IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-3, Issue-10 E-ISSN: 2347-2693

MANETs: Overview of Vulnerabilities, Security Threats and Prevention and Detection Techniques

Kewal Vora[1*], Jugal Shah[2], Shreyas Parmar[3] and Shivani Bhattacharjee[4]

[1*,2,3,4]*Department of EXTC, Mumbai University, India*

www.ijcseonline.org

Received: Sep/16/2015 Revised: Oct/11/2015 Accepted: Oct /20/2015 Published: Oct /31/ 2015

***Abstract*—** Mobile Ad Hoc Network (MANET), because of its decentralized architecture, dynamic topologies and also due to rapid advancement of wireless devices has become a popular area of research. Though the self-configuring characteristic of Ad Hoc network finds application in various domains, they are exposed to vulnerabilities by malicious attackers which might compromise the entire network and reduce the overall performance of the network. These threats need to be dealt; giving rise to various solutions that would not only maintain the network efficiency but also ensure a successful data transmission along with high level of security. Such solution would require detailed information about the vulnerabilities and different type of attacks which would then lead to computing different detection and prevention mechanisms. This paper gives an overview of vulnerabilities of MANETs, different types of threats and discusses various detection and prevention mechanisms against them.

***Keywords*—** MANET, ad hoc security, vulnerabilities, prevention, detection

1. INTRODUCTION

With the advancement in technology, today almost everyone carry various portable devices such as cell phones, laptops, PDAs, for professional as well as personal use. These devices usually function without any interaction. But if these devices could interact with each other for sharing data, would be very convenient for the users. We could share data wirelessly; view data which resides on your laptop on your mobile phone; mails can be rerouted to your PDA. An ad hoc network allows this to happen. It helps to establish communication between devices without any aid of central infrastructure.

A mobile ad hoc network (MANET) is a wireless network that is established spontaneously as soon as the nodes or the devices connect [1]. Each device is a node of the network and acts as a router to route the data packets. There is no central monitoring in the network which provides it more flexibility and security against failure of a particular node in the network. Also, due to the distributed network nature the nodes are themselves responsible for discovering other nodes. These nodes perform function of hosts as well as routers to forward the network traffic through them. The nodes in the network deliver the packets on multi hop basis which improves the battery life of the devices in the network. The communication medium of the MANET is broadcast. The devices enter and leave the network without any notice and their position is changing frequently which results in a dynamic topology. Places where installing an infrastructure network is not feasible or a temporary network is to be set up, MANETs are established.

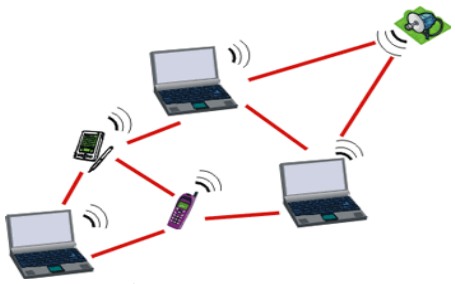

Figure 1: A MANET

The MANETs are very appealing for many applications due to its characteristics such as lack of infrastructure, dynamic topology and no centralized monitoring. However, these characteristics are also responsible for the vulnerabilities in the MANETs. Integrity, confidentiality, authentication, non repudiation and availability are the important security factors taken into consideration while establishing a mobile ad hoc network. Different vulnerabilities of ad hoc networks and security threats in network and routing are proposed in this paper. It also gives various security measures that can be taken to make the wireless ad hoc network more secure.

2. VULNERABILITY IN AD HOC NETWORKS

2.1 Dynamic Topology

The MANETs function by forming a wireless temporary network which is decentralized and has no established infrastructure [1,2]. This dynamic topology of the network allows the nodes to be mobile and enter and leave the network without notifying others. The network is self organizing and it changes rapidly and frequently, often without any security association. This makes it difficult to identify any malicious activities in the network.

2.2 Wireless Links
The wireless network is shared by both authorized users and malicious attackers making it susceptible to active interference or eavesdropping. Thus, the attackers in the radio transmission range can easily launch attacks. The attackers may also cause problems by consuming the bandwidth as the wireless links have lower bandwidth.

2.3 Distributed Network
Due to their dynamic nature, the MANETs work on cooperation and participation of all the nodes in the network [5]. Authentication and key distribution is difficult due to lack of centralized authority. The cooperative algorithms can be disrupted by the attacker as he can easily become a node in the network. It can also intrude and disturb the routing mechanisms by broadcasting false routing information.

2.4 Resource constraints
MANETs support a range of devices with different computing and storage capacities. Attackers may create huge load by targeting a node by performing expensive processes and transmitting additional data. This results in draining of resources such as bandwidth, memory, battery life and computational speed. Due to this denial of service attacks become common in the network.

2.5 Network Size
Though there are many commercial applications of Ad hoc networks, there is a limit on the size of the network due to its dynamic topology and time required to establish and communicate through such networks.

2.6 Cooperativeness
The nodes in a MANET are cooperative and non malicious is the primary assumption of different routing algorithms deployed [3]. This results in a malicious attacker gaining an easy access to the network. The attacker may disturb network operations by denying the protocols thereby disrupting the cooperativeness of the MANET.

3. TYPES OF ATTACKS

3.1 Network security attacks

3.1.1 Passive attacks
Passive attacks do not alter the data or normal functioning of the network. The primary objective of the opponent is to get access to unauthorized information. These attacks are difficult to detect as the attacker may passively collect information without being noticed. Thus, prevention of passive attacks is considered by various ciphering techniques.

3.1.1.a Release of message contents
Confidential and sensitive information might be transmitted or received over the network. It is both undesirable and dangerous if this information reaches to an unintended person.

3.1.1.b Traffic analysis
In this an external adversary tries to analyze the pattern of communication between other nodes.
On the basis of the pattern of the messages any unauthorized user may gather information such as identity of other nodes, network topology, geographical location and knowledge of other nodes in the network.

3.1.2 Active attacks
Active attacks involve alteration of message packets or generation of invalid message packets [2]. Attacker aim of this type of attack is to corrupt or destroy the data as well as network itself. These types of attacks are easier to detect as there is alteration of information.

3.1.2.a Masquerading
It is a threat action whereby an external adversary gains access to the network by behaving as an authenticate user. It is generally done to gain access to a system, or to steal important data from the system. It can be done by impersonating another authenticate user. Once attacker gains access, they get full access to the network for altering data or other network policies.

3.1.2.b Replay
Also known as playback attack, in this delay in transmission of data a network jam is created by an attacker through retransmission of data multiple times. It creates an unauthorized effect by passive capturing and retransmission of subsequent information.

3.1.2.c Modification of messages
The original data sent by an authenticate user is modified by an attacker such that it becomes non meaningful or its sense is changed. Data manipulation or destruction results in loss of integrity of the information.

3.1.2.d Denial of Service (DoS)
This attack consumes the network resources making the communication facilities unavailable for the user to communicate securely. It is generally done by interrupting in the network connections between the users, making some services unavailable to the user or disrupting the entire network by overloading it with unwanted messages.

3.1.2.e Sleep deprivation torture
This attack is induced by DoS where communication between the nodes is disabled by excessive consumption of resources [4]. The malicious node engages other nodes in heavy computation and processing using false information.

Such an attack exhausts the battery life of the legitimate node and if no charging is possible it can kill an active node from the network. The power constraints of the devices in a MANET make sleep deprivation torture an important issue.

3.2 Attacks that disrupt the various routing protocols

3.2.1 Routing Table Overflow

The malicious node overwhelms the network with false routes and thus the routing protocol fails to function. The attacker floods the network with routes to nonexistent nodes in order to prevent new routes to be created.

3.2.2 Routing Table Poisoning

The malicious nodes in the network send false routing updates thereby creating false entries in the routing tables. The actual route packets sent to uncompromised nodes may also be altered. Thus, it is very important to authorize and authenticate the routing messages.

3.2.3 Blackhole attack

A malicious node announces itself as having the ideal path to the node whose messages it wants to hijack [3,5]. Once a route is established through the malicious node, it can intercept and modify all the message packets. It can also drop all the message packets leading to DoS attack.

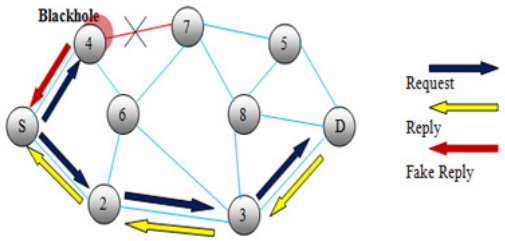

Figure 2: Black-hole attack

3.2.4 Sinkhole attack

A single compromised node attracts traffic from all the nodes in the network resulting in network congestion or jamming at that node. It uses the loopholes in the routing algorithms to present itself the best route in the network. On receiving the traffic the compromised node may modify the message packets or even drop them.

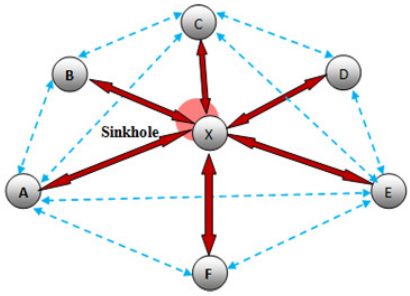

Figure 3: Sink-hole attack

3.2.5 Wormhole attack

In this type of attack, two compromised nodes in the network collude together to create a tunnel to route the message packets [3,5]. They attract network traffic by advertising false routing information. Wormholes prevent the discovery of any other route in the network and even without the knowledge routing protocols in the network can rupture the routing mechanism in the network.

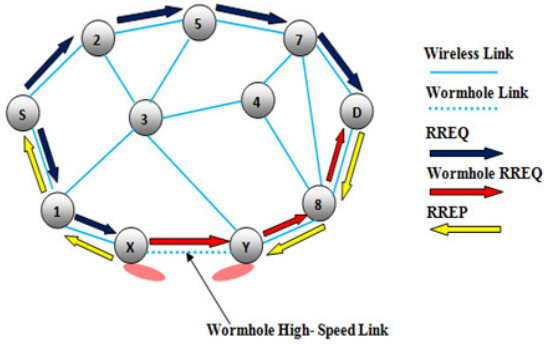

Figure 4: Wormhole attack

3.2.6 Sybil attack

Sybil nodes are the additional identities that an attacker acquires. Using a single physical device, the Sybil attacker generates fake identities of a number of additional nodes. Thus, it becomes difficult to track the attacker as we see it as a large number whereas in reality it is a single entity. It disrupts the routing protocols as the Sybil nodes appear at different position in the network. The resource allocation between the nodes is unfair.

4. APPROACHES TO SECURE MANETS

There are mainly two methods for securing mobile ad hoc networks which are categorized based on the functions they perform named as proactive and reactive. In order to prevent an attack, various cryptographic methods are executed, which is the function of proactive method. On the contrary, reactive method detects a security threat empirically and acts accordingly. Both the methods are used on sub domain basis individually, however due to absence of the clear line of defense, a hybrid model of both the methods is been implemented for prevention, detection and reaction. Prevention technique is basically used to prevent the attacks on the system by increasing the adversities of permeating in to the system. However, as no system is ideal, attacks can take place and thus to identify those attacks a detection mechanism is used which checks the aberrant behavior either from source to destination basis or by adjoining nodes. After the detection of an attack, reaction mechanism is used to substantiate whether an attack is going on and thereupon takes action against it which could be either avoiding or eliminating the node from the network.

4.1 Preventive Mechanisms

Here we introduce the trust models or encryption techniques for communication that creates the base of the idea of prevention from intrusions. The requirement to provide security and authentication for proper functioning of the network, various ad hoc routing protocols and techniques along with trust models have been developed which are discussed in this section.

4.1.1 Cryptographic Mechanisms

Authentication of messages using the hash function technique adds an enumerated e-signature to the message which is verified by the recipient for trusted communication. [10] However, there are many adversities related to the addition of the signature such as overhead length, system response, QoS and the ability to adapt to the dynamic network.

4.1.1.a Hashed Message Authentication Codes (HMAC)

Here the server and the client both are provided with a private and public key. When the customer requests for service, it attaches its HMAC with the request and the server regenerates it unique HMAC when the request is received. If both match then the client could be trusted. Since, every client has to be provided with a pair wise shared key, the number of total keys for n nodes that would be generated is n(n-1)/2. This technique has both pros and cons; it provides with lower overhead, efficacy but requires only intended receivers without the facility of broadcast.

4.1.1.b Digital Signature

To ensure security, this technique makes use of asymmetric key cryptography system. Here, the type of algorithm used is RSA for improved secrecy and to cope with demand of digital signature MD-5 hash function is used. Though it has a few advantages, there is one major flaw; the attacker can create false signatures so that a node with computational resources exhausts.

As we saw the different mechanisms, keys either symmetric or asymmetric played the major role in communication security. As we know that only one shared key would hamper the security of the system, the need for set of unique keys per node is felt. Since we are opting for a set of unique keys for each node, the hindrance of our path is the distribution of the keys without hampering the authenticity of the system. There are various solutions proposed to this predicament in Y.Hu and A. Perrig [7].

4.1.2 Trust Management

Since we have adopted a decentralized network, trust is handled at node level. A reliable Certificate Authority (CA) issues individual authorized certificate which is transferred between nodes which is verified for trusting the nodes. The certificate consists of node address, its public key, a signature provided by the CA. While sending a message, the certificate is attached with it, through which the recipient verifies the authenticity of the node and then use the public key to scrutinize the signature.

CA serves various purposes such as issuing, storing, validating, revoking, key management, etc. CA distributes public keys to nodes which authenticates the certificate registered by the CA's private key. To fulfill the demands, CA's have to be plugged in 24x7. A distributive key management system is used which contains numerous CAs because a single CA system can easily die off.

The distributive system depends on mainly three parameters: fault tolerance, vulnerability and availability. Fault tolerance is the capability of the system to handle node failures; vulnerability is the figure of the compromised nodes the system can brace; and availability is the ability to reach the essential CAs. An idea of implementing a large number of CAs is proposed to optimize fault tolerance however this leads to degradation of availability and vulnerability. The idea is not recommended because of two reasons, firstly, it may happen that one of the CAs is attacked and as all share the same private key in the same domain of the network it, leads to the degradation of security. Secondly, all CAs might not be accessible every time thus it requires a complicated system to be built to fulfill the demands. There also many proposed ideas which result in a large overhead thus would be ineffective in the case of high mobility state. Hence, a system could only be optimized by compromising one of the factors.

Another idea which has become popular is the reputation scheme; where the nodes update the trust levels of other nodes dynamically on the basis of their behavior. This scheme is helpful for distinguishing between nodes thus allowing them to use a trusted path without any malicious components in it. The scheme uses various methods to update the trust levels such as their observation, second-hand observation, etc and thus render a particular node as malicious. Once the malfunctioning node is detected, it is abandoned for a time being after which the scheme allows the technique for the redemption of the node. Thus, this scheme amalgamates all the three components which were discussed above which are: supervising, reputation and redemption mechanisms.

4.2 Detection mechanism

The self configuring Ad Hoc network uses detection mechanism to monitor the on-going attacks on the network and also keeps a check on the aberrant nature of the malicious nodes. The Intrusion Detection System (IDS) [6] is defined a system which monitors the entire network for the anomalous behaviour of nodes taking part in the transmission of packets and notifies other nodes about the

same in order to avoid the misbehaving node. The IDS also has the added responsibility of determining the type of attack besides identifying the attacker. Thus, detail information of the attack is provided and the IDS then dynamically change the threshold of the network, thus making the network more secured. In here we talk about the following detection techniques:

4.2.1 Localized detection technique

This technique is also called as watchdog [8] technique since it makes use of a node within the network to monitor the transmission of the packet taking place in the neighbouring nodes. Such nodes are called as monitor nodes. This special node overhears the packet transmissions of neighbouring nodes for detecting anomalies in packet forwarding. It evaluates the behaviour of neighbouring nodes by assuming bi-directional symmetrical connectivity. See fig 5.

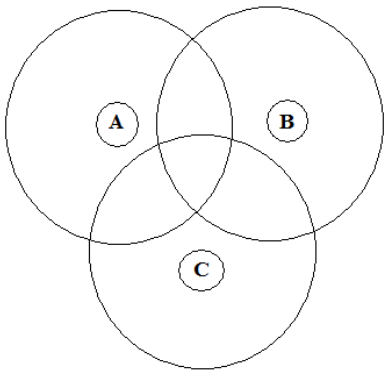

Figure 5: Nodes in the network and their transmission ranges

[9] Bidirectional symmetry means if A can hear B, then B can hear A. Since the path from A is specified, when A forwards a packet to B, it overhears the channel expecting B to forward the packet to C, if B does not transmit, a time out occurs at A's end and a failure's tally associated with B is increased, if the number of failure of B increases beyond a certain threshold, or if A detects that B changed the integrity of the forwarded packet its misbehaviour is reported. Now consider B as a monitor node and the route of packet transmission from node A to node C. The monitor node B overhears the packet transmission from A to C and also checks if C has transmitted the packet or has dropped it intentionally. If node C misbehaves, node B reports about this misbehaviour (dropping the package or mangling with it) to all the other nodes within its radio range in the network and accordingly asks for a different route path so as to exclude node C from the participating in the transmission process.

4.2.2 Acknowledge based detection technique:

This is one of the most effective ways of keeping a track on the packet transmission and ensuring that the abnormal node is detected and punished by rendering it useless. In this technique even the destination node is cross checked for its behaviour. The source first sends a request to the destination to check its availability. On receiving ACK [10], the sender node requests for the signature to check whether the destination node is malicious or not. After the verification of the signature (IP address, MAC address and other node entities), the encrypted data is sent to the destination using the routing protocol. This technique also monitors the behaviour of the intermediate nodes. The encrypted data has a public key for the intermediate nodes and a private key for the destination node. This public key is used for verification and authentication of the intermediate nodes. On receiving the data from the sender node, the neighbouring node uses the key and sends an acknowledgement back to the sender. This chain of ACK goes on from the intermediate nodes to the sender node which helps to verify that the packet is not dropped or tampered in between its transmission path. If any malicious node intentionally drops the packet, the next node is then unable to send the verification or the ACK to the sender node. On not receiving the ACK within a stipulated time interval, the sender node detects the malicious node and then uses the routing protocol to send the packet through a different route. Thus, this explicit acknowledgement form the nodes in the network helps to detect and prevent the malicious nodes from participating in the packet transmission, thereby providing better security to the network.

4.3 Reaction Mechanism

This mechanism has the responsibility of protecting the network from the adverse effects of an intrusion or misbehaviour. On the detection of malicious activity, reaction mechanisms are employed to either avoiding the node from the routing selection or to exclude it completely. Two mechanisms techniques are available:

4.3.1 Global Reaction

Using the collaborative Intrusion Detection System (IDS) wherein the nodes cooperate to detect falsely behaving nodes, a consensus is reached by these neighbouring nodes. This results in the isolation and denial of participation of that node from the network.

4.3.2 End Host Reaction

The end host reaction makes use of the reputation trust model and the watchdog detection technique to prevent the participation of malicious nodes. A path rater [8] system is used by each node wherein the nodes maintain a rating (trust rating) for each of its neighbouring nodes which is related to its behaviour and also its transmission efficiency. A decrease in the rating indicates misbehaviour of that

particular node and an increase in the rating indicates trusted and efficient transmission path. The routing protocol makes use of these ratings and the source then computes average rating of the different paths and selects the one with highest rating. Thus, using this trust table maintained by each node, a proper route is selected that would exclude the malevolent nodes from the network.

5. CONCLUSION

The discussed topic, mobile ad hoc network, has many benefits like the decentralized management, ability to accept new nodes without any configurations, etc which has made it very popular. As every system is not an ideal one, here also the advantages are achieved on the loss of battery and open system easily available for attacking. Such various adversities due to resource constraints, network size, cooperativeness, etc were discussed in this paper. The different types of attacks are classified depending on their effects on the system into parts namely passive and active attacks i.e. network security attacks. Vulnerability was also classified as attacks that disrupt the various routing protocols. To overcome the cited problems various solutions are discussed in the security section where all the problems are classified under proactive and reactive components which encircle the three main domains: prevention, detection and reaction, for security of the system. The security measures under preventive components are categorized as cryptographic and trust management systems. In the remaining two domains of security, various other methods were discussed such as localized and ACK based detection, global and local end node reactions to protect the system for attackers intruding the network. Thus, in this paper we have highlighted various problems associated with MANETs and its solutions.

REFERENCES

[1] Mohammad Ilyas, "The Handbook of Ad Hoc Wireless Networks" Text Book.

[2] Amitabh Mishra, "Security and Quality of Service in ad hoc wireless networks" (chapter 1, 3), ISBN- 13 **978-0-521-87824-1** Handbook

[3] Sukla Banerjee , "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October **22 - 24**, **2008**, San Francisco, USA.

[4] Gangotri A Khiratkar and Swati S Mahajan, "Performance Analysis of Cluster Based Routing Protocol for Ad hoc Networks", International Journal of Computer Sciences and Engineering, Volume-02, Issue-04, Page No (141-143), Apr -**2014**, E-ISSN: 2347-2693

[5] Pradip M. Jawandhiya, Mangesh M. Ghonge, Dr. M.S.Ali, Prof. J.S. Deshpande, "A Survey of Mobile Ad Hoc Network Attacks ", International Journal of Engineering Science and Technology, Vol. 2(9), **2010**, 4063-4071

[6] Dipali D. Punwatkar and Kapil N. Hande, "A Review of Malicious Node Detection in Mobile Ad-hoc Networks", International Journal of Computer Sciences and Engineering, Volume-02, Issue-02, Page No (65-69), Feb - **2014**, E-ISSN: 2347-2693

[7] Y.C. Hu, A. Perrig, and D.B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proc. 2003 ACM Workshop on Wireless Security (WiSe 2003), ACM Press, **2003**, pp. **30–40**.

[8] D.Anitha and Dr.M.Punithavalli : A Collaborative Selfish Replica with Watchdog and Pathrater in MANETS. In IJCSMC, Vol. 2, Issue. 3, **March 2013**.

[9] S.Madhavi and Dr. Tai Hoon Kim: An Intrusion Detection System in Mobile Ad Hoc Networks. In International Journal of Security and Its Applications Vol. 2, No.3, July, **2008**.

[10] Ali EI-Mousl and Ashraf Suyyagh: Ad Hoc Networks Security Challenges. In 7th International Multi-Conference on Systems, Signals and Devices, **2010**.