Volume 4, No. 4, March-April 2013

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

REVIEW ARTICAL

Available Online at www.ijarcs.info

Security Issues in Mobile Ad-hoc Networks Routing

Ipsita Panda
Sr. Lecturer, Dept of CSE, S.I.E.T
Dhenkanal, India
ipsita.panda24@gmail.com

Abstract: MANET is a self organized and self configurable network where the mobile nodes move arbitrarily.. The wireless nature of MANET gives the security to the designers, although security problems in MANETs give more attention but in last some days researchers have find out many types of attacks and system security, which means how to give security to the system. The routing Protocol which gives the shortest path it gives more collisions and delay in between. In order to avoid all loss in performance and gives less chance to collision this paper gives some techniques to discover the active shortcuts and best possible path.

Keywords: Security, Routing, MANET, Attack, Protocols.

I. INTRODUCTION

A. *MANET Concept:*

MANET is a self organized and self configurable network where the mobile nodes move arbitrarily. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time. The traffic types in ad hoc networks are quite different from those in an infrastructure wireless network, including:

- ***a. Peer-to-Peer*:** Communication between two nodes which are within one hop.
- ***b. Remote-to-Remote*:** Communication between two nodes beyond a single hop but which maintain a stable route between them.
- ***c. Dynamic Traffic:*** This occurs when nodes are dynamic and moving around. Routes must be reconstructed. This results in a poor connectivity and network activity in short bursts.

B. *MANET Features:*

MANET has the following features:

- ***a. Autonomous terminal*:** In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router.
- ***b. Distributed operation:*** Since there is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.
- ***c. Multihop routing:*** Basic types of ad hoc routing algorithms can be single-hop and multihop, based on different link layer attributes and routing protocols. Single-hop MANET is simpler than multihop in terms of structure and implementation, with the cost of lesser functionality and applicability. Multihop routing, when delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes.
- ***d. Dynamic network topology:*** MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming their own network on the fly. A user in the MANET may not only operate within the ad hoc network, but may require access to a public fixed network [1].
- ***e. Fluctuating link capacity:*** The channel over which the terminals communicate is subject to noise, fading, and interference, and has less bandwidth than a wired network. In some scenarios, the path between any pair of users can traverse multiple wireless links and the link themselves can be heterogeneous.
- ***f. Light-weight terminals:*** In most cases, the MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions [3].

II. ROUTING PROTOCOLS AND ATTACKS

In ad hoc mobile networks, routes are mainly multi hop because of the limited radio propagation range and topology changes frequently and unpredictably since each network host moves randomly. Therefore, routing is an integral part of ad hoc communications. Routing is to find and maintain routes between nodes in a dynamic topology with possibly uni-directional links, using minimum resources.

A. *Types of Routing Protocols:*

a. *Table-driven or Proactive Protocols:*

Proactive routing protocols attempt to maintain consistent, up-to-date routing information between every pair of nodes in the network by propagating, proactively, route updates at fixed intervals. Representative proactive protocols include: Destination-Sequenced Distance- Vector (DSDV) routing, Clustered Gateway Switch Routing (CGSR), Wireless Routing Protocol (WRP), Optimized Link State Routing (OLSR) and *The Fisheye State Routing (FSR)* flood the network with control messages.

b. On-demand or Reactive Protocols:

A different approach from table-driven routing is reactive or on- demand routing. Reactive protocols, unlike table-driven ones, establish a route to a destination when there is a demand for it, usually initiated by the source node through discovery process within the network. Reactive protocols, unlike table-driven ones, establish a route to a destination when there is a demand for it, usually initiated by the source node through discovery process within the network. Representative reactive routing protocols include: Dynamic Source Routing (DSR), Ad hoc On Demand Distance Vector (AODV) routing, Temporally Ordered Routing Algorithm (TORA) and Associativity Based Routing (ABR) [4].

B. Routing Protocols:

a. Dynamic Source Routing (DSR) protocol:

Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting computer requests one.

There are 2 major phases:-

Route discovery – uses route request and route reply packets.

Route maintenance–uses route error packets and acknowledgments.

The protocol allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets, for example for use in load balancing or for increased robustness. Other advantages of the DSR protocol include easily guaranteed loop-free routing, support for use in networks containing unidirectional links, use of only "soft state" in routing, and very two hundred nodes, and is designed to work well with even very high rates of mobility. The **advantage** is route maintenance in this protocol is fast and simple, in case of a fatal error in the data-link layer. One of the major **disadvantages** of DSR protocol is an implementing the route discovery process [2]. Source will transmit the RREQ messages to all the neighbouring nodes to find the route to destination. In case the network size is very high and participating nodes are numerous, then there will be a possibility to have so many routes to the destination.

b. Optimized Link State Routing (OLSR) protocol:

The protocol is an optimization of the classical link state algorithm tailored to the requirements of a mobile wireless LAN. The key concept used in the protocol is that of multipoint relays (MPRs). MPRs are selected nodes which forward broadcast messages during the flooding process. This technique substantially reduces the message overhead as compared to a classical flooding mechanism, where every node retransmits each message when it receives the first copy of the message. In OLSR, link state information is generated only by nodes elected as MPRs. Thus, a second optimization is achieved by minimizing the number of control messages flooded in the network. As a third optimization, an MPR node may chose to report only links between itself and its MPR selectors. Hence, as contrary to the classic link state algorithm, partial link state information is distributed in the network [4]. This information is then used for route calculation. OLSR provides optimal routes (in terms of number of hops). The protocol is particularly suitable for large and dense networks as the technique of MPRs works well in this context.

c. Ad Hoc On -Demand Distance vector (AODV):

Mobile nodes in the ad hoc network are dynamic and they use multi-hop routing by using Ad-Hoc On-Demand Distance Vector algorithm. AODV will not maintain the routes unless there is a request for route. Mobile nodes respond to the any change in network topology and link failures in necessary times. In case of the link failures the respective defective nodes are notified with the message, and then the affected nodes will revoke the routes using the lost link. This will help AODV to avoid the Bellman-Ford "counting to infinity" problem and then its operation is known as loop-free. AODV uses Destination Sequence Numbers (DSN) for every route entry. DSN is created by the destination this DSN and the respective route information have to be included by the nodes while finding the routes to destination nodes. Routes with the greatest DSN are preferred in selecting the route to destination [5]. AODV uses the message types Route Request (RREQ), Route Replies (RREP) and Route Error (RERR) in finding the route from source to destination by using UDP user datagram protocol) packets. A typical AODV protocol follows the following procedure while routing.

a) A source node intending to communicate to a destination it generally uses the RREQ constituting the source address and the broadcast ID address to its neighboring nodes to find the route to destination,
b) This broadcast ID is incremented for every new RREQ. Once neighbors notice a destination route it will respond with RREP to the source.
c) If the destination route is not found then it will rebroadcast the RREQ to its corresponding neighboring nodes by incrementing hop count.
d) In this process a node participating in communication may receive the numerous copies of the broadcast packets in the pool of transmissions from all the corresponding nodes. Then the node cross check the broadcast ID of the request if the broadcast ID is new and have not received so far by the particular node then it will process the request if not the node drops down the superfluous RREQ and avoids the rebroadcast.

III. SECURITY SERVICES

The ultimate goals of the security solutions for MANETs is to provide security services, such as availability, confidentiality, integrity, authentication, nonrepudiation, anonymity to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack. There is no single mechanism that will provide all the security services in MANETs. The common security services are described below.

A. Authentication:

Authentication ensures that the access and supply of data is done only by the authorized parties. It is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function is to assure the recipient that the message is from the source that it claims to be from.

B. Availability:

Availability is concerned with the (unauthorized) upholding of resources. A variety of attacks can result in the loss of or reduction in availability. Some of these attacks are amenable to automated countermeasures such as authentication and encryption whereas others require some sort of action to prevent or recover from loss of availability of elements or services of a distributed system. Availability ensures the survivability of network services despite of various attacks.

C. Nonrepudiation:

Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. On the other hand, after sending a message, the sender can prove that the message was received by the alleged receiver.

D. Confidentiality:

Confidentiality ensures that certain information is only readable or accessible by the authorized party. Basically, it protects data from passive attacks. Transmission of sensitive information such as military information requires confidentiality. Routing and packet forwarding information must also remain confidential so that the enemies could never take the advantages of identifying and locating their targets in a battlefield.

Table 1 : Security Attacks And Security Issues On Each Layer In Manet

Layer	Attack	Security Issue
Application layer	Repudiation, data Corruption	Detecting and preventing viruses, worms, malicious codes and application abuses
Transport layer	Session hijacking, SYN Flooding	Authentication and securing end-to-end or point-to-point communication through data encryption
Network layer	Wormhole, blackhole, Byzantine, flooding, resource consumption	Protecting the ad hoc routing and forwarding protocols
Data link layer	Traffic analysis, monitoring, Disruption MAC (802.11), WEP,Weakness	Protecting the wireless MAC protocol and providing link layer security support
Physical layer	Eavesdropping, Jamming, interceptions,	Preventing signal jamming denial-of-service attacks

E. Integrity:

Integrity guarantees that the authorized parties are only allowed to modify the information or messages. It also ensures that a message being transmitted is never corrupted. A connection-oriented integrity service, one that deals with a stream of messages assures that messages are received as sent, with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under integrity service. Thus it addresses both message stream modification and denial of service.

F. Scalability:

Scalability is not directly related to security but it is very important issue that has a great impact on security services. Security mechanisms should be scalable to handle a large network. Otherwise, the newly added node in the network can be compromised by the attacker and used for gaining unauthorized access of the whole system.

IV. ATTACKS IN MANET

A. Passive attacks:

In a passive attack an unauthorized node monitors and aims to find out information about the network. The attackers do not otherwise need to communicate with the network. Hence they do not disrupt communications or cause any direct damage to the network. However, they can be used to get information for future harmful attacks. Examples of passive attacks are eavesdropping and traffic analysis.

B. Active Attacks:

These attacks cause unauthorised state changes in the network such as denial of service, modification of packets, and the like. These attacks are generally launched by users or nodes with authorisation to operate within the network. We classify active attacks into four groups: dropping, modification, fabrication, and timing attacks. It should be noted that an attack can be classified into more than one group. [6]

C. Attacks using Modification:

Modification is a type of attack when an unauthorized party not only gains access to but tampers with an asset. In modification attack, adversaries make some changes to the routing messages, and thus endanger the integrity of the packets in the networks. Since nodes in the ad hoc networks are free to move and Denial of service (DoS) is another type of attack, where the attacker injects a large amount of junk packets into the network. These packets overspend a significant portion of network resources, and introduce wireless channel contention and network contention in the MANET. A routing table overflow attack and sleep deprivation attack are two other types of the DoS attacks. In the routing table overflow attack, an attacker attempts to create routes to nonexistent nodes. Meanwhile the sleep deprivation attack aims to consume the batteries of a victim node. For example, consider the following Fig. 3. Assume a shortest path exists from **S** to **X** and **C** and **X** cannot hear each other, that nodes **B** and **C** cannot hear each other, and that **M** is a malicious node attempting a denial of service attack. Suppose **S** wishes to communicate with **X** and that **S** has an unexpired route to **X** in its route cache. **S** transmits a data packet toward **X** with the source route **S --> A --> B --> M --> C --> D --> X** contained in the packet's header. When **M** receives the packet, it can alter the source route in the packet's header, such as deleting **D** from the source route. When **C** receives the altered packet, it attempts to forward the packet to **X**. Since **X** cannot hear **C**, the transmission is unsuccessful [7, 11].

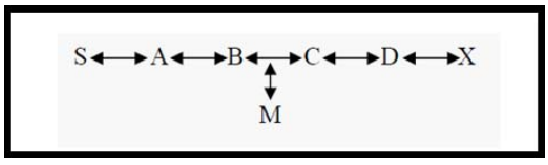

Figure 1: Ad hoc network and a malicious node

D. Attacks Using Impersonation:

As there is no authentication of data packets in current ad hoc network, a malicious node can launch many attacks in a network by masquerading as another node i.e. spoofing. Spoofing is occurred when a malicious node misrepresents its identity in the network (such as altering its MAC or IP address in outgoing packets) and alters the target of the network topology that a benign node can gather. As for example, a spoofing attack allows forming loops in routing packets which may also result in partitioning network. Here we have described the scenario in details [3]. ***A*** can hear ***B*** and ***D***, ***B*** can hear ***A*** and ***C***, ***D*** can hear ***A*** and ***C***, and ***C*** can hear ***B***, ***D*** and ***E***. ***M*** can hear ***A***, ***B***, ***C***, and ***D*** while ***E*** can hear ***C*** and next node in the route towards ***X***. A malicious node ***M*** can learn about the topology analyzing the discovery packets and then form a routing loop so that no one nodes in his range can reach to the destination ***X***. ***M*** changes its MAC address to match ***A***'s, moves closer to ***B*** and out of the range of A.

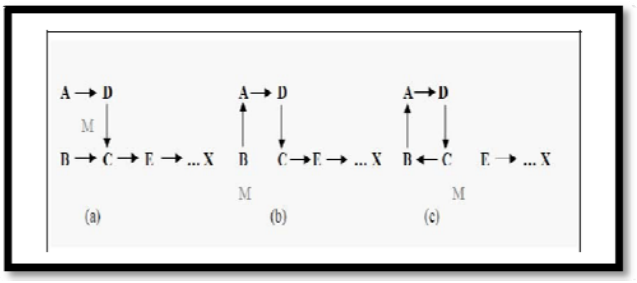

Figure 2: A sequence of events forming loops by spoofing packets.

In the above figure there exists a path between five nodes. ***B*** that contains a hop count to ***X*** which is less than the one sent by ***C***, for example *zero*. Now ***B*** changes its route to the destination, ***X*** to go through ***A*** as shown in the *fig 6(b).* Similarly, ***M*** again changes its *MAC* address to match ***B***'s, moves closer to ***C*** and out of the range of ***B***. Then it sends message to ***C*** with the information that the route through ***C***ontains hop count to ***X*** which is less than ***E***. Now, ***C*** changes its route to ***B*** which forms loop as shown in *fig.* Thus ***X*** is unreachable from the four nodes in the network [8].

E. Attacks through Fabrication:

In *MANET*, fabrication is used to refer the attacks performed by generating false routing messages. Suppose node ***S*** has a route to node ***X*** via nodes ***A***, ***B***, ***C***, and ***D***. A malicious node ***M*** can launch a denial-of service attack against ***X*** by continually sending route error messages to ***B*** spoofing node ***C***, indicating a broken link between nodes ***C*** and ***X***. ***B*** receives the spoofed route error message thinking that it came from ***C***. ***B*** deletes its routing table entry for ***X*** and forwards the route error message on to ***A***, who then also deletes its routing table entry. If ***M*** listens and broadcasts spoofed route error messages whenever a route is established from ***S*** to ***X***, ***M*** can successfully prevent communications between ***S*** and ***X.***

F. Wormhole Attacks:

Wormhole attack is also known as tunneling attack. In wormhole attack, a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through wired link between two colluding attackers or through a single long-range wireless link. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel. Though no harm is done if the wormhole is used properly for efficient relaying of packets but it puts the attacker in a powerful position compared to other nodes in the network, which the attacker could use in a manner that could compromise the security of the network [9].

For example in Fig. 3, **X** and **Y** are two malicious nodes that encapsulate data packets and falsified the route lengths.

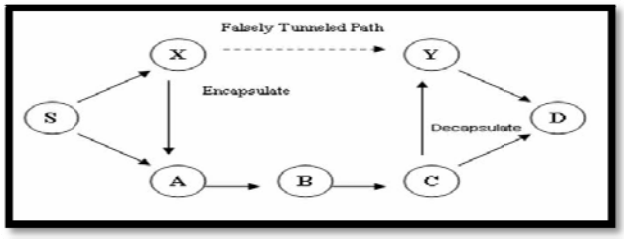

Figure 3: Wormhole attack

Suppose node **S** wishes to form a route to **D** and initiates route discovery. When **X** receives a route request from **S, X** encapsulates the route request and tunnels it to **Y** through an existing data route, in this case {**X --> A --> B --> C --> Y**}. When **Y** receives the encapsulated route request for **D** then it will show that it had only travelled {**S --> X --> Y --> D**}. **X** and **Y** not update the packet header. After route discovery, the destination finds two routes from **S** of unequal length: one is of 4 and another is of 3. If **Y** tunnels the route reply back to **X**, **S** would falsely consider the path to **D** via **X** is better than the path to **D** via **A**.

G. Lack of Cooperation:

Mobile Ad Hoc Networks *(MANETs)* rely on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a *MANET* gets. But one of the different kinds of misbehavior a node may exhibit is selfishness. A selfishness node wants to preserve own resources while using the services of others and consuming their resources [9]. This can endanger the correct network operation by simply not participating to the operation or by not executing the packet forwarding. This attack is also known as the black hole attack [10].

V. CONCLUSION

Mobile Ad Hoc Networks have the ability to setup networks on the fly in a harsh environment where it may not possible to deploy a traditional network infrastructure. Security is an important feature for deployment of MANET. In this paper, we have overviewed the challenges and solutions of the security threats in mobile ad hoc networks. In our study, we present a variety of attacks related to different layers and find that network layer is most vulnerable than all other layers in MANET. This isolation of attacks on the basis of different layers makes easy to understand about the security attacks in ad hoc networks. We focus on the potential countermeasures either currently used in wired or wireless networking or newly designed specifically for MANET.

VI. REFERENCES

[1]. Gurjeet Singh "Security Threats and Maintains in Mobile Adhoc Networks". IJECT Vo l. 2, Issue3, Sept. 2011.

[2]. ShuyaoYu,YoukunZhang,Chuck Song, Kai Chen " A security architecture for mobile Adhoc networks" preceding in Institute of Computing Technology, School of Software, 1999.

[3]. Jun-Zhao "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing" in IEEE communication magazine vol.3 pp. (316-321)2001.

[4]. Ipsita Panda "QoS Parameters Analysis to Improve QoS in MANETs Routing Protocol", International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE) Volume 1, Issue 7, September 2012.page 43-49.

[5]. J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks", Proc. Ninth Int'l Conf. Network Protocols(ICNP), Nov. 2001.

[6]. Sevil Şen, John A. Clark, Juan E. Tapiador "Security Threats in Mobile Ad Hoc Networks" availablewww.users.cs.york.ac.uk/~jac/Published Papers/SecurityThreats%20in%20MANEs.pdf.

[7]. Kamanshis Biswas and Md. Liakat Ali "Security Threats in Mobile Ad Hoc Network" Master Thesis,Computer Science.Available: http://studentyogi.com/wp-content/uploads/2010/02/Security-threats-in-Mobile-Ad-Hoc-Network.pdf

[8]. J-P. Hubaux, L. Buttyan and S. Capkun: "The Quest for Security in Mobile Ad Hoc Networks, Proceedings of the 2nd ACM MobiHOC, 2001".

[9]. L. Zhou and Z. Hass, "Securing Ad Hoc Networks" , IEEE network, vol. 13, no.6 pp24-30, 1999.

[10]. P. Papadimitratos, Z. Haas, "Secure routing for Mobile Ad Hoc Networks", Proceedings of CNDS, 2002.

[11]. S. Bonum, J.Ben-Othman, "Data Security in Ad Hoc Networks Using Multipath Routing ", Proc. 14th IEEE International Symposium on Personal, Indoor and Mobile Radio Communication, 2003.

Short Bio Data for the Author

Ms. Ipsita Panda is a Sr. lecturer in the Department of Computer Science and Engineering at Synergy institute of engineering and Technology (S.I.E.T), Dhenkanal, Odisha, India. She has more than five years of teaching experience. She has authored number of papers which have been published in both national and international journals. Her research interest is in the area of Mobile Adhoc Network and wireless sensor network.