Intl J Engg Sci Adv Research 2015 Sep;1(3):46-51

A Survey Paper on Secure Mobile Ad-hoc Network

Vikas Yadav
Harcourt Butler Technological Institute, Kanpur
vikas.yadav.cs@gmail.com,

Rohit Saxena
Department of CSE
Rama University, Kanpur,India
rohitsaxena9@gmail.com

Amit Gupta
Dr Ambedkar Institute of Technology Handicapped, Kanpur
amit.kan91@gmail.com

Abstract: **A Mobile ad hoc Network (MANET) is a self-organizing, infrastructure-less, multihop network. Communicating nodes in a Mobile ad hoc Network usually seek the help of other intermediate nodes to establish communication channels. This wireless and distributed nature of MANET poses a great challenge to system security designers. Most research efforts have been focused on specific security areas, such as establishing trust infrastructure, securing routing protocols, or intrusion detection and response etc. There are several security issues in Mobile Ad hoc Network having their own advantages and disadvantages. In this review paper, we review some security issues in MANET as well as their current solutions**.

Keywords: MANET (Mobile Ad-hoc Network), DSR (Dynamic Source Routing), AODV (Ad-hoc On-demand Distance Vector Routing), MAC (Message Authentication Code), SAODV (Secure AODV), ARAN (Authenticated Routing for Ad-hoc Networks), RREQ (Route Request), RREP (Route Reply).

I. Introduction

A Mobile ad hoc Network (MANET) is a system of independent wireless mobile nodes without any support of fixed infrastructure. In MANET there is no router or access point (AP) in the network. It's just a collection of mobile node, where each node can work as sender, receiver and router. The mobile nodes that are in radio range of each other can directly Communicate, if the nodes are not within the radio range they can communicate with each other using multi-hop routing. Every packet that comes in network is delivered to its destination by the help of other nodes in sender's vicinity. The characteristics of these networks are as following:

- In MANET Wireless link between nodes is highly vulnerable because of the continuous movement of nodes.
- The topology of MANET is highly dynamic because of the movement of nodes. It causes frequent change in routing information at every node.
- Because of the moving nature of nodes, all nodes operate on battery so there is a need of energy efficient operations in MANET.
- It operates on same bandwidth as WLAN (2.4 GHz ISM band).

With the advancement of wireless technology, MANET systems are gaining its ground day by day. There are certain advantages of MANET which includes, infrastructure-less structure due to which these networks can be set up at any place and any time. They provide access to information and services regardless of geographic position. Applications of MANETs include:

- Battle field applications (Military and Police Exercise)
- Disaster and Rescue works
- Civilian applications like an outdoor meeting or an ad hoc classroom
- Mine cite operations

II. Security Issues In Manet

Before Going to the details of security solutions of MANET we have to look for how secure is MANET? In this section we discuss various vulnerabilities that exist in the MANET.

A. *Vulnerabilities of the Mobile Ad Hoc Net- works*

Since MANET is far vulnerable than the traditional wired network due to its different features like:

- Open Architecture: We can't precisely define boundaries of MANET, nodes may join and leave network any time. Due to this open architecture attacker can communicate with other nodes if it is in range of node.
- Distributed Control: Traffic cannot be monitored from a centralized point instead the control is distributed at each node. The detection becomes more difficult when the advisory changes the attack pat- tern and the target of the attack.
- Limited Energy Resource: In MANET alternate power sources are assumed to be absent. The adversary can sent huge traffic to the target node. The target node may be continuously busy in handling these packets; this will cause the battery power to be exhausted.
- Cooperative Operations: The operations (e.g. route discovery, packet forwarding, route maintenance etc.) in MANET are cooperative in nature. Selfish nodes may not cooperate in running such common algorithms

- Changing Scale: In MANET it is difficult to predict the number of nodes in network at some future point. Protocols designed for MANET Must is Compatible to scalability.

B. *Attacks in Mobile Ad Hoc Networks*

There are numerous kinds of attacks which are possible in MANET but as in MANET there is no infrastructure all nodes are involved in routing. So, routing is the area to emphasize upon if we want to secure the MANET. Such vulnerabilities fall into two categories:

1) Routing Attacks: The family of routing attacks refers to any action of advertising routing updates that does not follow the specifications of the routing protocol. The specific attack behaviors are related to the routing protocol used by the MANET. For example, in the context of DSR, the attacker may modify the source route listed in the RREQ or RREP packets by deleting a node from the list, switching the order of nodes in the list, or appending a new node into the list. When distance vector routing protocols such as AODV are

Claiming falsi fied short distance information); the attacker attracts traffic and can then discard it [2].

- Gray hole Attack: It is a special case of a black hole; an attacker could create a Gray hole, in which it selectively drops some packets but not others, for example, by forwarding routing packets but not data packets [2].
- Wormhole Attack: In a wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. For tunneled distances longer than the normal wire- less transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive sooner than other packets transmitted over a normal multi-hop route [3]. For Example, when used against an on-demand routing protocol such as DSR or AODV, a powerful application of the wormhole attack can be mounted by tunneling each ROUTE REQUEST packet directly to the target node of the REQUEST. This attack prevents any node from discovering routes more than two hops long. Periodic protocols are also vulnerable to this kind of attack. For example, OLSR and TBRPF use HELLO packets for neighbor detection, so if an attacker tunnels to B all HELLO packets transmitted by A and tunnels to A all HELLO packets transmitted by B, then A and will believe that they are neighbors, which would cause the routing protocol to fail to find routes when they aren't actually neighbors [2].

2) **Packet Forwarding Attacks**: It is possible for a malicious node to correctly participate in the route discovery phase but fail to correctly forward data packets. The security solution should ensure that each node indeed forwards packets according to its routing table [1].

used, the attacker may advertise a route with a smaller distance metric than its actual distance to the destination, or advertise routing updates with a large sequence number and invalidate all the routing updates from other nodes [1].

Routing Attacks either could be a Routing-disruption attacks, In which the attacker attempts to cause legitimate data packets to be routed in dysfunctional ways or it could be a Resource-Consumption Attacks, In Which the attacker injects packets into the network in an attempt to consume valuable network resources such as bandwidth or to consume node resources such as memory (storage) or computation power. From an application-layer perspective, both attacks are instances of a denial-of-service (DoS) attack [2]. Few attacks under this category are-

- Black hole Attack: An attacker might create a routing black hole, which attracts and drops data packets. An attacker creates a black hole by distributing forged routing information (that is,

III. Security Requirements In Magnet

It is necessary to find out how one can judge MANET is secure or not or we can say that what should be covered in the security criteria for the MANET when we want to inspect the security state of the MANET. Some of the basic securities are as below:

- Availability: A node should maintain its ability to provide all the designed services regardless of the security state of the network. This property is basically challenged during the DoS Attack. For Example, unnecessary transmission of RREQ and RREP packets should be prevented.
- Integrity: Integrity guarantees for the no modification or altering of the transmitted message. It can be compromised in only two ways malicious altering and accidental altering. For Example, the hop-count or metric field in routing packet should not be modified by intermediate node.
- Confidentiality: Confidentiality means that certain information is only accessible to those who have been authorized to access it. For Example message should be readable by receiver only.
- Authenticity: It provides assurance that participants in communication are genuine and not impersonators. It is necessary for the participants to provide their identities as what they have claimed. E.g. signing a message could provide authentication.

- Non-repudiation**:** It ensures that the sender and the receiver of a message cannot disavow that they have ever sent or

Layer	Security issues
Application layer	Detecting and preventing viruses, worms, malicious codes, and application abuses
Transport layer	Authenticating and securing end-to-end communications through data encryption
Network layer	Protecting the ad hoc routing and forwarding protocols
Link layer	Protecting the wireless MAC protocol and providing link-layer security support
Physical layer	Preventing signal jamming denial-of-service attacks

Fig. 1. Security Requirement at Different layers [1]

Useful when we find out some abnormal behavior of some nodes.

- Authorization: This property assigns different access rights to different types of users. For example a network management can be performed by network administrator only [4].
- Anonymity: It means that all the information which is used to identify the owner or any node should be kept secret and should not be disclosed among other nodes. The basic requirements that are needed to be achieved to ensure the security of MANET in the form of protocol stack are shown in fig. 1.

IV. Security Solutions In Magnet

As in the previous section we have introduced several well known attack types on MANET now in this section we discuss some popular security schemes that aim to handle different kind of attack.

Assumption in following solutions is-

1. All nodes in the network are having its public and private keys distributed to it.
2. All nodes have access to CA (Certificate Authority) and having its certificate and CRL (Certificate Revocation List) updated.

A. Packet Leashes: A Defense against Wormhole Attacks

Packet Leashes is a general mechanism for detecting and thus defending against wormhole attacks. A leash is any information received such a message, which is that is added to a packet designed to restrict the packet's maximum allowed transmission distance. Here are two types of leashes geographical leashes and temporal leashes.

1) Geographical Leashes: To construct a geographical leash, in general, each node must know its own location and all nodes must have loosely synchronized clocks. When sending a packet, the sending node includes in the packet its own location, ps, and the time at which it sent the packet, it's; when receiving a packet, the receiving node compares these values to its own location, pr, and the time at which it received the packet, tr. If the clocks of the sender and receiver are synchronized and v is an upper bound on the velocity of any node, then the receiver can compute an upper bound on the distance between the sender and itself, dsr. Specially, based on the time stamp ts in the packet, the local receive time tr, the maximum relative error in location information _, and the locations of the receiver pr and the sender ps, then dsr can be bounded by dsr _k ps □ pr k +2v:(tr □ ts + _) + _. A regular digital signature scheme, e.g., RSA, or other authentication technique, can be used to allow a receiver to authenticate the location and time stamp in the received packet [3].

2) Temporal Leashes: To construct a temporal leash, in general, all nodes must have tightly synchronized clocks, such that maximum difference between any two nodes' clocks is _. The value of the parameter must be known by all nodes in the network, and for temporal leashes, generally must be on the order of a few microseconds or even hundreds of nanoseconds. This level of time synchronization can be achieved now with off-the-shelf hardware based on LORAN-C, WWVB or GPS. To use temporal leashes, when sending a packet, the sending node includes in the packet the time at which it sent the packet, ts; when receiving a packet, the receiving node compares this value to the time at which it received the packet, tr. The receiver is able to detect if the packet travelled too far, based on the claimed transmission time and the speed of light. Alternatively, a temporal leash can be constructed by instead including in the packet an expiration time, after which the receiver should not accept the packet; based on the allowed maximum transmission distance and the speed of light, the sender sets this expiration time in the packet as an offset from the time at which it sends the packet. A regular digital signature scheme or other authentication technique can be used to allow a receiver to authenticate a time stamp or expiration time in the received packet.

B. Secure Routing in Mobile ad hoc Network

There are three cryptographic primitives widely used to authenticate the content of messages exchanged among nodes.

- HMAC (message authentication codes): If two nodes share a secret symmetric key K, they can efficiently generate and verify a message authenticator hK() using a cryptographic one-way hash function h. However, an HMAC can be verified only by the intended receiver [1].
- Digital Signature: Digital signature is based on asymmetric key cryptography (e.g., RSA), which involves much more computation overhead in signing/decrypting and verifying/encrypting operations.
- One-way HMAC Key Chain: A one-way hash chain is built on a one-way hash function. Like a normal hash function, a one-way hash function H maps an input of any length to a fixed-length bit string. Thus, H: f0; 1g? ! f0; 1g_, where _ is the length in bits of the hash function's output. The function H should be simple to compute yet must be computationally infeasible in general to invert. To create a one-way hash chain, a node chooses a random x 2 f0; 1g_and computes the list of values h0; h1; h2; h3; _ _ _ ; hn

where h0 = x, and hi = H(hi□1) for 0 < i _ n,

for some n. The node at initialization generates the elements of its hash chain using this recurrence, in order of increasing subscript i; over time, it uses certain elements of the chain to secure its routing updates[2].Here is the secure ad hoc routing mechanism proposed by Researchers-

1) Secure Source Routing: Source Routing protocols such as DSR, the main challenge is to ensure that each intermediate node cannot remove existing nodes from or add extra nodes to the route. The basic technique is to attach a per-hop authenticator for the source routing forwarder list so that any altering of the list can be immediately detected (or after the key is disclosed for HMAC key-chain-based authentication). A secure extension of DSR is Ariadne. It uses a one-way HMAC

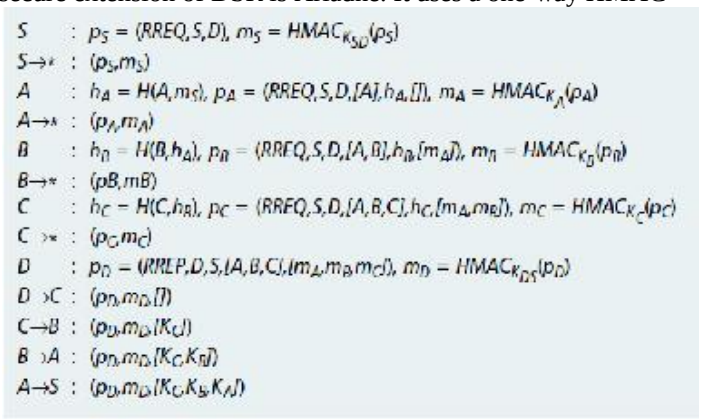

Fig. 2. Ariadne: A Secure Extension of DSR [1]

key chain (i.e., TESLA) for the purpose of message authentication. Through key management and distribution, a receiver is assumed to possess the last released key of the sender's TESLA key chain. Take the following example for an illustration. The source node S uses source routing to connect to the destination D through three intermediate nodes A, B, and C. The protocol establishes a hash chain Fig. 2.

Ariadne: A Secure Extension of DSR [1] at the destination, H(C; H (B; H (A; HMACKSD(S; D)))), where HMACKSD (M) denotes message Ms HMAC code generated by a key shared between S and D. The well known one-way hash function H authenticates the contents in the chain, and HMACKSD(S; D) authenticates the source-destination relation. The propagation of the route request (RREQ) and route reply (RREP) messages is described in Fig. 2, where * denotes a local broadcast and HMACKX (:) denotes HMAC code generated on node X. At the destination, D can compute mS because information of pS is contained in pC. D dynamically computes hCs value according to the explicit node list embedded in pC, then compares this hC to the one embedded in pC for forgery detection. At the RREP phase, there is no need to generate separate authentication code for every RREP packet. By trapdoor commitment, any forwarder X already committed the one-way function outputs mX = HMACKX (:) at the RREQ phase; then at the RREP phase the commitment mX! KX is fulfilled by revealing key KX [1].

2) Securing AODV: For distance vector routing protocols such as DSDV and AODV, the main challenge is that each intermediate node has to advertise the routing metric correctly. For example, when hop count is used as the routing metric, each node has to increase the hop count by one exactly. A hop count hash chain is devised so that an intermediate node cannot decrease the hop count in a routing update. [1] Researchers have designed two protocols to secure AODV (Ad-hoc On-demand Distance Vector) routing protocols-

- Authenticated routing for ad hoc

networks (ARAN): Each node has a certificate signed by a trusted authority, which associates its IP address with a public key. ARAN is an on demand protocol, broken up into route discovery and maintenance.

- Route Discovery**:**

To initiate a route discovery, the initiator (e.g. S) broadcasts a signed ROUTE REQUEST packet that includes the target (e.g. D), its certificate (certS), a nonce N, and a time-stamp t. The nonce and time-stamp together ensure freshness when used in a network with a limited clock skew. Each node that forwards this REQUEST checks the signature or signatures. In our example, node C checks node B's certificate certB, and then checks the signature on the outer message. C then verifies the certificate certS for initiator S and uses the key in the certificate to verify the signature on the REQUEST. If the signatures (or signature, when the packet is directly received from the initiator) are valid,

the forwarding node removes the last forwarder's signature and certificate (if applicable), signs the original REQUEST, and includes its own certificate. The node then broadcasts the REQUEST. In the example, node C removes node Bs signature, signs the resulting REQUEST, and includes its own certificate. Node C then broadcasts the REQUEST. When the first ROUTE REQUEST from a route discovery reaches the target, the target signs a ROUTE REPLY and sends it to the node from which it received the REQUEST. In our example, the target D returns a signed ROUTE REPLY to the previous hop C. The ROUTE REPLY is forwarded in much the same way as the REQUEST, except that each node unicast the REPLY to the node from which it received the REQUEST. In particular, each node receiving a REPLY checks the signature or signatures. In our example, node B checks node Cs certificate certC, then checks the signature on the outer message. B then verifies target Ds certificate certD and uses the key in the certificate to verify the signature on the REQUEST. If the signatures (or signature, when the packet is directly received from the target) are valid, the forwarding node removes the last forwarder's signature and certificate (if applicable), signs the original REPLY, and includes its own certificate. It then unicast the REPLY to the node from which it received the associated REQUEST. In the example, node B removes node Cs signature, signs the resulting REPLY, and includes its own certificate. Nodes B then unicast the resulting REPLY to A, from which it had previously heard the REQUEST [2]. Any node X receiving RREP from D to S maintains a reverse path entry in its routing table from X to D taking next hop the node which X has received RREP from.

- Route Maintenance:

The intermediate node sends a ROUTE ERROR to the previous hop, indicating that the route has been broken. This ROUTE ERROR includes the source, destination, intermediate node certificate, and a nonce and timestamp generated by the intermediate node for freshness. This packet is forwarded unchanged to the source.

$$
\begin{aligned}
S \rightarrow *: &\quad (\text{ROUTE REQUEST}, D, \text{cert}_S, N, t)_{K_S^-} \\
A \rightarrow *: &\quad ((\text{ROUTE REQUEST}, D, \text{cert}_S, N, t)_{K_S^-})_{K_A^-}, \text{cert}_A \\
B \rightarrow *: &\quad ((\text{ROUTE REQUEST}, D, \text{cert}_S, N, t)_{K_S^-})_{K_B^-}, \text{cert}_B \\
C \rightarrow *: &\quad ((\text{ROUTE REQUEST}, D, \text{cert}_S, N, t)_{K_S^-})_{K_C^-}, \text{cert}_C \\
D \rightarrow C: &\quad ((\text{ROUTE REPLY}, S, \text{cert}_D, N, t)_{K_D^-} \\
C \rightarrow B: &\quad ((\text{ROUTE REPLY}, S, \text{cert}_D, N, t)_{K_D^-})_{K_C^-}, \text{cert}_C \\
B \rightarrow A: &\quad ((\text{ROUTE REPLY}, S, \text{cert}_D, N, t)_{K_D^-})_{K_B^-}, \text{cert}_B \\
A \rightarrow S: &\quad ((\text{ROUTE REPLY}, S, \text{cert}_D, N, t)_{K_D^-})_{K_A^-}, \text{cert}_A
\end{aligned}
$$

Fig. 3. Route Discovery in ARAN[2]

$$
\begin{aligned}
B \rightarrow A: &\quad \langle(\text{ROUTE ERROR}, S, D, \text{cert}_B, N, t)_{K_B^-}\rangle \\
A \rightarrow S: &\quad \langle(\text{ROUTE ERROR}, S, D, \text{cert}_B, N, t)_{K_B^-}\rangle
\end{aligned}
$$

Fig. 4. Route Maintenance in ARAN[2]

Because ARAN uses public-key cryptography for authentication, it is particularly vulnerable to DoS attacks based on flooding the network with bogus control packets for which signature verifications are required. It don't uses hash Chain to verify for hop count it only uses extra signature.[2] Under attack, ARAN need only verify one signature in an attacker's packet by blacklisting a node that doesn't correctly verify the inside signature the initiator's signature in the case of an RREQ or the target's signature in the case of an RREP. An attacker, then, is unlikely to include a valid outer signature with an invalid inner signature. As a result, any bogus packet would have only a bogus outer signature [2]

- Secure AODV (SAODV):

The idea behind SAODV is to use a signature to authenticate most fields of a route request (RREQ) and route reply (RREP) and to use hash chains to authenticate the hop count.

- Route Discovery:

In SAODV, an RREQ packet includes a Route Request Single Signature Extension (RREQ-SSE). The initiator chooses a maximum hop count, based on the expected network diameter, and generates a one-way hash chain of length equal to the maximum hop count plus one. This one-way hash chain is used as a metric authenticator, much like the hash chain within ARIADNE.

The initiator signs the RREQ and the anchor of this hash chain; both this signature and the anchor are included in the RREQ-SSE. In addition, the RREQ-SSE includes an element of the hash chain based on the actual hop count in the RREQ header. We call this value the hop-count authenticator. e.g., if the hash chain values h0; h1; ; hN were generated such that hi = H[hi+1], then the hop count authenticator hi corresponds to a hop count of N □ i. With the exception of the hop-count field and hop count authenticator, the fields of the RREQ and RREQSSE headers are immutable and therefore can be authenticated by verifying the signature in the RREQSSE extension. To verify the hop-count field in the RREQ header, a node can follow the hash chain to the anchor. e.g., if the hop-count field is i, then hop-count authenticator hca should be Hi[hN]. Because the length (N) and anchor(hN) of this hash chain is included in the RREQ-SSE and authenticated by the signature, a node can follow the hash chain and ensure that hN = HN□i[hca]. Fig. 5 shows an example of route discovery in SAODV. When forwarding an RREQ in SAODV, a node first authenticates the RREQ to ensure that each field is valid. It then performs duplicate suppression to ensure that it forwards only a

single RREQ for each route discovery. The node then increments the hop-count field in the RREQ header, hashes the hop count authenticator, and rebroadcasts the RREQ, together with its RREQ-SSE extension. When the RREQ reaches the target, the target checks the authentication in the RREQ-SSE. If the RREQ is valid, the target returns an RREP as in AODV. A Route Reply Single Signature Extension (RREP-SSE) provides authentication for the RREP. As in the RREQ, the only mutable field is the hop count; as a result, the RREP is secured in the same way as the RREQ. In particular, an RREP-SSE has a signature covering the hash chain anchor together with all RREP fields except the hop count. The hop count is authenticated by a hop-count authenticator [hca], which is also a hash chain element. As before, a hop-count authenticator of hi corresponds to a hop count of N □ i. A node forwarding an RREP checks the signature extension. If the signature is valid, then the forwarding node sets its routing table entry for the RREPs original source, specifying that packets to that destination should be forwarded to the node from which the forwarding node heard the RREP. e.g., in Fig. 5, when node B forwards the RREP from C, it sets its next hop for destination D to C. SAODV allows intermediate-node replies through the use of a route reply double signature extension (RREP-DSE). An intermediate node replying to an RREQ includes an RREP-DSE. The idea here is that to establish a route to the destination, an intermediate node must have previously forwarded an RREP from the destination. If the intermediate node had stored the RREP and signature, it can then return the same RREP. If the sequence number in that RREP is greater than the sequence number specified in the RREQ [2].

$$
\begin{aligned}
S \rightarrow *: &\quad \langle (\text{RREQ}, \text{id}, S, \text{seq}_S, D, \text{oldseq}_D, h_0, N)_{K_S^-}, 0, h_N \rangle \\
A \rightarrow *: &\quad \langle (\text{RREQ}, \text{id}, S, \text{seq}_S, D, \text{oldseq}_D, h_0, N)_{K_S^-}, 1, h_{N-1} \rangle \\
B \rightarrow *: &\quad \langle (\text{RREQ}, \text{id}, S, \text{seq}_S, D, \text{oldseq}_D, h_0, N)_{K_S^-}, 2, h_{N-2} \rangle \\
C \rightarrow *: &\quad \langle (\text{RREQ}, \text{id}, S, \text{seq}_S, D, \text{oldseq}_D, h_0, N)_{K_S^-}, 3, h_{N-3} \rangle \\
D \rightarrow C: &\quad \langle (\text{RREP}, D, \text{seq}_D, S, \text{lifetime}, h'_0, N)_{K_D^-}, 0, h'_N \rangle \\
C \rightarrow B: &\quad \langle (\text{RREP}, D, \text{seq}_D, S, \text{lifetime}, h'_0, N)_{K_D^-}, 1, h'_{N-1} \rangle \\
B \rightarrow A: &\quad \langle (\text{RREP}, D, \text{seq}_D, S, \text{lifetime}, h'_0, N)_{K_D^-}, 2, h'_{N-2} \rangle \\
A \rightarrow S: &\quad \langle (\text{RREP}, D, \text{seq}_D, S, \text{lifetime}, h'_0, N)_{K_D^-}, 3, h'_{N-3} \rangle
\end{aligned}
$$

Fig. 5. Route Discovery in SAODV[2]

$$
\begin{aligned}
B \rightarrow A: &\quad (\text{RERR}, D, \text{seq}_D)_{K_B^-} \\
A \rightarrow S: &\quad (\text{RERR}, D, \text{seq}_D)_{K_A^-}
\end{aligned}
$$

Route maintenance in SAODV. The main differences between ARAN and SAODV route maintenance is that each SAODV that forwards a route error signs it, whereas forwarding nodes in ARAN simply rebroadcast the packet.

Fig. 6. Route Maintenance in SAODV[2]

- Route Maintenance:

SAODV also uses signatures to protect the route error (RERR) message used in route maintenance. In SAODV, each node signs the RERR it transmits, whether its originating the RERR or forwarding it. Nodes implementing SAODV do not change their destination sequence number information when receiving an RERR because the destination does not authenticate the destination sequence number. Fig. 6 shows an example of SAODV route maintenance [2].

V. Conclusion

Security in the MANET is a major concern to be looked upon. In this survey paper we tried to find out the various security issues in the Mobile ad hoc networks. Since MANET assumes to be resource constrained and having the characteristics like high mobility, dynamic topology, open architecture which makes MANET more vulnerable rather then any traditional network. As a result a higher security is needed in MANET rather than wired network. There is need for energy efficient protocols and algorithms, because energy consumption is a major problem in MANET.

Finally we concluded the current security solution to various routing issues in Mobile ad hoc networks, which included Secure DSR, Prevention for wormhole attack, Secure routing for AODV etc. In this survey we have only emphasized upon routing issues. There are still many pitfalls with current mechanism that is needed to be taken into account.

References

[1.] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, AND Lixia Zhang "Security in Mobile ad hoc Networks:Challenges and Solutions"

[2.] Yih-Chun Hu and Adrian Perrig "A Survey of Secure Wireless Ad Hoc Routing"

[3.] Yih-Chun Hu, Adrian Perrig, and David B. Johnson "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks"

[4.] Rashid Sheikh, Mahakal Singh Chandel, Durgesh Kumar Mishra"Security Issues in MANET: A Review"