A Review on Security in MANET

Vaishali
Department of Computer Science HMRITM
Delhi, India

Priyank Pandey
Department of Computer Science
BPIBS
Delhi, India

Prashant Goel
Department of Computer Science
MAIT
Delhi, India

Abstract— **Networks formed for specific applications are called ad-hoc networks. In an ad-hoc model wireless devices can communicate with each other without the need of any central entity. All the devices that are in range of each other can discover and communicate to each other. Ad-hoc networks are flexible in every way, means they can be constructed, partitioned or merged with any other of the type on the go. In ad-hoc network, nodes are mobile in nature and uses wireless communication. In this case these are called as Mobile Ad-hoc Network (MANET). For these networks to find peer-to-peer path between working nodes, several protocols have been proposed. These routing protocols are supine to attack by the malicious nodes. The need of time is to detect and prevent the attacks caused by the malicious nodes without abruption in network services. In this paper, we present the study about various threats in security of MANETS and their detection and prevention techniques.**

Keywords— ***Ad-hoc networks, MANET, Wireless network, malicious node, Routing Protocols, Security***

I. INTRODUCTION

Ad-hoc networks are created for short term use with some specific purpose. The assumption behind these networks is that there exists an end-to-end path between nodes present. These networks are very useful in conditions where the infrastructure for network is not available. This is in fact the basic characteristic for ad-hoc networks. These networks are formative and facile to reconfigure. Ad-hoc networks have confined resources. The reason behind this is paucity of fixed infrastructure. For proper functioning of the network several resources like bandwidth and power source have to be used aptly. When nodes in ad-hoc networks are mostly dynamic in nature, they are called as MANET. These nodes are devices with wireless capability like smart phones or PDAs. Due to their location changing tendency they use dynamic topology. The whole concept of MANET is a self-organized system. Each node in such network is capable of routing messages and assuring security on its own. Above self-sufficient nature makes these networks cost-effective. Figure 1 is an example of how nodes communicates in an ad-hoc network. In above scenario communication is in between five wireless nodes A, B, C, D and E. Node A here wants to send message to node E. in such cases routing is done in multiple hop manner. Node A will send the message to node B. node B will forward this message to node C. in this manner the message will be received by the destination node E.

The paper is organized as follows. Section 2 details the various routing protocols used in ad-hoc networks. Section 3 provides details about various security related issues in ad-hoc networks. Section 4 is about routing attacks and section 5 deals with network attacks and their categories. The detailed conclusion is presented in section 6 along with the future scope.

These are also called on demand routing protocols. Whenever a node wants to send message to any other node presents in the network, it floods the request packets for route (RREQ) to its neighbors. Any node in between, if have the path to the destination, then replies to the source with the route reply messages (RREP) and in this manner routing is completed. This kind of routing is useful in medium sized networks with high mobility of nodes. The problem of

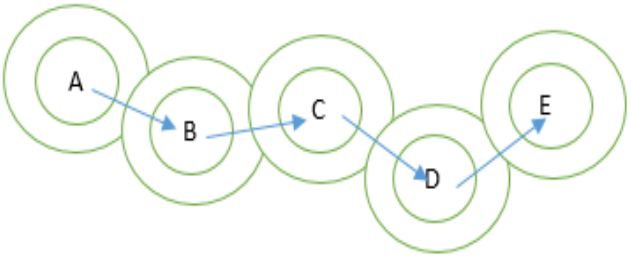

Figure 1: Example of Ad-hoc Wireless Network

II. ROUTING PROTOCOLS IN MANETS

Routing protocols [2] in MANET use to find an optimal path between the source and destination nodes. This optimal path should have to be with minimum bandwidth, minimum overhead and minimum time delay between the concerned nodes. Most of the nodes in such networks are wireless mobile so there is no fix topology for these networks. As result the nodes have to discover the topology of network regularly for efficient routing of messages. For the reason of this changing topology there is a need for different routing protocols. A particular protocol can be selected with few parameters under consideration like density and mobility of the wireless nodes in the network

A. Routing Protocols based on Network Topology

MANETS have mobile nodes with dynamic topology. The network may have uni-directional as well as bidirectional links at any point of time. On the basis of topology used, routing protocols can be divided as follows:

1. Pro-active Protocols

Each node present in network maintains a routing table. Pro-active routing protocols uses the information present in these tables. This is also called as table driven routing. Each node contains information of its neighboring node in the routing

table. Nodes exchanges the tables with their neighbors within a predefined time interval. Pro-active routing algorithms are best suited for small size networks with lower node mobility. There may be chances of failure in network due to the dynamic topology. Since the routing tables are not much frequently updated so there may be chances for failure in links.

Few pro-active routing protocols are Landmark Routing Protocol (LANMAR), Optimized Link State Routing (OLSR) etc. OLSR applies a multi-tiered practice associated with multi-point relays (MPR). With the help of MPR's it is possible to apply scope flooding instead of full node flooding. This can help in reduce the amount of exchanged data. The MPR's are selected in such a way that only those nodes with bi-directional links to another nodes can be the service providers. Optimized Link State Routing protocol works in dispersed environment and the MPR approach also does not require any focused entity.

2. Reactive Routing Protocols

network congestion may happen in these routing protocols due to heavy flooding of request and reply packets. Also there may be a large time delay in routing the message from source to destination due to different packet transactions.

Few Reactive Routing protocols are Admission Control Enabled on Demand Routing (ACOR), Ad-hoc on Demand Distance Vector (ADOV) [12] etc. ADOV is a unicast type routing protocol. It uses to facilitate multi hop routing. The source node does not specify the address of the whole path, instead it provide address of the next hop only. For security concerns in AODV, IPsec is one of the possible solution.

3. Hybrid Routing Protocols

Hybrid approach of routing uses Proactive and Reactive both the methodologies for routing. Initially the nodes find route with the help of some proactive algorithm and then for demand routing it uses reactive methods. The use of one of the above protocols is dependent on the scenario of the network. With the benefits of both the mentioned protocols, Hybrid approach is an optimal solution.

Few Hybrid Routing Algorithms are Zone-Based Hierarchical Link State (ZHLS), Zone Routing Protocol (ZRP) etc.

III. SECURITY CONCERNS IN MANETS

As the nodes are mobile and responsible for routing the packets in MANET, the network is more prone to attacks than normal networks. There are few basic security concerns in MANET as below mentioned:

a. Those cryptographic solutions which are applicable to wired networks are not feasible for ad-hoc networks due to lack of resources. That is why there is a need to find new solutions in this domain.
b. There is a lack of privacy due to interoperability in wireless devices. Messages can be easily eavesdropped in these.
c. Since the nodes in ad-hoc networks are involved in relaying process of messages, so any malicious node can take advantage of this to misuse the networks traffic either by modifying it or by eavesdropping.
d. Location of nodes in network is also an issue for security. The nodes of ad-hoc networks may be deployed in an unsecure environment. This may encourage many physical attacks to the deployed nodes.
e. The dynamic nature of network topologies in ad-hoc networks provides more opportunities for malicious nodes to attack.

A. Basic Security Constraints for MANETS

There are four major constraints to be followed in construction of ad-hoc networks.

a. Confidentiality:
Data should not to be disclosed to any unauthorized party while the transfer. Confidentiality ensures that the routing information of a certain node should be kept secret to only those who are authorized to access. Unauthorized nodes should not have an access to routing table. This mechanism is beneficial to restrict the critical information to known nodes only. Confidentiality is highly required in the case of ad-hoc networks where transmission of critical information so that no intruder is successful in order to gain any kind of information. Failure of confidentiality creates dreadful outcomes that becomes a barrier in achieving security. Encryption of data is the important technique in achieving confidentiality.
b. Integrity:
If the message is modified in between the transmission then integrity is violated. Integrity should have to be maintained to prevent the unauthorized users from modifying the content. Integrity preserves the correct information to be transmitted between source node and destination node. Whenever sender sends some kind of message to receiver, receiver should have a mechanism to check whether the message is altered or not. It should provide untampered data. No outsider node should have the privilege to modify or corrupt the message. Lack of integrity leads to inconsistent data.
c. Availability:
The formation of any network is for exchange of data and information. This constraint ensures that the data is available at any point of timed in the network. This constraint can be violated by Denial-of-Service attack. Availability should be able to deliver all the services whenever a legitimate user wants to access them. Messages or the data should be accessible despite of the attacks in the network. The network should be operational or active even in the case of any malicious attack. In order to ensure high availability, the attacks like Denial of Service (DoS) or excessive flooding of messages in the network should be prevented.
d. Non-Repudiation:
Non-Repudiation is a phenomenon where the messages that are delivered to the receiver (sent by the sender) cannot deny later that the messages have not been received. If a message is found to be

erroneous, no sender can prove that this message has not been sent by him. In order to prevent this ambiguity, digital signatures with security techniques have been applied as a proof, which contains a unique identity of sender.

e. Key Management:

Managing keys [13] for security is corrival task in Mobile Ad-hoc Network. The difficulty arises because of its dynamic topology, limitation in resources, different capacities of links and operation with larger constraints. Various cryptographic key schemes are used in MANET like public key, symmetric key and hybrid key. In public key two different keys are used for encryption and decryption. In symmetric key type, same key is shared between two parties. There is a key called as Group key which is assigned to a group of mobile nodes in MANET. Group key protocol can be parted in three ways as centralized, distributed [14] and decentralized. In centralized way, single entity is responsible for group key. In distributed method each node in group is responsible for the group key. In decentralized method more than one entity from the group is responsible for the group key process.

IV. ATTACKS IN MANETS

In MANET attacks can be of two types: Passive attack that usually eavesdrops the data and information and Active attack that are used for the modification and alteration of data and information. All the active attacks are basically external ones. These causes congestion in network, false traffic information and delay. Several pre-defined mechanism like firewalls and encryption methods are there to prevent these external attacks. On the other hand internal attacks are more severe. The malicious nodes in this attack are usually part of the network so there is no effect of security mechanism on them. These malicious nodes may also work in group. They can use the genuine security aspects to protect them as they are insiders. These nodes are also called as compromised nodes.

A. Sleep Deprivation Attack

This is a type of flooding attack. A node or a group of nodes are targeted for attack. The purpose of this attack is to exhaust the capability and resources of a node. For this malicious node sends fake requests to the targeted node from the false nodes. This will exhaust the resources like computational power and battery life of the targeted node. In the time period of attack the targeted node cannot process any genuine request. In result the genuine targeted node will not be able to participate in the process of routing and will become absolute for other nodes in the network.

An example network arrangement is shown in figure 2 for SDA. Here node D is a malicious node and sends false requests to genuine node A in the network. Due to overhead energy depletion occurs at node A

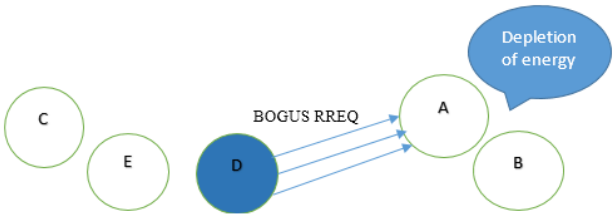

Figure 2: Sleep Deprivation Attack

B. Black Hole Attack

In ad-hoc networks the term Black Hole defines a node that ingests all the data traffic going through it. It does not forwards the data to the next node. Due to dropping of data packets re-transmission increases and leads to congestion in the network. The black hole node receives the request and sends back the response to the source as it is the genuine destination. In turn the source sends all the data to the black hole node. The malicious black hole node also can advertise that it has the shortest path to any given destination node. In below example in figure 3, node K is the black hole node. It receives the request from node J for node L. its sends back the reply to J that it has the shortest path to L. when J sends data to the black hole node K, it drops the data packets.

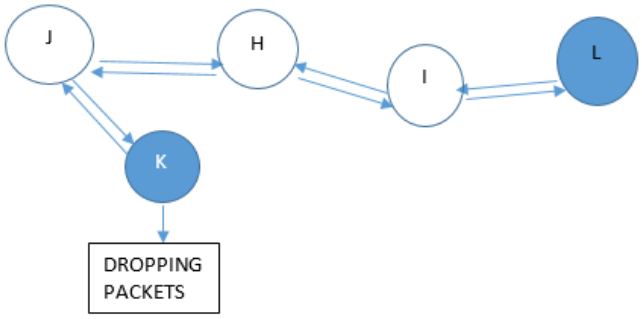

Figure 3: Black Hole Attack

Black Hole attacks can be detected in many ways. It can be detected by over hearing the actions of all the neighbor nodes in the network. For prevention of Black Hole attacks and to ensure routing security [4] there are two suggested ways as follows

For routing the packets the algorithm finds more then on route. Sender sends the request to its neighbors including the malicious node. It then waits for the reply. In reply the sender matches the paths with common nodes. If it did not get any path with common node then it waits a bit longer. There may be a case when there is no path with common nodes. No forwarding of data happens in that case. Time elapse is one of the drawback for this type of approach.

In another method, each node have to maintain two extra tables, one for storing last packet number of last packet received from each node and another for storing last packet number of the last data packet sent to every node. When

source node will throw its request to other node then each node including malicious node will reply with a number received from the source node. Now the source can identify the reply of malicious node by analyzing the number in reply.

C. *Impersonation Attack*

In ad-hoc networks if any malicious node takes place of any genuine node by spoofing its physical or logical address then impersonation attack is possible. After getting identity of a trusted node it may damage the authentication ethics of the network. The malicious node uses the address of the trustworthy node for sending data and then receives the data meant for the original node. With this it can also interrupt the routing knowledge of other nodes. One can impersonate a node in network by guessing the details of that node or by corrupting the authentication mechanism of the network. In figure 4 node E is a malicious node and it is behaving like node D. Any message sent for node D will be forwarded to it as shown. The malicious node will first of all send packet to its neighbors with the address of node D. Few routing protocols can be used with digital signatures to prevent this attack

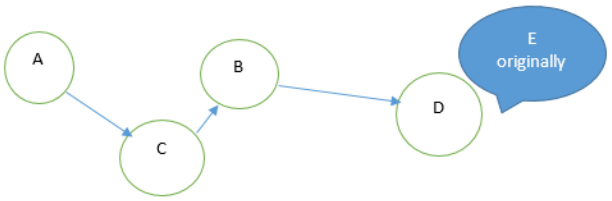

Figure 4: Impersonation Attack

D. *Rushing Attack (RA)*

Rushing is used because an attacker will try to speed up the process for becoming hop of the path for target node. For this the malicious node will forward the request packets faster than any other node in the network. Doing this will increase the probability of malicious node getting in the path. After getting in the hop path, malicious node can tamper the data flowing through it. The attacker can flood its neighbor nodes with false request packets to slow down their processing speed. It will increase the forwarding speed of the attacker. In other way forwarding speed can also be enhanced by using higher transmission rate. With higher transmission rate less number of hops will be needed.

In Figure 5, node A is source and E is destination. The usual route was ABCDE. Malicious node F floods node D with fake requests and takes place of it in the path. Now the data for node E will be going through node F.

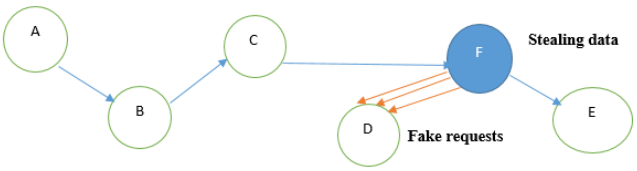

Figure 5: Rushing Attack

E. *Poisoning of Routing Table Attack (PRTA)*

In this attack, the attacker corrupts the nodes in its neighbor by exploiting their routing tables. By tempering the routing tables of the nodes several faults like fake optimal path problem, false routes, formation of circuits and congestion in network can happen. Poisoning of tables may be happen in several ways. A malicious node can broadcast false traffic and may alter the entries in other nodes table in the network. In another way the malicious node can delete the genuine path with lower sequence number by generating fake high sequence number path.

In figure 6, malicious node D sends fake requests to node B and C. it will corrupt the routing tables of both the nodes. Due to this a loop is formed between nodes A, B and C. A one way chain hash can be used to prevent the malicious node from decreasing the hop count in the path. Generation of packets with high sequence number is the basic reason for poisoning of routing tables. Due to these high sequence numbers the route with low sequence number got discarded

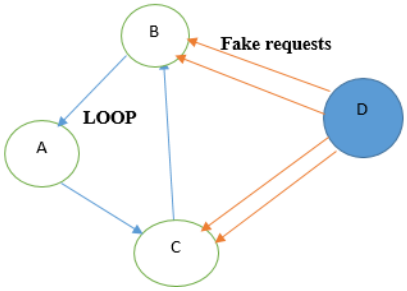

Figure 6: Poisoning of Routing Table Attack

V. ANALYSIS OF ATTACKS

On the basis of type, the above mentioned attacks have their causes. There are detection and prevention techniques for these network attacks. In the below table 1, we have shown the analysis of the attacks with their causes and prevention techniques in the tabular form.

TABLE I. SUMMARY OF ATTACKS: CAUSES & PREVENTION

Name of Attack	Causes	Prevention
Sleep Deprivation Attack	Transition of false request to ensure consumption of resources of target node.	In a cluster, the cluster head uses a threshold value to forward a packet to any node. After threshold no data packet will be entertained [6].
Black Hole Attack	Fake replies from malicious node with higher order sequence numbers.	By finding routes with common nodes. Based on selection of more than one route for packet transmission [9].
Impersonation Attack	Spoofing of physical or logical address.	By use of digital signatures with routing protocols [11].
Rushing Attack	Increased speed of packet forwarding and higher transmission rate.	Some generic methods that will defend from Rushing Attack [7].
Poisoning of Routing Table Attack	By creating false entries in the routing table of nodes with the help of fake traffic.	Use of Hash chain to prevent the generation of false higher order sequence numbers [8].

VI. CONCLUSION AND FUTURE SCOPE

This work presented a review over various network attacks on MANETS like Black Hole Attack, Sleep Deprivation Attack, and Rushing Attack, Impersonation Attack etc. An analysis of the causes and prevention of the above attacks has also been done in this paper. Various points related to the security of MANETS have also been discussed. Every attack that effects the network has its very own characteristics. With the help of those characteristics these attacks can be detected and prevented. By detecting the malicious node in the network it is possible to mitigate the risk by removing the node from the network.

In future work, using these kinds of detection as well as prevention techniques, we will be doing implementing a secure system for MANET. Various flaws and limitations are being detected in this paper that should be rectified so that primary concern which is security is well integrated along with the traditional routing protocols for MANET. The in detail review and comparison of different attacks and their prevention will help the future research in the area. The protocols used for prevention of attacks can be modified and be reviewed further.

REFERENCES

[1] Donatas Sumyla, “Mobile Ad-hoc Networks (MANETS)” , 2006

[2] S. Corson and J. Macker, “mobile Ad-hoc Networking: Routing Protocol Performance Issues and Evaluation Considerations.” The Internet Society, 1999.

[3] Hao Yang and Haiyun Luo, “Security in Mobile ad-hoc networks Challenges and solutions.” Wireless Communications, IEEE, Vol.11, 2004.

[4] Hongmei Deng, Agarwal, D.P. “Routing Security in Ad-hoc Wireless Networks.” Communications Magazine, IEEE, Vol.40, 2002.

[5] M. Umaparvathi and D.K Varghese, “Two Tier Secure AODV against Black Hole Attack in MANET’s.”, European Journal of Scientific Research, 2012.

[6] M. Sarkar and B.D Roy, “Prevention of Sleep Deprivation Attack Using Clustering.” ICECT, Third International Conference, IEEE, Vol.5, 2011.

[7] Y.C Hu, A. Perrig and D. Johnson, “Rushing Attacks and Defense in Ad-hoc Wireless Network Routing Protocols” Proceedings of the ACM Workshop on Wireless Security (WiSe), pp. 30-40, 2003.

[8] Y.C Hu, D. Johnson and A. Perrig, “Secure Efficient Distance Vector Routing for Mobile Ad-hoc Network.” , Ad-hoc Networks, 2003.

[9] M. Al- Shurman, S-M. Yoo and S. Park, “Black Hole Attack in Mobile Ad-hoc Networks.” Asian Southeast Regional Conf., 2004.

[10] T.Bhattasali, R. Chaki, S. Sanyal, “Sleep Deprivation Attack Detection in Wireless Sensor Network.”, International Journal of Computer Applications, , February 2012, Foundation of Computer Science, New York, USA,Vol.40, 2012

[11] Manel Guerrero Zapata., “Secure Ad-hoc on-demand Distance Vector Routing.”, IETF MANET List, 2001.

[12] C.E. Perkins and E.M Royer, “Ad-hoc on Demand Distance Vector Routing.”, Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, 1999.

[13] Bing Wu, Jie Wu and Yuhong Dong, “An efficient Group Key Management Scheme for Mobile Ad-hoc Networks.” International Journal and Networks, 2008.

[14] Aldar C-F. Chan, “Distributed Symmetric Key Management for Mobile Ad-hoc Networks”, IEEE, 2004.

[15] Chauhan, Radhika, Nitin Goyal, and Rakesh Kumar. "A Review on Tuning Of OLSR Routing Protocol IN VANET." International Journal of Advanced Research and Innovative Ideas in Education 2.2 (2016): 508-512.