or control. In an ad hoc network, malicious nodes may enter and leave the immediate radio transmission range at random intervals, may collude with other malicious nodes to disrupt network activity and avoid detection, or behave maliciously only intermittently, further complicating their detection. A node that sends out false routing information could be a compromised node, or merely a node that has a temporarily stale routing table due to volatile physical conditions. Packets may be dropped due to network congestion or because a malicious node is not faithfully executing a routing algorithm.

The usage of intrusion prevention techniques is more limited in their effect. For instance, we can use encryption or user authentication to implement defense. However, in wireless network, it is very possible that some nodes, such as a hand held device get stolen and compromised, which rarely happens in wired network. And such nodes have private key on them. This will void the encryption defense.

The intrusion detection technique is basically independent from the architecture or environment. In other words, anomaly and misuse detection can be utilized in wireless environment just as they are in wired network. The difference in implementation is mainly on what audit data to take as input to the algorithm. However, most IDS in MANET utilize anomaly detection because of the special nature of MANET. An IDS contains an audit data collection agent, which keep track of the activities within the system, a detector which analyzes the audit data and issues an output report to the site security officer (Axelsson, 2000).

Intrusion detection system serves as an alarm mechanism for a computer system. It detects the security comprises happened to a computer system and then issues an alarm message to an entity, such as a site security officer so that the entity can take some actions against the intrusion (Axelsson, 2000;Greg, 2004).

5. ATTACKS IN MANET

The attacks in MANET can roughly be classified into two major categories, namely passive attacks and active attacks, according to the attack means. Passive attacks obtain data exchange in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a

MANET. Table 1.1 shows the general taxonomy of security attacks against MANET. Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay.

The attacks can also be classified into two categories, namely external attacks and internal attacks, according the domain of the attacks. Some papers refer to outsider and insider attacks. External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attack since the insider knows valuable and secret information, and possesses privileged access rights.

Attacks can also be classified according to the network protocol stacks. Table 1.2 shows an example of a classification of security attacks based on protocol stack; some attacks could be launched at multiple layers. Some security attacks use stealth, whereby the attackers try to hide their actions from either an individual who is monitoring the system or an intrusion detection system (IDS). But other attacks such as DoS cannot be made still. Some attacks are non-cryptography related, and others are cryptography primitive attacks. Table 1.3 shows cryptography primitive attacks and some examples.

Table 1.1: Security Attacks Classification

Passive Attacks	Eavesdropping, traffic analysis, monitoring
Active Attacks	Jamming, spoofing, modification, replaying, DoS

Table 1.2: Security Attacks on Protocol Stacks

Layer	**Attacks**
Application Layer	Repudiation, data corruption
Transport Layer	Session hijacking, SYN flooding
Network Layer	Warmhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks
Data Link Layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical Layer	Jamming, interceptions, eavesdropping
Multi-layer attacks	DoS, impersonation, replay, man-in-the-middle

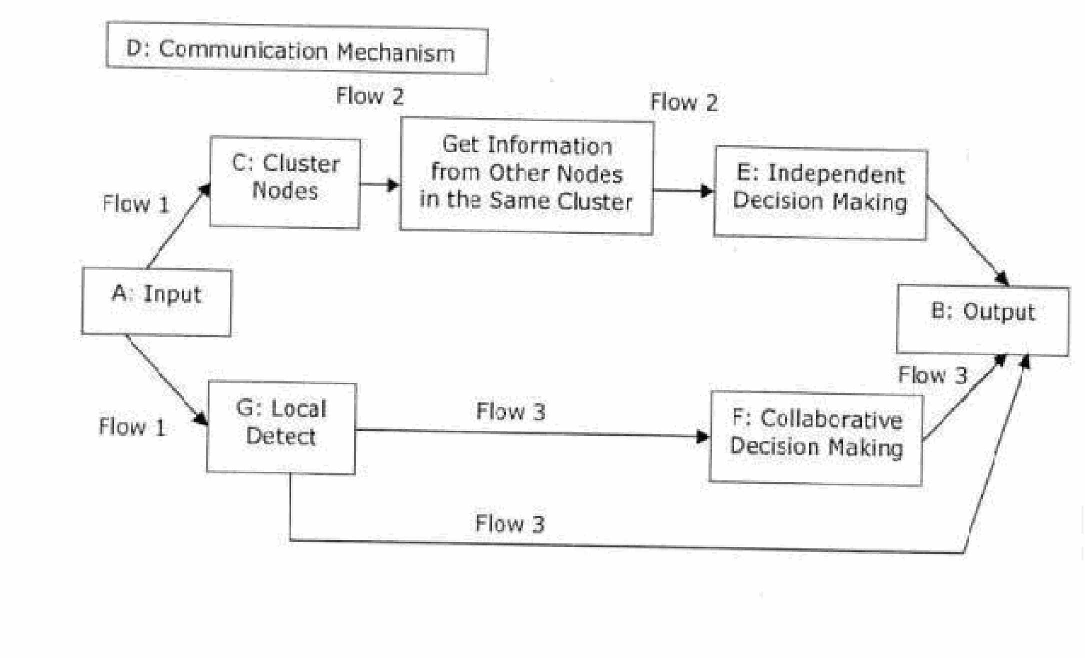
Table 1.3: Cryptography Primitive Attacks

Cryptography Primitive Attacks	**Examples**
Pseudorandom number attack	Nonce, timestamp, initialization vector (IV)
Digital signature attack	RSA signature, ElGamal signature, digital signature standard (DSS)
Hash collision attack	SHA-0, MD4, MD5, HAVAL-128, RIPEMD
Security handshake attacks	Diffie-Hellman key exchange protocol, Needham-Schroeder protocol

6. FRAMEWORK ON COMPARISON STUDY

Figure 1.2 illustrated a framework developed in the current research for the comparison study on intrusion detection in MANET. There are mainly three flows and seven components. The detailed descriptions for each of these flows and components are presented in the following.

Figure 1.2 Framework of Comparison Study on Intrusion Detections in MANET


D: Communication Mechanism
Flow 2
Flow 2
C: Cluster Nodes
Get Information from Other Nodes in the Same Cluster
E: Independent Decision Making
Flow 1
A: Input
B: Output
Flow 3
Flow 1
G: Local Detect
Flow 3
F: Collaborative Decision Making
Flow 3

Proc ISECON 2004, v21 (Newport): §3233 (refereed) © 2004 EDSIG, page 7

Input : The data to be collected by the IDS. It mainly includes system audit data, network packet or statistics of such data, for instance the statistics of updates in routing table.

Cluster nodes : certain algorithms are run on the network so that the network be partitioned into a number of clusters. A cluster usually has a node as the cluster head. The network partition and cluster head selection is dynamic.

Local detect : The IDS module or agent on a single node run intrusion detection algorithm to determine whether intrusion happens on the local node.

Get information from other nodes : This usually happens on cluster head. Because of the distributed and ad hoc nature of MANET, the local information on a single node is often insufficient for detection decision making. Therefore, the IDS need to collect information from other nodes rather than the node it resides in to make accurate detection.

Independent detection decision making: The IDS on the cluster head make intrusion decision with all the information it acquires.

Collaborative detection decision making : Several nodes participate in a collaborative decision making process, for instance a voting to make the intrusion decision. Usually, before the voting, each of the participating nodes already makes an initial decision. They need to aggregate the initial decisions to make a more accurate group decision.

Flow 1 : First input is collected for IDS. Then, some IDS group network nodes into clusters or zones and other IDS do not group nodes.

Flow 2 : In IDS with clusters, the member nodes in the cluster usually pass some local security information to the cluster head. Then cluster head makes intrusion decision independently on the basis of the information collected.

Flow 3 : In IDS without cluster, there are two ways of detection decision making. One is that the IDS module on one node makes decision directly and issue intrusion alarm. However, this is rarely used in MANET, since local information is often insufficient for making intrusion decisions. Another way is the collaborative decision making.

7. INTRUSION DETECTION METHODS IN MANET

The intrusion detection techniques can be categorized into ***misuse detection*** and ***anomaly detection.*** The misuse detection uses patterns of well-known attacks to match and identify known intrusions. This technique can accurately and effectively detect instances of known attacks. However this technique is unable to detect newly invented attacks. In ad hoc networking due to its dynamic nature it is difficult, but not impossible to define traffic patterns that indicate and attack. The anomaly detection technique observes activities and network traffic that significantly deviates from the established normal usage and identifies intrusions. Thus, after the normal behavior of the network traffic has been established this technique does not require any prior knowledge of the attack, and for the reason it can detect newly invented attacks. Other intrusion detection techniques process partial data & local data on the host as well as gather information from neighboring hosts to perform co-operative intrusion detection.

Appendix 1.1 illustrated the detailed comparison study on existing methods for intrusion detection for MANET based on inputs, process methods, outputs, advantages and disadvantages. The letters of A through G are related to the letters in Figure 1.1. In Appendix 1.1, the existing intrusion detection methods are presented.

Method 1 is efficient and bandwidth-conscious. It targets intrusion at multiple levels and fits the distributed nature of IDS for MANET. The method has clusters and the IDS on cluster head employs independent detection decision-making after gathering information from other nodes. It utilizes mobile agent for the communications among nodes.

Method 2 implements local and collaborative decision making in anomaly detection. In this approach, individual IDS agent works by itself and collaborate in decision making. Each IDS agent runs on a node and monitors local activities. If a node detects locally intrusion with strong evidence, then the node can conclude intrusion happens and then initiate an alarm response. However, if the evidence is not strong enough but needs investigation in a wider area in the network, then the IDS agent can start an collaborate procedure which is a distributed consensus algorithm (Zhang and Lee, 2003).

Method 3 the authors proposed a cluster-based scheme in which a cluster head is elected by a group of nodes in a neighborhood (citizen nodes) and the head node monitor the citizen nodes. Once the cluster head is elected, then other nodes need to transmit the features it obtains locally to the cluster head. This IDS uses anomaly detection implemented with data mining as its detection technique (Lee, 2002).

Method 4 each node runs a local IDS. Each node detects intrusion locally and use external data to confirm the detection. The nodes use mobile agents to communicate and collaborate.

Method 5 implements an IDS which use collaboration mechanism in anomaly detection. In this model, a network is divided into logical zones. Each zone has a gateway node and individual nodes. Individual nodes has IDS agent working and detect intrusion activities individually. Once an individual node detects intrusion, it generates an alert message. Gateway node aggregate and correlate the alerts generated by the nodes in its zone. An algorithm is used in aggregate the alerts based on the similarities in the attributes of the alert. Only gateway nodes can utilize alert to init alarm (Sun, Wu and Pooch, 2003).

Method 6 also utilize cluster and cluster head employs the independent decision making. It also utilizes the mobile agent for communications among nodes. The intrusion detection engine is a case-based agent designed with the principle of artificial intelligence.

Method 7 mainly introduces a detection algorithm which uses the statistics of packets, namely the relations between different features, such as the correlation between the number of packet dropped and the percentage of change in routing table. This algorithm can be used as an intrusion detection engine in other IDS architecture.

Method 8, the normal behavior of critical objects in the Network is constructed into normal specification first. Then the actual behavior is compared to the normal specification. It uses distributed network monitor to trace the request-reply flow in the routing protocol. The network monitor runs a specification based detection algorithm to make decisions (Sekar, 2002; and Okazaki, 2002).

Method 9, the two neighboring nodes of one node is used to ensure that the packets are not modified when traveling in the network. This is done by comparing the information in each packet at each hop. It has two modes: passive mode-to protect a single host and active mode-to collaboratively protect the nodes in a cluster. In active mode, a cluster head starts a voting algorithm to determine whether intrusion really happens.

Method 10, information in the management information base (MIB) is used as input data. It also uses mobile agent and a collaborative decision making mechanism.

8. CONCLUSIONS

The objective of the current research is to provide a big picture of the current state of the research on IDS in MANET, and provide a guideline on how to select intrusion detection methods for IDS in MANET. Specifically, this paper first surveyed the existing literatures about the IDS, the MANET and the IDS for MANET and discussed the requirement of IDS in MANET. It can also help the decision makers, such as security officer, who needs to select proper IDS for their MANET. The results of the current research are useful for educational and industrial professionals who are interested in information systems security in the wireless world.

REFERENCES

1. *D. Dharmalingam and V. Vetriselvi (August 31–Sept 1,2007) "Securing Data and Routing For Mobile Ad Hoc Network", Proceedings of National Conference on Information Technology, pp.19*
2. *Aparna K.S and Shivaprakash Vastrad (August 31–Sept 1,2007) "Intrusion Detection in Mobile Adhoc Networks", Proceedings of National Conference on Information Technology, pp. 221-222*
3. *Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/ Mobile Network Security, pp.2 (Chapter-12)*
4. *Alberts, Patrick and Olivier Camp, 2002, "Security in Ad hoc Networks: a general Intrusion detection acrchitecture enhancing trust based approaches", Proceedings of the First International Workshop on wireless Information Systems.*
5. *Yi Li and June Wei, "Guidelines on Selecting Intrusion Detection Methods in MANET", Proc ISECON 2004, v21 (Newport): 3233 (refereed) (c) 2004 EDSIG.*
6. *Zhang, Yongguan and Wenke Lee, 2003, "Intrusion detection techniques for mobile manet", ACM/ Kluwer Wireless Network Journal (ACM WINET), 9, 5, pp.545-556.*
7. *A. Patwardhan, J.Parker, A.Joshi, A. Karygiannis and M. Iorga, "Secure Routing and Intrusion Detection in Ad Hoc Networks", Third IEEE International Conference on Pervasive Computing and Communications 2005.*
8. *A. Karygiannis, E.Antonakakis, and A. Apostolopoulos, "Detecting Critical Nodes for MANET Intrusion Detection Systems", National Institute of Standards and Technology.*
9. *Y. Zhang and W. Lee, "Intrusion detection in wireless ad hoc networks", In Proceedings of the 6th annual international conference on mobile computing and networking, pp.275-283. ACM Press, 2000.*
10. *Y. Zhang, W. Lee and Y. Huang, "Intrusion detection techniques for mobile wireless networks", ACM/ Kluwer Mobile Netoworks and Applications (MONETS), 2002.*
11. *C-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, "A specification- based intrusion detection system for AODV", In Proceeding of the 1st ACM workshop on Security of ad hoc and sensor networks, pp.125-134, ACM Press, 2003.*