Malicious Behavior of Nodes in Mobile Ad-hoc Networks And Ways to Deal with them

Abdul Naeem Shaikh & Jitendra Kumawat
Amity School of Engineering & Technology, Amity University Rajasthan, India

ABSTRACT: *MANETs find their use particularly in the field where infrastructured network are not possible without having any centralized administration. Where this feature helps in rapidly deploying and establishing the ad Hoc networks, it makes it highly susceptible for attacks. Mobile ad-hoc networks (MANETs) rely on cooperation of all participating nodes. Any node under attack in ad hoc network exhibits an anomalous behavior called the malicious behavior. In this situation, the entire operation of a network gets disturbed and to preclude such malicious behavior several security solutions have been discovered. In this paper, malicious behavior of a node is defined and to defend such behavior, security solutions are presented which are used in furnishing a secure and reliable communication in ad hoc.*

Keywords*- Cryptography, intruder, malicious, Mobile ad hoc networks, mobile node, packet forwarding, routing protocols, vulnerability.*

I.INTRODUCTION

Mobile ad-hoc network is a collection of wireless mobile nodes that forms a temporary network without any centralized administration. In such a environment, it may be necessary for one node to enlist other hosts in forwarding a packet to its destination due to the limited transmission range of wireless network interfaces. Each mobile node operates not only as a host but also as a router forwarding packets for other mobile nodes in the network that may not be within the direct transmission range of each other. Each node participates in an ad-hoc routing protocol that allows it to discover multihop paths through the network to any other node. This idea of mobile ad-hoc network is also called infrastructure less networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly. Any malicious node in the network can disturb the whole processor can even stop it. Several attacks like blackhole, wormhole, rushing etc have been come into the picture under which a legitimate node behaves in a malicious manner. It is quite difficult to define and detect such behavior of a node. Therefore, it becomes mandatory to define the normal and malicious behavior of a node. Whenever a node exhibits a malicious behavior under any attack, it assures the breach of security principles like availability, integrity, confidentiality etc. An intruder takes advantage of the vulnerabilities presents in the ad hoc network and attacks the node which breaches the security principles.

II. NEED OF SECURITY IN AD HOC NETWORK

Though the ad hoc networks are widely used but still it has some vulnerability in it. Therefore, there is a need of security to defend such problems. An intruder utilizes this vulnerability to know about the network processes and then attack the network. Following are some present vulnerability in ad hoc networks:

Mobility- Each node in ad hoc network is movable. It can join or leave a network at any instant of time without informing any node. This gives chance to intruder to easily
enter in the network and even participating in its operations.

Open Wireless Medium- All the communication between nodes is taking place through the medium of air instead of wires. An intruder can easily access this medium to gain information about the communication or can easily trap it.

Resource Constraint- Every node in mobile ad hoc network has limited resources like battery, computational power, bandwidth etc. An intruder can unnecessarily waste these limited resources in order to make it unavailable to perform.

Broadcast Channel- In ad hoc network, the communication among nodes is broadcast in nature than point to point communication. It means

whenever a node transmits a request, it broadcast it to every surrounding node. Any malicious node can utilize that information in a wrong manner.

Dynamic Network Topology- As the nodes are highly movable in nature, so the topology changes every time the communication takes place. The packets from source to destination may take different path for communication. An intruder can introduce itself in any path.

Scalability- Ad hoc network may consist of number of nodes. This number is not fixed. In a network of its range, as many as number of nodes can take part. Intruder simply takes advantage of this parameter as there is no limitation on number of nodes.

Reliability- All the wireless communication is limited to a range of 100 meter which puts a constraint on nodes to be in range for establishing communication. Due to this limited range, some data errors are also generated. For attacking a particular node, an intruder needs to be in its range.

Quality of Service (QoS)- The processes which are taking place among nodes defines a factor called Quality of Service which means higher the QoS, higher will be the reliability on the network. An intruder can easily decrease the QoS parameter by disturbing the process.

III. DEFINING NORMAL AND MALICIOUS BEHAVIOR OF A NODE

The vulnerabilities discussed in previous section provide intruder a way to compromise legitimate nodes and make them malicious in nature. In this section, an attempt has been made to define a normal and malicious behavior of a node. First of all, normal behavior of a node is defined and then malicious behavior.

Normal Behavior- "When any operation is performed in an ad hoc network (for example-all the packets from source node to destination node is delivered) while maintaining the security principles (Confidentiality, Integrity, Availability, Authenticity and Non-Repudiation), then it is called the normal behavior of a node."

Malicious Behavior- "When a node breaches any of the security principles and is therefore under any attack. Such nodes exhibit one or more of the following behavior:

Packet Drop- Simply consumes or drops the packet and does not forward it.

Battery Drained- A malicious node can waste the battery by performing unnecessarily operations.

Buffer Overflow- A node under attack can fill the buffer with fake updates so that genuine updates cannot be stored further.

Bandwidth Consumption- Whenever a malicious node consumes the bandwidth so that no other legitimate node can use it.

Malicious Node Entering- A malicious node can enter in the network without authentication.

Stale Packets- This means to inject stale packets into the network to create confusion in the network.

Delay- Any malicious node can purposely delay the packet forward to it.

Link Break- This can result in restricting the two legitimate nodes from communicating if the malicious node is between them.

Message Tampering- A malicious node can tamper the content of the packets.

Denying from Sending Message- Any malicious node may deny from sending messages to other legitimate nodes.

Fake Routing- Whether there exists a path between nodes or not, a malicious node can send fake routes to the legitimate nodes in order to get the packets or to disturb the operations.

Node Not Available- An intruder can isolate the node from taking part in any operation so as to create delays when the source node chooses another alternative path.

Stealing Information- Information like the content, location, sequence number can be stolen by the malicious node to use it further for attack.

Session Capturing- When two legitimate nodes communicate, a malicious node can capture their session so as to take some meaningful information.

Others- There are other ways also in which a node behaves in a malicious manner.

IV. SECURITY SOLUTION TO DEFEND MALICIOUS BEHAVIOR

In order to defend the malicious behavior which is defined in previous section, there are several security solutions which are used in ad hoc networks. Security can be provided through the methods of Cryptography, Protocols, Intrusion Detection System (IDS) and Trusted Third Party (TTP) which are discussed below.

4.1 Security through Cryptography-

In Ad Hoc Network, the data is sent using cryptography. Cryptography means to convert (or encrypt) the original data (which is to be send) into the unreadable format. Even if the intruder accesses the data, it should not be able to understand the content of it. Cryptography can be symmetric (which uses same key to encrypt and decrypt the data) and asymmetric (which uses one key to encrypt and other to decrypt the data). This security preserves the integrity and confidentiality of data. Techniques like MD5 (Message Digest 5), Digital Signature, SHA (Secure Hash Algorithm), MAC (Message Authentication Codes) are used to preserve the security principles.

4.2 Security through TTP (Trusted Third Party)-

This service comes in picture when the security to the nodes in ad hoc network is provided by the some third party which can be trusted. A common example can be Public Key infrastructure (PKI) in which a trusted third party like Certifying Authority
(CA) issues a certificate to the legitimate nodes for authenticating them. This preserves authentication security principle. Another example can be a watchdog node which monitors all the nodes for availability. This node checks the packet forwarding from source node to intermediate node and then to destination node. A Random Walker Detector (RWD) also monitors the node's activity to check whether a node is under attack or not.

4.3 Security through IDS (Intrusion Detection Systems)-

Intrusion Detection System in ad hoc network monitors the node for malicious behavior. Anomaly based IDS is used in such process where any anomaly in the network confirms an attack. Profiles are maintained in the database of IDS which is the normal behavior of a node. These profiles are made under training period. Such profiles can either be static or dynamic in nature. IDS can be designed inside the node or can even work as TTP.

4.4 Security through Secure Protocols-

In recent research, many secure protocols have been proposed which are intended to provide security to the network. Protocols like SEAD (Secure Efficient Ad Hoc Distance Vector Routing Protocol), SAR (Secure-Aware Ad Hoc Routing protocol), ARAN (Authenticated Routing for Ad Hoc Networks), ES-AODV (Efficient Security Ad-Hoc On-Demand Distance Vector) are the example of secure protocols. These protocols are designed with the concept of certification system, cryptography and other security solutions.

4.5 Security through other methods-

Several models and algorithms have been proposed which assures in detecting and preventing the malicious behavior of nodes. Such methods constituent the concept of above security solutions like cryptography, certification system, intrusion detection system etc.

Table 1: Malicious Behavior Affecting the Security Principle & Its Defensive Methods

S. NO	Malicious Behavior	Affected Security Principle	Suggested Defensive Methods
1.	Message Tampering	Integrity	Cryptograpy-MD5
2.	Stealing Information	Confidentiality	Cryptography
3.	Bandwidth consumption, Battery Drained Buffer Overflow, Node Not Available	Availability	TTP (RWD, Watchdog) and IDS
4.	Entering Malicious node in the Network	Authentication	PKI Certification System

5.	Node Denies of sending message	Non-Repudiation	Digital Signature

V. CONCLUSION

In this paper, normal and malicious behavior of nodes is defined. Security solution to defend such behavior is presented. Malicious behavior which is defined in section 3 cannot be confined to any number and depends on the operating environment and intruder's way to attack the network. Table 1 given below concludes the malicious behavior of a node, the affected security principle and the security solution for it.

VI. REFERENCES

[1] William Stallings "Cryptography and Network Security", Fourth Edition, Pearson Education. ISBN 978-81-7758-774-6, 2006

[2] Patcha,A and Mishra,A - Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks, IEEE. 2003

[3] Panos,C Xenakis,C and Stavrakakis,I - A Novel Intrusion Detection System for MANETs International Conference on Security and Cryptography (SECRYPT) 2009

[4] "Intrusion Detection System" http://www.intrusiondetection- system-group.co.uk/, Link visited on December 2010

[5] Sahu, S and Shandilya, S K - A Comprehensive Survey On Intrusion Detection In Manet, International Journal of Information Technology and Knowledge Management, Volume 2, No. 2, pp. 305-310July-December 2010

[6] C.Siva Ram Murthy and B S Manoj, -Mobile Ad Hoc Networks-Architecture and Protocols, Pearson Education, ISBN 81-317-0688-5 ,2004.

[7] Theodore S. Rappaport, "Wireless Communication" Prentice Publisher, ISBN 0133755363, January 1994.

[8] B. Wu et al, -A Survey of Attacks and Preventions in Mobile Ad Hoc Networks,Wireless/Mobile Network Security, Springer, Vol 17, 2006.

[9] Kimaya Sanzgiti, Bridget Dahill, Brian Neil Levine, Clay shields, Elizabeth M, Belding-Royer, "A secure Routing Protocol for Ad hoc networks", In Proceedings of the 10thIEEE International Conference on Network Protocols (ICNP' 02), pp. 78-87, November 2002.

[10] Alfawaer,Z. And Al Zoubi,S. , "A Proposed Security Subsystem for Ad Hoc Networks" International Forum on Computer Science Technology and Applications,IEEE 2009.