RESEARCH ARTICLE OPEN ACCESS

Detecting Malicious Node: Survey

Charusheela Pandit, Seema Ladhe
Computer Engineering, MGMCET, Kamothe Navi Mumbai, India
Computer Engineering, MGMCET, Kamothe Navi Mumbai, India

Abstract
Now-a-days people are more habitual of using portable devices like laptops, mobile phones, mp3 players etc. The Ad hoc networking allows communication between these devices without any central administration. But this flexibility is threatened by various security issues. To overcome this we need the robust security solution. In order to meet this requirement, we have first focused on various network attacks for which MANET is vulnerable. Later we have discussed many security goals related to MANET. Finally we emphasized on various security solutions. It also compares standard and secure routing protocol on the basis of security aspects.

Keywords: AODV, MANET, Malicious Node, Network Attack, Trust Value.

I. Introduction

Pervasive computing allows the devices to be available anytime and anywhere. It is not possible to get wired network link between the two ubiquitous devices every time and everywhere. Due to this reason MANET, the mobile ad hoc network has grabbed the attention of many researchers which uses wireless communication technology. e.g. IEEE 802.11 Wi-Fi.

MANET is dynamically self organized mobile network with lack of infrastructure and central support. Using mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that are not in the direct communication range use intermediate node(s) as routers to communicate with each other. The packets are forwarded from one source to one destination with the help of these intermediate nodes to create “multihop” paths. The routing protocols are supposed to find such multihop paths. Routing protocols used in MANET are: DSDV, OLSR, TBRPF, AODV, DSR, TORA, ZRP etc. The detail classification of these protocols is mention in section II.

MANET can provide information and services all time and everywhere at any geographic position. It can be very easily deploy at any place and time as it does not require any well established infrastructure. Because of these magnificent distinctiveness MANET has many applications.

In adverse geographic conditions and locations MANET can establish distributed network system without any base stations. MANET has no central administrator or infrastructure. Due to this flexibility in the implementation of MANET it can be used in during natural calamities such as earthquake or flood like situations. It is used during emergency services, military or police operations. It plays important role in setting ad-hoc conferencing.

Apart from these recompense MANET has few confines as well. Due to limited resources i.e. energy supply, limited bandwidth and also due to mobility of nodes, it is difficult to establish wireless communication link between two nodes. Due to continuous mobility MANET has certain disadvantages like frequent change in the topology which may allow any compromised node to join network without being noticed. Owing to open medium and intrinsic trust among the nodes it is very difficult to discriminate among normal and malicious node. All these limitations make MANET vulnerable to network attacks and its security issues become the prime area of concern.

This paper focuses on security issues of MANET protocols. Our contribution in this paper is we have presented the detail comparison of few traditional routing protocols and secure routing protocols on the basis of security aspects. This paper is organized as follows: Section II gives classification routing protocols and execution of few traditional routing protocols. Section III gives the details of various attacks of MANET. Section IV discusses security objectives of MANET. Section V provides the literature survey available on various secure routing protocols. The detail comparison of few traditional routing protocols and secure routing protocols on the basis of security aspects is specified in Section VI. Concluding remark is the part of Section VII.

II. Traditional routing protocols

Routing protocols are classified depending on many parameters like network structure, routing scheme, availability of information, latency, network overhead etc. Depending on the routing scheme, MANET's routing protocols are categorized as

- Proactive
- Reactive
- Hybrid

List of protocols in each category is listed in the fig.1.

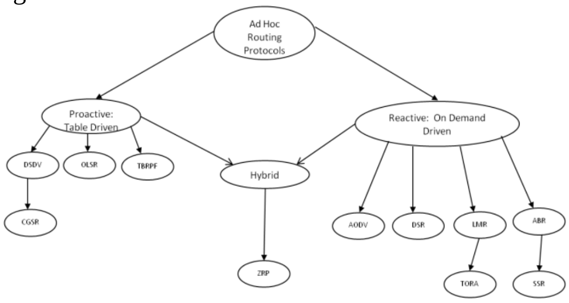


Fig.1 Classification of Routing Protocols of MANET

A. Reactive Protocol

Reactive protocol is also known as source initiated on-demand routing protocol. In this type, route is discovered only when source node needs it. When source node require path for particular destination it searches its route cache for the availability of path. If path is not available it performs route discovery. Route will be maintained by route maintenance procedure until route is no longer required or destination is not approachable from all paths from source. Routing overhead is less in these protocols but it increases latency due to route discovery. Latency is increased due to every intermediate node involve in route discovery. These protocols are used where less routing overhead is required.

1. AODV: AODV or Ad-hoc on demand routing protocol is the reactive protocol. When source need to send message to the destination it searches its routing cache for route to destination. If route does not found it initiates route discovery. AODV supports both multicasting and unicasting routing. AODV uses three control messages while routing information within the network:

Route Request Message (RREQ)

Source initiates route discovery by sending RREQ message to its neighbours. Neighbour sends RREQ message to its neighbour likewise it uses expanding ring technique to reach to the destination. RREQ message contains source IP address, source sequence number, destination IP address, destination sequence number, hop count and broadcast ID.

Route Reply Message (RREP)

RREP message is generated in three cases:

1. When node does not have path to the destination it generates RREP message and sends to source. The elements of RREP message are source address, destination address, destination sequence number, hop count and lifetime.

2. When intermediate node have destination sequence number higher than the destination sequence number in RREQ message then intermediate node generates RREP message and sends it. The elements of RREP message are source address, destination address, destination sequence number, hop count and lifetime.

3. When RREQ reaches to destination, it selects the shortest path from all received RREQ and sends RREP message to source node. The elements of RREP message are destination sequence number, destination ip address, originator ip address and lifetime.

Route Error Message (RERR)

The node sends RERR message to its previous node from which it has received RREQ message if it finds link to its next hop is broken. A node can also send RERR message if it received the data packet for the destination for which it does not have active path.

Route Discovery in AODV

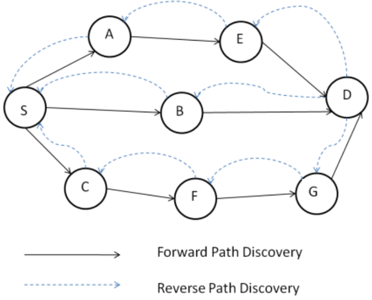


Fig.2 Route Discovery Process in AODV

Source node S initiates route discovery by sending RREQ message to its neighbour. By opting the ring expanding technique neighbour sends RREQ to its neighbour. Ultimately RREQ message reaches to the destination. As shown in fig. 2 the destination node D receives three RREQ messages each from node E, node B and node G. Out of these, node D selects the shortest path i.e. S-B-D and generates RREP message and sends to source node S. Each intermediate node processes RREQ message either by generating RREP message or by rebroadcasting the RREQ message after incrementing hop count and by updating its routing table by storing the details of its previous node from which it has received RREQ message, so that, it can be used in reverse path discovery. The intermediate node generates RREP message either if it does not have path to the destination or if it has greater destination sequence number. If node found broken link to its next hop it generates RERR message.

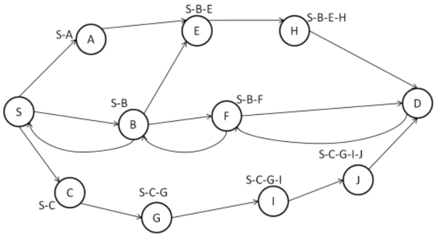
Route Maintenance in AODV

Each node maintains the lifetime field for each row in its routing table. If route is not used within that time then route is not considered as active route and gets deleted from the routing table entry of that node.

2. DSR: Dynamic source routing or DSR is a reactive protocol. In this protocol intermediate node does not store routing information rather routing information is stored in routing cache. DSR route cache entries do not have lifetime entry. In DSR each node replies to every duplicate RREQ. Because of the source routing in DSR the size of the RREQ packet header grows as number of intermediate nodes increases. DSR has two main components:

Route Discovery in DSR

When source node has packet to send to some destination, it checks its route cache to find whether it has route to that destination. If not, it initiates route discovery by flooding RREQ message. Each intermediate node who receives RREQ message checks whether it has path to that destination otherwise appends its own address to route record of request packet. If intermediate node has un-expired path to the destination in its route cache then it can also generate reply message. Finally when RREQ reaches to the destination it generates reply message. RREP message travels the route which is obtained by reversing the route appended to the RREQ message. When source node has data packet to send to the destination, the entire path is included in the packet header. Intermediate nodes with the help of this path, decides to whom it has to forward the data packet. So, from fig. 3 source node S will use S-B-F-D path to send data packet to destination node D.



Source node will use path S-B-F-D to send data packet to destination node D.

Fig.3 Route Discovery in DSR

Route Maintenance in DSR

A node can transmit data packet, RREP or REER. It must cross check that it has been properly received by its neighbour i.e. its next hop. Otherwise node should generate error message and send to source. Source should initiate the route discovery again.

B. Proactive Protocol

Proactive routing protocols are also called as table driven routing protocols, where each node maintains the routing table. This routing table will have information from every node to every other node. Routing information is propagated by every node periodically or whenever network topology changes in order to maintain the consistent network view. Proactive protocols are not apposite for large network as it has to maintain large routing tables. As routing information is available in advance, node can find best path to destination, hence latency is decreased. These protocols are used where minimal latency is required.

1. DSDV: The protocol Destination Sequenced Distance Vector is abbreviated as DSDV. It is proactive protocol and works on Bellman-Ford algorithm. Each node of DSDV maintains routing table which contains next hop, cost metric towards each destination a sequence number that is created by the destination itself. Each node lists all destinations and number of hops to those destinations. Each node knows the shortest path to destination in advance. When node has significant new route information it transmits that information to its neighbour by monotonically increasing its sequence number so that it should be even number. DSDV support periodic and triggered routing updates. If the link between the nodes is broken then it is designated as infinity. This protocol guarantees loop free paths.

Working of DSDV

Consider the following figure:

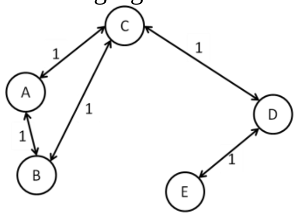


Fig.4A DSDV Routing Update

Consider the following network scenario: All nodes broadcast with sequence number 1.Each node accept routing update from its neighbour. Thus from fig. 4A, for node A, distances to other nodes are node B=1, node C=1, node D = node E = ∞

When node D sends message to node C, then distances for node A will be

node B=1, node C=1, node D = 2, node E = ∞

In the second round of forwarding from node C, node A will get new set of distances

node B=1, node C=1, node D = 2, node E = 3

Now node B moves to the new position in the network as shown in fig. 4B. Also it has received new message from node E with sequence number 2.

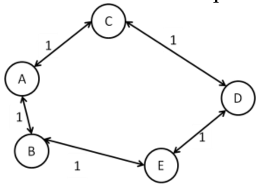


Fig.4B DSDV Routing Update

Now node A has two distances for node E: Initial one with distance equal to 3 and sequence number equal to one. And second one from node B with distance equal to 2 and sequence number equal to two. Node A will compare the sequence number of both messages. Later has most recent sequence number. Hence node A will update its routing table and changes its distance to node E from 3 to 2.

Route Maintenance

When node finds the broken link, it increments sequence number by 1, so that, sequence number will be the odd number. It sets the metric value to infinity and advertises the packet.

C. Hybrid Protocols

Hybrid routing protocols inherits the potency of both protocols (Reactive and Proactive). It reduces the routing overhead of proactive protocols and decreases the latency of reactive protocols. The Zone Routing Protocol or ZRP is the first hybrid routing protocol. ZRP segregate the topology in zones. The radius whose value is equal to the parametric value X which is equal to the number of hops decides the size of zone. ZRP's structure is modular, as different protocols are used within and between the zones depending on their advantages and disadvantages. Proactive protocols are used inside the zone so that nodes have uniform routing information about each node within the zone. Due to this, communication of the nodes within the zone is faster, reducing the latency. However, inter-zone routing uses reactive protocols. This reduces the need of each node to have fresh information about entire network. [1]

III. Security Vulnerabilities of MANET

Mobile Ad-hoc network is far more vulnerable than traditional wired network. Hence security maintenance of Ad-hoc network is much more difficult. MANET is vulnerable to the following attacks:

Attacks in the MANET can be classified as

- Passive Attacks
- Active Attacks
- External Attacks
- Internal Attacks

A. Passive Attacks

Passive attack does not disturb the network operation. It is used to steal the confidential information from the targeted network. Examples of passive attacks are eavesdropping attacks and traffic analysis attacks.

1. Passive Eavesdropping: Eavesdropping is the attack, where attacker listen the communication between nodes throughout the network. The attacker will try to obtain secrete information about network (like public key, private key, passwords and location) which is important to settle the authenticity of nodes. This information should be kept out of reach of unauthorized users. [13]

2. Traffic Analysis Attack: It is used against the internet encryption. It analyse the type of information (chat, email, web page request) being communicated even if it in encrypted form or scrambled. This attack is more effective against encrypted proxies.

B. Active Attack

Active attack intentionally alters the data to disturb the operation of the network. The examples of active attack are message modification, message fabrication and denial of service.

1. Message Modification: A malicious node will try to modify the fields of protocol.

2. Message Fabrication: Fabrication attack refers to generating false routing messages.

3. Denial of Service attack (DOS): In denial of service attack, the malicious node consumes the bandwidth of a network by repeatedly propagating request package to target node. This exhausts the processing power of target and consumes the resources (storage capacity, processing power, computation resources) available by target.

4 Active Interfering: Active interfering attack is attack where attacker jams the radio signals, distorting the communication. As communication channels are blocked nodes cannot forward or receive packets. This gives an effect of broken link and nodes have to search for another path to communicate. This is special type of Daniel of service attack.

5. Gray Hole Attack: In Gray hole attack, initially malicious node behaves normally i.e. during route discovery. But, as soon as it starts receiving the data packets it begins dropping it. Sometimes attacker node behaves normally while forwarding the data packet, whereas sometimes it behaves maliciously by dropping the data packets.

C. Internal Attack

A node, which a part of network performs malicious task that affects the overall functioning of network badly, then it, is called as internal attack.

1. Internal Black Hole Attack: In black hole attack, a malicious node will claim that it has freshest and shortest path to the destination without referring to the routing table. In this way attacker node will always reply to the route request and thus intercept the data packet and retain it.

2. Rushing Attack: The node sends request packet to its entire neighbor. Out of these neighbor if one node is compromised node then it will forward the route request packet without authenticating the sender as soon as possible. So, that it can get entry in the network. Rushing attack is difficult to identify and rectify.

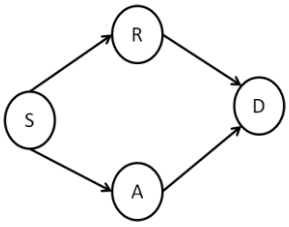


Fig.5 Rushing Attack

From fig. 5 source node S has send message to node A and R. Node R will rush the message received from S to D without authenticating S.

3. Sybil Attack: Sybil attack represents multiple identities for malicious intent. From fig. 6 node A forwards the packet to its neighbours e.g. node B, node C, and node M. If node M is compromised node it will represents M_1, M_2, M_3 nodes giving illusion to node A that it has 6 neighbours instead of 3.

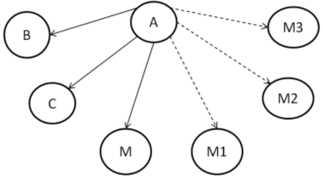


Fig.6 Sybil Attack

D. External Attack

When external node forcefully tries to be the part of network and performs malevolent behaviour, then it is called as external attack.

1. External Black hole Attack: In external black hole attack, attacker will deny the access to the network with the help of denial of service attack or by congestion in the network or by disturbing the entire network.

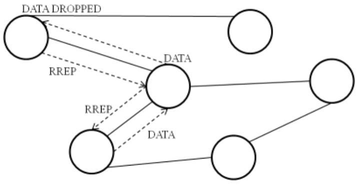


Fig.7 External Black Hole Attack

2. Impersonation: As there is low level of trust among the nodes of the MANET, the adversary captures few nodes from the network. Initially these nodes behave as gentle node. When they get entered in the network they start performing malicious behaviour e.g. propagating fake routing information, grab the improper priority to access unauthorized or confidential data.

3. Wormhole Attack: In Wormhole attack, malicious nodes are at strategic position in the network with shortest path among themselves. These nodes advertise this shortest path among themselves in the network. They create tunnel between them so that data is received at one end of the tunnel and diverted to another position of the network from other part of tunnel.

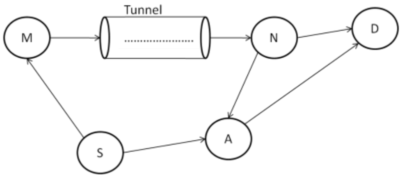


Fig.8 Wormhole Attack

From above fig.8 node S is source node and node D is destination node. Node M and N has created tunnel and diverted the received data.

4. Jellyfish Attack: Jellyfish attack refers to creating delay in the network. In this attack, attacker first get access to the network and becomes part of it. As it starts getting the packets it delays its forwarding. This introduces delay in the network. Once delay gets propagated in the network packets are released. This affects the performance of networks, increases end-to-end delay, increases jitter delay.

Table 1 describes the stack of attacks at different layers of network.

TABLE 1 Possible Attacks at Different Layers of Network [2]

Network Layer	**Possible Attacks**
Application Layer	Malicious code, Repudiation
Transport Layer	Session hijacking, Flooding
Network Layer	Sybil, Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing, Link Withholding, Location disclosure etc.
Data Link/MAC	Malicious Behavior, Selfish Behavior, Active, Passive, Internal External
Physical	Interference, Traffic Jamming, Eavesdropping

IV. Security Objectives of MANET

MANET is weak to many attacks. To maintain the safety of data or message the following security objectives needed to achieve.

A. Availability

The term availability means node should be able to provide services as and when required. The denial-of-service attack can affect the services provided by node. By repeatedly generating the route request malicious node exhaust the processing power of target and make the services provided by it unavailable.

A. INTEGRITY

Means that the information is not modified or corrupted by unauthorized users or by the environment. Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways [3]: Malicious altering and Accidental altering.

B. CONFIDENTIALITY

Confidentiality means secrecy. Confidentiality can be gained only when the certain data can be accessed by authorized people. Other elements of the networks should not have privilege to access it.

C. AUTHENTICITY

Authenticity checks that the participating node is genuine one, not the impersonator. As there is less authenticity among nodes, adversary will make few nodes in the network to propagate fake routing information disturbing the operation of the network.

D. AUTHORIZATION

Authorization assigns permissions and privileges to nodes to services of the network. Authorization process is done with the help of certificate authority. Different access rights are given to different user at different levels. The network administrator has access to entire network management function.

E. NON REPUDIATION

To repudiate means deny. So, non repudiation does not allow any node to deny any action i.e. any message it has send or received. It is basically useful when we want to identify whether the node is normal node or compromised node. Any node can take help of erroneous message which it has received to declare any node as malicious node. Non repudiation can be obtained using digital signature.

F. ANONYMITY

Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. This criterion is closely related to privacy preserving, in which we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities. [4]

G. SCALABILITY

Scalability is not directly related to security but it is very important issue that has a great impact on security services. An ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network. [4]

V. Secure Ad Hoc Routing Protocols

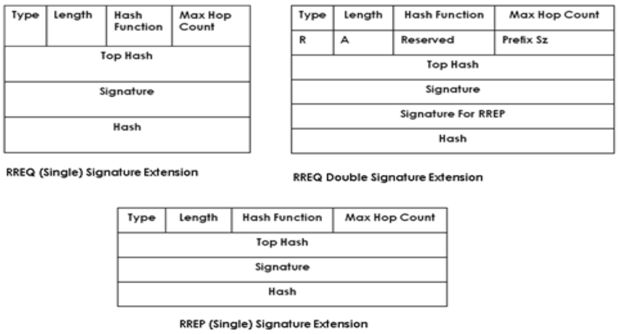
To allow data/request packet to travel throughout the network safely, it should be keep safe from all network attacks so that the security objectives of the network will be achieved. There are many routing protocols that identify compromised nodes and establishes secure path for packets to travel. Some of the secure routing protocols are discussed below:

A. Securing Ad Hoc Routing Protocols [5]

Securing Ad hoc Routing Protocols are used to secure the routing packets of AODV.

The request messages are sent directly to the immediate neighbor, where they are processed, modified and resent. As a part of processing the intermediate node may modify their routing tables. So, intermediate nodes need to check the authenticity of the information in the request message.

In this paper it is mentioned that there are two types information in request message: mutable and non mutable. Hop count is the mutable information and all other information in request message comes under non-mutable. Hash chain is used to secure hop count and non mutable fields are authenticated using digital signature. In this paper the signature extension is suggested, that is transmitted with AODV message, which contains the information about hash chain and digital signature. Hash chain prevents unauthorized modification of hop count whereas digital signature is used at node level to authenticate the receiver.



RREQ (Single) Signature Extension

RREQ Double Signature Extension

RREP (Single) Signature Extension

Fig. [9] RREQ and RREP Signature Extensions

If intermediate node has higher destination sequence number in its routing table than destination sequence in RREQ packet then intermediate node uses RREQ Double Signature Extension to process the RREQ packet.

Protocol is vulnerable to tunneling attack due to two consecutive compromised nodes.

B. SEAD [6]

A Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks is based on

Destination Sequenced Distance Vector routing protocol. In this paper Message Authentication Code (MAC) is used to authenticate the neighbor node and one-way hash chain is used to authenticate routing updates. Due to one-way hash chain any node can only increase the metric in the routing update but cannot decrease it. Each node generates list of hash chain h0, h1, h2… hn where x=h0 x Є {0, 1}p, where p is length of bits of the output of hash function. Initially node generates values from left to right as shown above. But while using these values, node progresses from right to left i.e. if node knows hi-3 it can authenticate hi by H(H(H(hi-3))) and validate this result with hi. Node includes hash value in each routing update. When node has routing update it includes destination address, sequence number, metric, and hash value which is equal to the hash of the hash value it has received from the routing update entry for that destination. When a node receives the routing update it authenticate each entry in that update with the help of destination address, sequence number, metric and hash value. The node hashes the received hash values correct number of times to check the values with prior authentic value. If a value matches it concludes that routing update is authentic.

This paper increases the overhead on network due to increased number of routing advertisements and due to increased in size of each advertisement from the addition of the hash value on each entry for authentication.

C. Mitigating Routing Misbehaviour in Mobile Ad Hoc Netwoks [7]

This paper is based on Dynamic Source Routing (DSR). It has introduced two extensions to DSR to diminish the effects of misbehaving nodes: the watchdog and the pathrater.

The watchdog detects the malicious nodes. It is implemented by maintaining the cache. As shown in fig. [10] node A maintains cache of all recently send packets. It checks whether node C has received those packets i.e. whether node B has forwarded the packets or not. As packet is received by node C respective packet will get removed from node A's cache. If particular packet remain in the node A cache for longer time than certain timeout then failure tally of node B will incremented by one. If failure tally of node B crosses the threshold value then node B will be declared as malicious node.

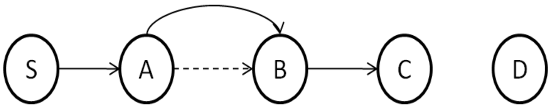


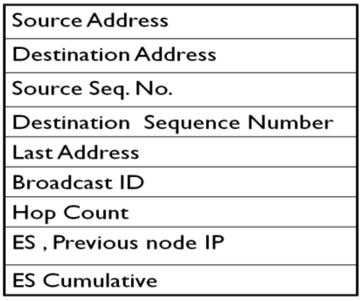
Fig. [10] Watchdog Implementation

Each node runs the pathrater and each node knows the rating of every other node in the network. Pathrater assigns 0.5 rating to every node discovered during route discovery. It increases the rating of each node by 0.01 after every 200ms. If node is found as malicious node then its rating get reduce by 0.05. Pathrater calculates path metric and path with the highest path metric is selected.

This protocol cannot deal with colluding attack i.e. if node C does not forward the packet but node B does not report node A. If some node has temporarily performed malfunctioned (i.e. due to broken link does not able forward the packet) it gets excluded from the network for longer time.

D. ES-AODV[8]

The Effective Secure AODV algorithm is used to find the malicious node free path than shortest path. In this paper each node has got some unique value to define the level of trustworthiness of a node over another called as trust level. The basic idea behind this protocol is that each intermediate node modifies route request packet by appending the trust level and IP address of its predecessor and by increasing the cumulative ES field by trust value of its predecessor and then broadcast that packet. The structure of route request packet is shown in fig.11. After broadcasting, predecessor verifies if node had appended correct value or not to ensure information authenticity. Otherwise predecessor sends warning message questioning malicious action of a node. The final route selection is based on maximum Cumulative Trust Level. The destination selects the path with maximum Cumulative Trust Level. If more than one packet has same trust-level than hop count is used in selecting the path.



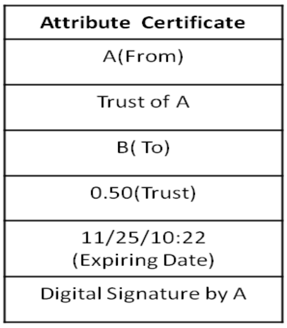
Source Address
Destination Address
Source Seq. No.
Destination Sequence Number
Last Address
Broadcast ID
Hop Count
ES , Previous node IP
ES Cumulative

Fig. [11] Route Request Packet Structure in ES-AODV

In this paper modified RREQ packet can be received by the next node as predecessor checks the authenticity of its successor after it broadcast the RREQ packet. This increases the overhead on network as it need to compute the trust level and signature of its successor. It can face the Newcomer attacks (NCA).

E. *Trust Level Evaluation for Communication Paths in MANETs by Using Attribute Certificates[9]*

This paper has offline phase where the trust value of each node is calculated. The node whose trust level is calculated is called as calculated node and node who is calculating the trust level is called as calculating node. The calculating node gives trust value information to calculated node in the form of Attribute Certificate (AC).



Attribute Certificate

A(From)

Trust of A

B(To)

0.50(Trust)

11/25/10:22
(Expiring Date)

Digital Signature by A

Fig. [12] Structure of AC: AC Issued From Node A to Node B

From fig. 4 Node A puts all elements of AC into hash function to get hash value and attaches the value as digital signature. The calculated node can verify the AC if it has the valid public key of the calculating node. The calculated node can verify the public key of calculating node with the help of chain of PKCs.

The source node performs the route discovery for the particular destination. The source node has to decide the most trustworthy path. When intermediate node receives the RREP packet it attaches holding AC. Each intermediate node attaches the top three ACs to the RREP. Source node verifies all received AC and selects the path with highest trust metric.

The proposed solution in this paper increases the network overhead as size of each AC is 145 bytes & size of RREP packet is 1500 bytes, so, it can accommodate only 10 ACs (i.e. of 3 intermediate nodes). As hop count increases, more RREP will require for single path. Overhead on source node increases as it has to verify the PKCs for each AC to authenticate the public key in AC.

VI. Comparison of Routing Protocols

A. *Our Contribution:*

Table 2 Comparison of Standard Routing Protocols

	AODV	DSR	DSDV
Routing Scheme	Reactive	Reactive	Proactive
Routing Information Container	Routing Table	Routing Cache	Routing Table
Request Packet Size	Fixed	Depends on number of intermediate nodes	Fixed
Routing Advertisement	On demand	On demand	Periodic and triggered
Loop Free	Yes	Yes	Yes
Path Decision On	Hop count and sequence number	Hop count	Sequence number
Route Maintenance	Entry gets deleted after time expiration	If packet not received, sends error message to source	Increments sequence number by 1 and advertises with infinite metric

B. Our Contribution:

Table 3 Comparison of Secure Routing Protocol on The Basis of Security Aspects

	Securing AODV [5]	SEAD [6]	Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks [7]	ES-AODV[8]	Trust Level Evaluation for Communication Paths in MANETs by Using Attribute Certificates[9]
Routing Scheme	AODV	DSDV	DSR	AODV	SMR
Attack Vulnerability	Cannot deal with Warmhole Attack	Cannot deal with colluding	Cannot deal with colluding	May face Newcomer Attack	Gray Hole Attack
Authentication Scheme	One-Way Hash Chain, Digital Signature	One-Way Hash Chain and Message Authentication Code	Watchdog, Pathrater	Trust Levels, Message Authentication Code	Trust Levels, Digital Signature
Drawbacks	Cannot evaluate previous hash value	Temporary malfunctioned nodes are removed from network for longer time	Increases network overhead, more latency	Routing packets are forwarded to neighbours without checking its authenticity	More authentication overhead on source, more number RREP require, if intermediate nodes are more

VII. Conclusion

There are various drawback of MANET like continuous mobility of nodes which may result in frequent changes in topology, lack of infrastructure makes the MANET weaker to handle various network attacks. This paper has covered maximum network attacks and traditional routing protocol. This paper has emphasized on few secure routing protocols and its comparison with respect to its security issue. Additionally it provides the comparison of few traditional routing protocols.

References

[1] http://www.olsr.org/docs/report_html/node18.html

[2] http://en.wikipedia.org/wiki/Mobile_ad_hoc_ network

[3] Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/ Data_integrity

[4] Deepak Chayal, Dr. Vijay Singh Rathore "ASSESSMENT OF SECURITY IN MOBILE AD-HOC NETWORKS (MANET)" Volume 2, No. 6, June 2011, Journal of Global Research in Computer Science

[5] Manel Guerrero Zapata, N. Asokan "Securing Ad Hoc Routing Protocols" WiSe'02, September 28, 2002, Atlanta, Georgia, USA. Copyright 2002 ACM 1-58113-585-8/02/0009 ...$5.00

[6] Yih-Chun Hu, David B. Johnson, Adrian Perrig "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks" Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02) 0-7695-1647-5/02 $17.00 © 2002 IEEE

[7] Sergio Marti, Gluli, Lai, Baker: "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks" Copyright ACM 2000 1-58113-197-6/00/08...$5.00 Copyright ACM 2000 1-58113-197-6/00/08 …$5.00

[8] Zeyad M. Alfawaer, Saleem Alzoubi: "A proposed Security subsystem for Ad Hoc wireless Networks " 978-0-7695-3930-0/09 $26.00 © 2009 IEEE DOI 10.1109/IFCSTA.2009.183

[9] S.Inoue, M.Ishii, N.Sgaya, T. Yatagai, I. Sasase: "Trust Level Evaluation for Communication Paths in MANETs by Using Attribute Certificates" 978-1-4244-7057-0/10/$26.00 ©2010 IEEE

[10] Charles E. Perkins, Elizabeth M. Royer ”Ad-hoc On-Demand Distance Vector Routing " http://www.cs.washington.edu /education/courses/cse461/07wi/lectures/aodv.pdf

[11] Sonali Bhargava and Dharma P. Agarwal "Security Enhancements in AODV protocol for Wireless Ad Hoc Networks" 0-7803-8/01/$10.00 @ 2001 IEEE

[12] Elizabeth M. Royer, Charles E. Perkins "Multicast Operation of the Ad-hoc On-Demand Distance Vector Routing Protocol "@ACM 1999 1-58113-142-9/99/08…$5.00

[13] Wenjia Li, Anupam Joshi "Security Issues in Mobile Ad Hoc Networks – A Survey" http://www.cs.umbc.edu/~wenjia1/699_report.pdf

[14] Panagiotis Papadimitratos, Zygmunt J. Haas "Secure Link State Routing for Mobile Ad Hoc Networks" in Proceedings of the IEEE Workshop on Security and Assurance in Ad hoc Networks, in conjunction with the 2003 International Symposium on Applications and the Internet, Orlando, FL, January 28, 2003

[15] V. Manchikalapdi, S. Yelisetti, R. Surapaneni: "Detecting Misbehavior Nodes and Trust Levels in MANETS" Engineering Education: Innovative Practices and Future Trends (AICERA), 2012 IEEE International Conference on 19-21 July 2012 978-1-4673-2267-6

[16] K.Gonindan, P.Mohapatra: "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey" http://spirit.cs.ucdavis.edu/pubs/journal/kannan_survey.pdf

[17] Xia Li, Jill Slay, Shaokai Yu:" Evaluating Trust in Mobile Ad Hoc Networks" Workshop of International Conference on Computational Intelligence and Security 2005 http://esm.cis.unisa.edu.au/new_esml/resources/publications/evaluating trust in mobile ad-hoc networks.pdf