A Comprehensive Review of Security Issues in Manets

Saloni Sharma
Scholar
RIMT, Mandigobindgarh,
Mtech (CSE)

Anuj Kumar Gupta
Head of the Department
RIMT, Mandigobindgarh
Mtech (CSE)

ABSTRACT
During the past few years the emergence of Mobile adhoc networks (MANETS) and its various uses in different fields of communication has been observed. It has led to an instant growth in wireless technology. Many routing protocols have been designed and implemented for proper functioning of mobile adhoc networks. The prime objective of these routing protocols is to provide a specific and much effective route in a network. AODV which is a reactive protocol for MANETs is considered as the most effective routing protocol by Internet Engineering Task force. Due to MANET's infrastructure less nature, security is a prime issue to be maintained. This paper submits the brief introduction about mobile adhoc networks, their counter attacks, different routing protocols and their consecutive security measures.

Keywords
MANETs, Security, Routing Protocol, AODV, SAODV, ARAN. SEAD, Ariadne.

1. INTRODUCTION
MANETs are networks which are infrastructure less. In these networks there is no fixed topology because the nodes which communicate with each other are always mobile. Due to its mobile nature they offer great flexibility, higher throughput, low operating cost and better coverage. MANETs are largely used in military, rescue operations and even in mobile phones using Bluetooth. As the popularity of MANETs is increasing with the increase in scientific techniques, one of the biggest threats that still reside over MANETs is security. Due to its topology less nature security has become one of its main issue. Different challenges faced by MANETs are-

Confidentiality: Only the authenticated users must have access to the sent data.

Integrity: Data must not be transformed or changed in any form while it is sent from one network to another.

Authentication: Every node must authenticate themselves, so that no legitimate node interferes in the network.

Non-Repudiation: Sender or the receiver should not later deny the sending or receiving of message.

Since MANETs has been in an active research area and in recent years many routing protocols have been introduced. These protocols are divided into 3 categories- reactive, proactive and hybrid. The reactive routing protocols set up network and its routing information only on demand. It includes DSR, AODV etc. The proactive routing protocols are those in which every node maintains its own routing table including the entire topology of the network. Routing information is flooded in the entire network. It includes DSDV, HSR etc. Hybrid routing protocols are the combination of both proactive and reactive routing protocol. It includes ZRP etc.

2. WEAKNESSES OF MANETs
Since nodes in mobile network can move freely, the network tends to change its topology very frequently. This mobile nature of the nodes may create many security and other issues in Manets –

- *Lack of Centralized Management* - Since Manets form a random network and even the nodes are mobile so there is no centre management. Due to lack of centralized management the detection of attacks is very difficult.
- *Infrastructure less* - Manets infrastructure less nature brings difficulty in detecting any malicious node or faults in the network.
- *Dynamic Topology* – Since Manets have a dynamic topology because the nodes are ever changing this may weaken the relationship among nodes.
- *Packet Loss* – There are many reasons of packet loss problem in Manets. Packet loss may happen due to mobility of nodes, bit rate error, due to interference.
- *No network boundary* – Since Manets have no network boundary because the nodes are movable this may lead to increase in number of attacks on them. Any node may enter the network and may hinder the network communication.
- *Mobile Nodes*- At times the mobile nature of nodes may even create network error. Since nodes can freely join or leave a network so it is easy for nodes to behave maliciously.
- *Scalability* – Due to mobility of network the scale of the network is changing all the time.
- *Variation in nodes* – Each node has different transmission and receiving capabilities. In addition each mobile node has different software/hardware configurations which cause trouble in operating in a network. [1]
- *Security* – It is one of the major issue in mantes. All major networking tasks such as routing and packet formatting are done by nodes itself which are mobile [9]. Any attacker can easily attack on the network and can acquire the data.
- *Resource Availability* – For manets providing secure communication in such a challenging environment where the network is mobile and is vulnerable to attacks requires various resources and architectures [9].

3. ATTACKS ON MANETs
There are different types of attacks which are vulnerable to manets and which are active at different layers of network. Few of them are discussed below –

1. Blackhole Attack – The black hole attack is active at the network layer. It has two properties [2] First is that the attacker sends fake routing information, claiming that it has the valid route to the destination, due to which other nodes in the network route the data packets through the malicious one. Second, the malicious node targets the routing packets, drops them instead of normally forwarding them.

2. Wormhole Attack – It is another network layer attack where the attacker forms a tunnel from one location in the network to another. All the routing packets are tunneled, this tunnel is referred to as a wormhole.

3. Byzantine Attack – In this attack an intermediate node or a set of intermediate nodes work in collusion and carry out attacks such as creating routing loops, forwarding packets on non – optimal path which results in disruption and degradation of the routing system.[2]

4. Snooping – Snooping means illegal access of anyone's personal data. Snooping is just not limited to gaining access to the data, but also includes observance of other's activities.

5. Routing Attacks – These types of attacks include attacks related to the routing table which are routing table overflow, routing table poisoning, packet replication, rushing attack etc. All these attacks include the illegal access of the routing table, entries in the routing tables and the information carried by the routes.

6. Resource consumption Attack – This type of attack involves the illegal resource consumption of the network which includes battery life or by unnecessary forwarding packets to the malicious nodes.

7. Session hijacking Attack – Session hijacking attack is the attack which is active in the transport layer. The first step of the attacker is to spoof the IP address of the source node and determine its sequence number and hence perform denial of service attack on the source. In this way the attacker tends to behave as the system and continues the session with the target. [2]

8. Denial of service – DOS is one of the most studied attack as it can be launched at any layer of the network. In this attack the communication signal is jammed which disrupts the normal communication process. It can be carried out in many ways. It can be achieved by transmitting false routing packets or by flooding the routing packets to any intermediate node so that normal communication is no longer done. This attack basically hinders the availability of a node or even the entire network.

9. Cryptographic attacks – Cryptography provides security to the network and is also considered as a powerful tool to maintain confidentiality and authentication of the information which is to be send. It also hinders the illegal access of data by attackers by its key management system .These types of attacks include digital signature attack, pseudorandom number and hash collision attacks.

4. ROUTING IN MANETs

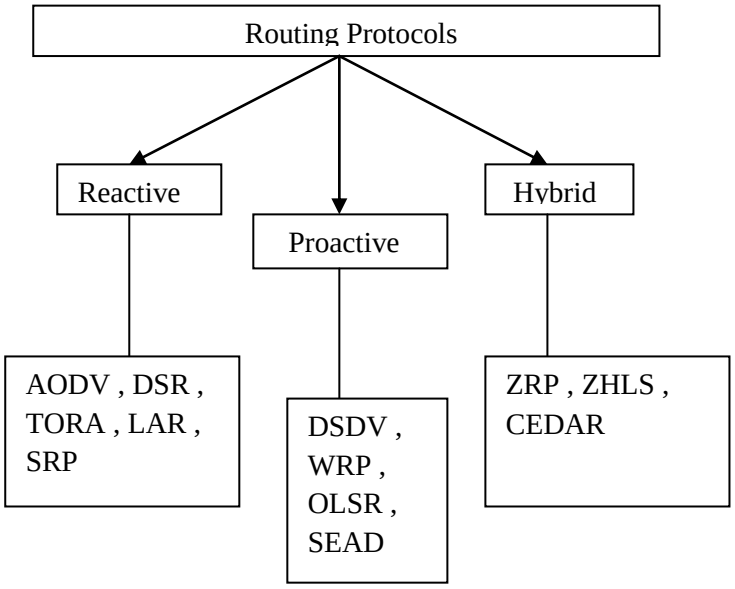

Fig 1: Different routing protocols in manets

A routing protocol specifies how the communication is carried between routers. [7] The choice of the route being selected is done by the routing algorithm. As in Fig 1 it is clearly shown that the routing protocols are divided into 3 categories Reactive protocols, Proactive protocols and Hybrid protocols.

Reactive protocol – Reactive protocols are also called on - demand protocols. They are named on – demand because they maintain or discover route only on demand [7]. A control message is flooded to the routes to discover the appropriate route. It only establishes the route when any node in the network wants to send a message or a packet to another node in the network. The main advantage of these protocols are that it reduces the routing table overflow and its major disadvantage is that due to its on demand nature while route discovery a longer delay is been found. The example of this type of protocol are DSR (dynamic source routing), AODV (ad hoc on demand distance vector routing), LAR (location aided routing), TORA (temporally ordered routing algorithm).

Proactive protocol – Proactive protocols are also named as table driven routing protocol. They maintain the routing table of the entire network constantly. Each node has to maintain one or more tables to store routing information and response to changes in network topology by broadcasting and propagating. [9] The routing tables are constantly updated whenever the network topology changes. Each node in the network sends a broadcast message to the entire network if there is any change in the network topology. This feature of maintaining routing entries of the entire network may affect the routing table but it provides the actual information of the entire network. For very large network the proactive routing protocols may not be recommended because they maintain entries of each node in the network which causes more bandwidth consumption and overload to routing table. The examples of proactive routing protocol are DV (distance vector), DSDV (destination sequence distance vector), OLSR (optimised link state routing), and WRP (wireless routing protocol) which is an enhanced version of DSDV.

Hybrid protocols – As according to the name hybrid routing protocols are a combination of both reactive and proactive routing protocols. Basically to overcome the shortcomings of reactive and proactive routing protocol the hybrid is used. It uses the route discovery and on demand mechanism of reactive routing protocol and the routing table management mechanism of proactive routing protocol. In hybrid routing protocol a large network is divided into zones. The routing inside the zones is done by using reactive approach and the routing outside the zone is done using reactive approach. [12] It is the most effective and appropriate routing protocol amongst all. The examples of hybrid protocols are ZRP (zone routing protocol), ZHLS (zone based hierarchical state).

4. COMPARISON OF ROUTING PROTOCOLS

Table 1. Comparison of routing protocols

Parameters	**Reactive Protocol**	**Proactive Protocol**	**Hybrid Protocol**
Routing Philosophy	Flat	Flat/ Hierarchial	Hierarchical
Routing Scheme	On demand	Table driven	Combination of both
Routing Overhead	Low	High	Medium
Latency	High due to flooding	Low due to routing tables	Inside zone low outside similar to Reactive protocols
Scalability level	Not suitable for large networks	Low	Designed for large networks

5. AODV ROUTING PROTOCOL

AODV is one of the most effective routing protocol which use routing messages between mobile computers. AODV stands for Adhoc On Demand Distance Vector routing protocol which is a reactive routing protocol. They enable nodes to communicate with each other which cannot communicate directly. Out of all other routing protocols AODV is chosen because it is simple and it's on demand nature does not over-flow the network and also the routing table. AODV work with the help of control messages to find a route to the destination. AODV is capable of doing both unicast and multicast routing. As the name suggests AODV uses an on demand approach that is, it only establishes a route when it is required by the source node for transmitting data packet.

5.1 Working of AODV

To initiate routing AODV uses its 3 message system. The neighbour nodes communicate and search for their route using these messages. The 3 messages are-

RREQ*:* Route Request. This message is flooded to all the next neighbours of the source node. When the source node desires to send a message it initiates the path by sending RREQ to all the neighbours. Neighbours are the next node corresponding the source node, which then forwards RREQ to its neighbours until they reach the destination which replies using RREP message. As this RREQ message travels from source node to destination node, each node receives the information of that address from which it was received. As shown in figure 1 below. The figure contains a network of 5 nodes in a wireless network which are numbered in the circles. Node 1 is the source node which has to send data to the destination node which is node 5, both source node and the destination node are specified with grey colours. Since node 2 and node 3 are the next neighbours of source node 1, it sends RREQ (which is specified with the bold line) to both node 2 and node 3 as it cannot directly communicate with node 5. The RREQ message contains several information which includes the source, the destination, the lifespan of the message and the sequence number which is the unique id. When node 2 and node 3 receives the RREQ message they will send a RREP back to node 1. Now since node 2 has a direct link to destination node 5 it replies to RREQ by sending a RREP.

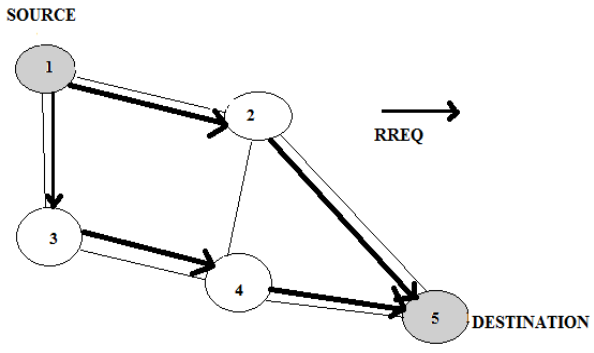

Fig 2: Source 1 sending RREQ to neighbors 2 and 3 and further to respective nodes

RREP - Route Reply messages. When the node is the requested destination or it has any route to the destination it sends back RREP to the source node. When RREP reaches the source node a route is established between the source node 1

and the destination node 5. Once the route is established between node 1 and node 5 the two nodes can communicate with each other. Fig 2 depicts the two messages RREQ and RREP. It shows the exchange of messages between source node and destination node.

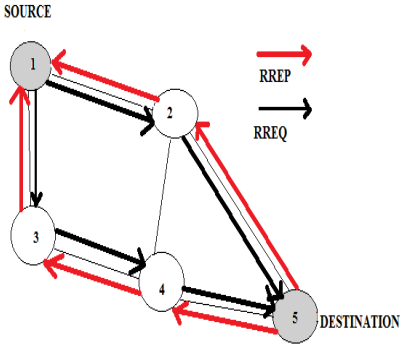

Fig3: Destination 5 sending RREP to source 1 through other nodes

RRER - Route Error is the message which is generated throughout the network whenever there is a link breakage or any error between the source and the destination. Whenever there is an unreachable link or link breakage between the source to the destination route RRER message is generated to the source node. In Fig 3 we can see that how link 4 to 5 is broken and how the node 4 sends back the RRER message to further nodes to the source node 1.

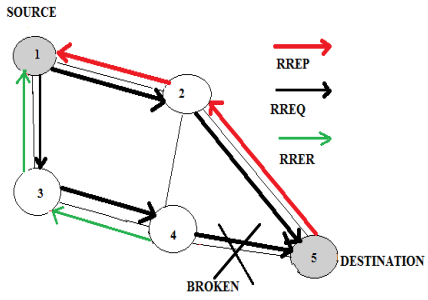

Fig 4: RRER message is sent from node 4 to source node 1 since node 4 to 5 is broken

5.2 Table Management

While the routing process the routitng tables entries are being filled. Destination IP address is filled. Destination Sequence number which are unique numbers, which increment themselves each time the node sends any type of message so that the fresher node is easily identified. Next hop entry which could be either the destination node or any intermediate node. Hop count which tells the number of hops from source. Lifetime which is the time for which the route is valid. Rouitng flags which indicates the state of the route valid, not valid or repair.

6. METHODS TO SECURE ROUTING PROTOCOLS

AODV does not take security into account: AODV messages are neither encrypted nor authenticated nor integrity protected, and basically are always assumed as trusted. Many kinds of attacks are possible, based on the possibility to forge packets and on the distributed and uncontrolled nature of the network. Due to these attacks many security techniques have been implemented on AODV. Those techniques are discussed below –

SAODV – Secure AODV is an extension to AODV routing protocol. It is proposed by M. Zapata and N. Asokan. It is based on public key cryptography and hash algorithm. SAODV routing messages (RREQs, RREPs, and RERRs) are digitally signed, in order to guarantee their integrity and authenticity. [10] There is a key management system which makes it possible for each node to obtain public keys from the other nodes of the network. How this is achieved depends on the key management scheme. Two mechanisms are used to secure the AODV messages: digital signatures to authenticate the non-mutable fields of the messages, and hash chains to secure the hop count information (the only mutable information in the messages). For the non-mutable information, authentication is performing in an end-to-end manner, but the same kind of techniques cannot be applied to the mutable information. To preserve the collaboration mechanism of AODV, SAODV includes a kind of delegation feature that allows intermediate nodes to reply to RREQ messages. This is called the *double signature*: when a node A generates a RREQ message, in addition to the regular signature, it can include a second signature, which is computed on a fictitious RREP message towards intermediate node itself.

A-SAODV – Adaptive secure AODV is another approach to secure AODV routing protocol from attacks and from malicious users. It is based on the AODV-UU implementation by Uppsala University. Unlike AODV-UU, A-SAODV is a multithreaded application. [6,] In A-SAODV, there are two execution threads: one carries the cryptographic operations and the other to all other functions (routing message processing, SAODV routing table management, timeout management, SAODV message generation, and data packet forwarding). The two threads communicate via a first input first output (FIFO) queue containing all the messages that must be signed or verified. [6]

SEAD – Secure efficient Adhoc distance vector is a proactive routing protocol. It is another routing protocol which is secure as it is based on one – way hash functions to provide authentication. Each nodes contains its individual hash chains which is separated into segments to prevent an attacker to forge sequence numbers. [3]

ARIADNE - It is another On-Demand Routing Protocol presented by Hun, Johnson & Perrig based on DSR. It is a secure on-demand routing protocol that can authenticate messages using one of the three ways: shared secrets between each pair of nodes, shared secrets between communicating

nodes combined with broadcast authentication, or digital signature. [3] The protocol is based on two steps- to verify that the route is authentic and to check that no node is missing from the route. However Ariadne is vulnerable to wormhole attack.

ARAN - It is proposed by Dahill. Authenticated Routing for adhoc networks detects the attacks from malicious nodes and also protects the network from forged actions. It uses cryptographic certificates for authentication purpose. The certificate includes the IP of the node, the public key of the source node, a timestamp of the time at which the certificate was created and another timestamp of the time at which the certificate expires. This is the first step which is covered. After the successful completion of the first step second step is preceded. It discovers the shortest path to the destination. It is an on- demand routing protocol. It is successful in protecting the network against impersonation attack but is vulnerable to wormhole attack. [3]

7. RELATION BETWEEN ATTACKS AND PROTOCOLS

Relation between attacks and different security protocols is shown in table 2.

Table 2. Relation between attacks and protocols

PROTOCOLS → / **ATTACKS**	**SAODV**	**SEAD**	**Ariade**	**ARAN**
Blackhole	No	Yes	No	No
DOS	Yes	Yes	Yes	Yes
Spoofing	No	Yes	No	No
Wormhole	Yes	Yes	Yes	Yes

8. CONCLUSION

In this paper different features of mobile adhoc networks, attacks on them and their respective routing protocols are discussed. Since AODV is considered as one of the most effective routing protocol so its working is studied and discussed in detail. Due to manets mobile and infrastructureless nature they are vulnerable to different types of attacks. Many security protocols have been designed to meet all the security needs. The study can be conluded by noting that not even a single security measure can insure the complete security of mobile adhoc networks. Each security protocol has one or the other flaw. So, more deep study needs to be done on the security aspect of mobile adhoc networks.

9. ACKNOWLEDGMENTS

The authors sincerely thank to their institution for giving this opportunity to work and providing environment to study and for research. The authors wish to thank the reviewers and editors for their valuable suggestions and expert comments that help improve the contents of paper.

10. REFERENCES

[1] imrich chlamtac , marco conti, jennifer j.-n. liu “mobile ad hoc networking: imperatives and challenges” in proceedings of 2003 elsevier

[2] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Carde “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks” in proceedings of WIRELESS/MOBILE NETWORK SECURITY Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. – - – °c 2006 Springer.

[3] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani “A Survey of Secure Mobile Ad Hoc Routing Protocols” in proceedings of ieee communications surveys & tutorials, vol. 10, no. 4, fourth quarter 2008.

[4] Davide Cerri and Alessandro Ghioni “Securing AODV: The A-SAODV Secure Routing Prototype” in proceedings of IEEE Communications 0163-6804/08/$25.00 © 2008 IEEE.

[5] Anuj K. Gupta “Secure Routing Techniques for mobile adhoc networks” in proceedings of 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6–7March 2009.

[6] Mohd Anuar Jaafar and Zuriati AhmadZukarnain “Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment” in proceedings of European Journal of Scientific Research ISSN 1450-216X Vol.32 No.3 (2009), pp.430-443.

[7] R.Devi, B.Sumathi, T.Gandhimathi, G.Alaiyarasi “Performance Metrics of MANET in Multi-Hop Wireless Ad Hoc Network Routing Protocols” in proceedings of International Journal of Computational Engineering Research (IJCER) ISSN: 2250-3005 National Conference on Architecture, Software system and Green computing.

[8] G. S. Mamatha and Dr. S. C. Sharma “analyzing the manet variations, challenges, capacity and protocol issues” in proceedings of International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.1, August 2010.

[9] Priyanka Goyal, Vinti Parmar, Rahul Rishi “ MANET: Vulnerabilities, Challenges, Attacks, Application” in proceedings of IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[10] Anil Suryavanshi and Dr. Poonam Sinha “Efficient techniques for saodv in mobile adhoc network” in proceedings of Journal of Global Research in Computer Science, Volume 2, No. 8, August 2011.

[11] Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma "Review of Various Routing Protocols for MANETs" in proceedings of International Journal of Information and Electronics Engineering, Vol. 1, No. 3, November 2011.

[12] Robinpreet Kaur & Mritunjay Kumar Rai "A Novel Review on Routing Protocols in MANETs" in proceedings of Undergraduate Academic Research Journal (UARJ), ISSN : 2278 – 1129, Volume-1, Issue-1, 2012.

[13] Pankaj Sharma , Yogendra Kumar Jain "Trust based secure aodv in manet" in proceedings of *Journal of Global Research in Computer Science* Volume 3, No. 6, June 2012.