An Efficient Secure Routing Protocol in MANET Security - Enhanced AODV (SE-AODV)

Rajdeep S. Shaktawat
Department of Computer Engg.
College of Technology and Engineering, Udaipur, India

Dharm Singh
Department of Computer Engg.
College of Technology and Engineering, Udaipur, India

Naveen Choudhary
Department of Computer Engg
College of Technology and Engineering, Udaipur, India

ABSTRACT

A MANET is a collection of independent mobile nodes with self configuring, self administrating features. In MANET initial work for routing was done addressing the path formation between nodes. A network in which any node can join and leave the network, routing protocol addressed for only efficient path formation makes the same network vulnerable to various attacks. Packets that are routed during route discovery need to be protected in such a way that it has least probability of having a malicious node in path formed. In this paper, a new secure routing protocol SE-AODV is proposed which adds extra features to same AODV routing protocol making path formation more secure. Malicious node in network tries to disrupt the path formation by various attacks and degrade the network performance. We followed evaluation of proposed algorithm performance by comparing it to SAODV and addressing the loopholes in SAODV and how proposed secure protocol overcomes it with Minimum overhead Maximum security.

Keywords

MANET, PKI, cryptography, AODV, Security, routing protocol, Secure Route, security enhanced AODV, secure routing in MANET.

1. INTRODUCTION

Security comes out to be the major concern in network like MANET where any node without any authentication comes in the network and leaves network. In MANET there is no central authority that can govern the authentication of nodes, which can make sure that the nodes in the network are not malicious. With network infrastructure where any node can come and leaves the network and while present in network act as a router forming a path between source and destination the major issue which arises is the security of the path. It could be that some malicious node can enter in a path formation. Initial routing protocols like AODV was introduced which is on demand routing protocol in which control packets are flood only when source want to establish a connection with destination. AODV addressed initially for efficient path formation in terms of delay etc. but there was no concern for security which is must in today's need as data serves out to be more confidential.

So in this paper a new security approach is addressed which adds up new security features to same AODV routing protocol. New approach makes AODV more efficient in terms of security making it sure that a malicious free path is formed for the communication. Malicious node always tries to modify the control packet information so that destination gets a false control packet and false information is used by two parties for establishing connection. So proposed new protocol secure control packets with such attacks.

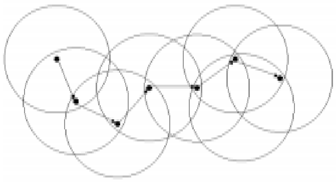

Fig1: A Simple MANET Structure

A MANET is a collection of independent nodes which communicate with each other via radio waves, the nodes which fall in the transmission range of other nodes, they can communicate directly but the nodes which are not in the transmission range can be communicated by sending the route discovery packets, forming a path to the destination. The independent nodes present in the network works to forward the route discovery packets and forward data packets during data transmission time. A MANET does not follow any fixed infrastructure, topology changes frequently, self configuring network, there is no base station, node's in MANET are independent and work together to form a communication channel between sender and receiver. All nodes in this network type have a wireless interface through which they communicate with other nodes in network. Routing protocols in AD-hoc are generally classified in two categories one is proactive or table driven and reactive or on demand. In proactive routes are kept in table which are continuously updated by nodes and route table are kept up-to-date. While in reactive the path is formed only when it is initiated by source or when there is need to communicate.

2. CHARACTERISTICS OF MANET[4]

Dynamic topology: In MANET as nodes are free to move the topology changes frequently. Nodes can leave any sub-network of MANET and comes in another sub-network of same network. There is no central authority which can govern this and makes this reflection known to other nodes in the network.

Bandwidth Constraint: Nodes in MANET has a wireless interface by which they communicate with each other it's obvious thing that wireless links has lower throughput as compared to wired counter parts and other factors like mobility always plays vital role in achieving throughput.

Resources constraint: in MANET a resource or a group of resource available to group of nodes cannot be available to other group as well.

Energy constraint: Each node in MANET has respective energy each node utilizes his energy to perform each and every operation in MANET.

Security: MANET is an open network no authentication of nodes. So they are more prone to attacks like eavesdropping, modification, spoofing, other attacks which are performed at network layer.

"Power, Bandwidth and distance are fundamentally related to each other. If we have twice power which can be equal to twice bandwidth but if the distance is twice it needs four time power."

3. SECURITY REQUIREMENTS AND CHALLENGES IN MANET[5,7,8,9]

To solve security issues of AD-HOC network we have to look at the requirements we have to achieve and various challenges to achieve same in a network of self configuring, self authentication and self administration.

Availability: Network on which nodes working, should be available to all nodes.

Confidentiality: It aims that a malicious node cannot be able to read the message which comes in between path.

Integrity: It aims at ensuring that when a data is sent from source to destination the contents of message are not changed.

Authentication: Nodes working in the network are authenticated.

Non-repudiation: if A sends a message to b then b can be able to verify that the message it received is sent from A only.

There are many attacks[11] at various layers we cannot have a general solution for all threats. The major attacks which constitute at network layers are held during the path formation like change of hop count, change of hop count is the source of major attacks where a malicious node tries to alter the hop count information, as for destination this hop count serves as major role in selecting the path for communication and second is the modification of control packets or Route Discovery packets.

4. BACKGROUND

There can be two approach for security in any network one is Preventive approach that is cryptographic approach in which various cryptography processes are used for security and second is reactive approach in which systems like intrusion detection systems are used for detecting attacks like IP spoofing etc. This paper will discuss preventive approaches that are used so far for security and then how proposed scheme proves out to be more efficient in terms of security with minimum overhead maximum security.

This paper will concentrate in one protocol AODV standardized by IETF. The fundamental difference that is in between ad-hoc networks and standard internet protocol is the security. That draws attention of many researchers over this note. Ad-hoc networks are more prone to any attacks. Attacks in ad-hoc network is not only constitute of modification, eavesdropping, Sybil attacks etc. but also like nodes not participating in routing, intentionally dropping the packets, changing contents that attract source and destination to choose path.

So the issue security gains too much attention, Which led to the development of ARIDANE[6] routing protocol in which pre deployed pair wise symmetric-keys or pre deployed pair wise asymmetric keys. One option of Aridane is to use a KDC which act as a key distribution system. It works that source and destination share some secret which is not possible as it's not possible that a common secret is shared between them and second it uses Tesla based authentication. It requires that the packets are delayed long route time. Trust Level Security approach cannot fully save the network as it's impossible to trust any node on any next path forming in a network where we think path can consist of malicious nodes.

Wormhole attack solution is defined in [2] but that require special hardware for high degree clock synchronization. The use of trust level security parameter in hierarchical organization is not possible as it requires a common secret to be shared between both.

There are many approaches that had been implemented on security of routing protocol in MANET following section addressed some secure routing protocols that turned out to be best among all.

Now we will be discussing various approaches for securing AODV. Securing a MANET is a major issue and which has to be done in such a manner that the implemented security algorithm does not degrade the routing performance. It should not be there that every node in MANET is made to do number of function each time they receive a packet as node in MANET has a limited amount of energy and this energy should be utilized by node in an optimal way. Approaches so far like in ARAN is considered as high secure algorithm but the amount of work each node has to done is very large that constitute the routing overhead.

5. SECURITY VARIANTS

5.1 ARAN(Authenticated Routing Protocol) [2]

It totally depends on third party for security and that's the reason it is also referred as third party security protocol. In this routing protocol whenever a node comes in a network a trusted third party authenticate it and provides a certificate to it with its IP address, timestamp and a key all signed by the private key of the trusted third party. In ARAN hop count field is neglected and hence this protocol works by selecting a path which is has less congestion. But as hop count field is not included one side it saves from other attacks as well as on other end sometimes it selects a longer path that affects the presence of packet in network and thus increasing the routing load and degrading the overall performance of network. ARAN make use of cryptographic certificate for accomplishing its task but that increase much overhead. ARAN lacks as it is not guarantee that the authenticated node in ARAN routing will do any malicious activity as a true node can authenticated itself from trusted third party and when one it comes in network it can do various malicious activity like DDOS attacks and rushing attacks etc with this ARAN has no control over selfish nodes and nodes dropping the packet intentionally. It also have no answer what if the third party is compromised.

The algorithm of ARAN works as follows:

T: Trusted Third party
T→ A: cert A= [IPA, KA+ ,t, e]KT-
A→ brdcst: [RDP, IPX, NA] KA-, CertA
B → brdcst: [[RDP, IPX, NA] KA-] KB-, CertA, CertB]
C→ brdcst: [[RDP, IPX, NA] KA-] KC-, CertA, CertC]
X→ D: [REP, IPA, NA] KX-, certx
D→ C : [[REP, IPA, NA] KX-] KD- , cert X, cert D]
C → B : [[REP, IP A, NA] KX-] KC- ,certx, cert C]
B → C : [ERR, IPA, IPX, Nb] KB- , certb

Whenever a new node A enters a trusted third party provides a certificate with its IP address and timestamp with key. During route discovery a nonce is used in RDP, nonce is a random number which separate each control packet and helps nodes to identify each packet separately. The whole certificate is signed by the private key of T. the control packet send by source for destination is termed as RDP packet. A node broadcast RDP, destination address and nonce signed by private key of A with its certificate provided by T. when an intermediate node accepts this packet it verifies it if found true it append his own certificate with the sender certificate. The next node then verifies the packet from which it accepted the packet it removes the intermediate node certificate attached and put its own certificate this is followed by all the intermediate nodes. Now when it reaches destination it has two certificate the destination can verify from the node it accepted and the sender by the process and the content in certificate provided by T. the certifying authority (CA) published that certificate to A that conveys the destination node that the content of certificate is signed by T and it is a legal document and no content is false. The destination node replies the RDP packet by REP and follows the same rule for intermediate as well as for source which is done when RDP is broadcast, the only difference is that RDP is broadcasted but REP is unicast by destination towards the source.

Now with above discussion one can easily sum up the questions like how can we have a scenario with malicious node where third party is never compromised and providing an authentication phase while entering in MANET there is no guarantee that a true node will not do any malicious activity after authentication. The various cryptographic operations like certification and control packet verification makes this protocol too loaded. The control packet size will become an overhead in scenario when route establishing taking place continuously for a short period of time. With this ARAN does not provide any security to DDOS attack, wormhole attack and rushing attacks, hop count is not included in packet but it creates a situation where a short route is neglected.

5.2 SAR(Secure Aware Routing)[13]

In SAR security metric is implemented with RREQ message. This security metric has many parameters or trust levels when an intermediate node receives a request from source or any other intermediate node it check the security metric and if the node can provide that security it forward the packet else drop the packet. If an end to end path is found by the intermediate node it can reply back to source. SAR can be implemented with any on demand routing protocol.

If SAR find two routes both satisfying the security measure SAR will select the route with least hop count and if the hop count comes out to be equal it selects the optimal path. SAR works on security metric and hence that metric are just the trust levels which can easily be modified by any malicious node so SAR does not provide any stable security to routing and always have a chance of loopholes.

Table1. Security Metric of SAR

Property	Technique
Timeliness	Timestamp
Ordering	Sequence number
Authenticity	Password, Certificate
Authorization	Credential
Integrity	Digest, Digital Signature
Confidentiality	Encryption
Non-repudiation	Chaining Digital signature

5.3 SAODV (Secure AODV)[1,3,10,12,7]

SAODV is a secure AODV routing protocol which works on hash chain of hop count and digital signature verification at each intermediate node. In this paper proposed algorithm is compared with SAODV – Single signature extension as this protocol is widely famous and used because of its low routing load and providing reasonable security. In SAODV all mutable field, mutable fields are those field which are changed by the intermediate nodes, these fields are present in RREQ as well as RREP, the field is hop count which is protected by hash chain mechanism and other field which are non mutable are protected by digital signature. All security algorithms which uses asymmetric cryptography attain non repudiation or overcome attack like when a malicious node fabricate a RREP behalf of destination. As in AODV if any intermediate has an active route towards the destination it replies RREP to source that it has a active route and sender can choose this path to send data. So as RREP reaches source, source find it more appropriable and start sending data by this path and that malicious drop while forwarding data drops data packets, but in SAODV- single signature extension destination only can reply as RREP and RREQ messages are signed by private key of destination and source so no other intermediate node can reply in single signature extension of SAODV. Which makes SAODV a secure algorithm against blackhole attack but a second side which is hop count, a malicious node can unchanged the hop count and forward the packet that will also contribute in path attraction for destination as it could have a low hop count path. So SAODV protect blackhole attack from seq. number view but not with the hop count effect. Secondly hop can be easily incremented by malicious node in SAODV. SAODV and ARAN both are vulnerable to rushing attacks, in which a node forwards the packet as soon as it receives. SAODV is also vulnerable to various attack if it is conducted via hop count, rushing attack, increase in hop count, equal hop count. It uses digital signature verification at each node for verification of non-mutable information.

The algorithm how SAODV work is described below
Whenever a node generates a RREQ or RREP message it does the following steps:

- A random number is generated (seed).
- Setting of Max_Hop_Count field to the TTL value.

  Max_Hop_Count = TimeToLive
- Sets the Hash_value field to the hashed(SHA) seed value.

  Hash_value = seed
- Sets the Hash Function field to the identifier of the hash function that it is going to use.

  Hash_Function = h
- Calculates Top_Hash by hashing seed Max_Hop _Count times.

$$\text{Top\_Hash} \quad = \quad = \quad h^{\text{Max\_Hop\_Count}} \quad (\text{seed})$$

Where:
– h is the hash function.
hi(x) is the result of applying the function h to x i times.
Whenever an intermediate node receives a RREQ or RREP is does the following function:

- Applies the hash function h to the Maximum_Hop _Count minus Hop_Count_value times the value in the Hash field, and verifies that resultant value is equal to the value in the Top Hash field.

$$\text{Top\_Hash} == h^{\text{Max\_Hop\_Count} - \text{Hop Count}} (\text{Hash})$$

If equal then control packet is forward else drop.

- Before forwarding an intermediate node hash the hash_ field value for the next hop by doing one hash.

  Hash_value = h(Hash_Value)

6. PROPOSED WORK SE-AODV

We have used hash chain mechanism to protect the increment, decrement and forward of equal HOP_COUNT value which is mutable field in control packet. We have used hash scheme followed by digital signature verification to protect the non mutable information in control packet.

6.1 Proposed Algorithm

RREQ Packet format

```
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 |   Type   |J|R|G|D|U|  Reserved | Hop Count  |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|                    RREQ ID                     |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|             Destination IP Address             |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|          Destination Sequence Number           |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|              Originator IP Address             |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|           Originator Sequence Number           |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|                    Full_hash                   |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|               Signature Extension              |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 |                Encrypted_rno                 |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 |                   rno_hash                   |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 |                   Node_List                  |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

RREP Format

```
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Type    |R|A|   Reserved    |Prefix Sz|  Hop Count  |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |            Destination IP address              |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Destination Sequence Number              |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |              Originator IP address             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                 Lifetime                   |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |               Full_Hash             |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |            Signature Extension             |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        |              rno_hash             |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                Node_List              |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

RERR Format

```
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
          |   Type |N | reserved   | Dest count |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                unreachable destination IP address     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |       unreachable destination sequence number       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                |   Signature Extension   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The proposed algorithm uses a fully distributed certifying authority approach in which every node in network is itself its certifying authority. When a node enters a network during its boot time it will generate two set of public and private key. One set is of 1024 bit key and other set is of 64 bit key. Each set contain one public key and one private key. Suppose Source S want to establish secure path to destination D the algorithm work as follows

$PUB_A key_s$: Public key of Source
$PRV_A key_s$: Private key of Source
$PUB_B key_s$: Public key of Source
$PRV_B key_s$: Private Key of Source
$PUB_A key_D$: Public key of Destination
$PRV_A key_D$: Private key of Destination
$PUB_B key_D$: Public key of Destination
$PRV_B key_D$: Private Key of Destination
Set A key : 1024 bit
Set B key : 64 bit
h= Hash function : SHA1
RSA 1024 to generate Signature
RSA 64 to encrypt random number.

At source (S) :

For Mutable Field :

- Generates a random number : X
- Generates Hash of X → h(X) → h'(X)
- Assign value h'(X) to rno_hash field in RREQ
- Encrypts X with Public key(64 bit) $PUB_B key_D$ of Destination X→X'
- Assign value X' to Encrypted_rno field in RREQ.

For Non Mutable Field :

- Hash for all non Mutable field(Fields above Full_hash in RREQ)
  h(RREQ)→h_2'
- Assign h_2' to Full_hash field in RREQ packet
- Sign above (Full_Hash) with its private key (1024 bit) $PRV_A key_s$ and assign Signature extension.

At Intermediate nodes:

For First receiving intermediate node in path :

- Generate hash for received RREQ(Excluding field not included by Source) and Compare with Full_hash.
- Not EQUAL →DROP
- Append rno_hash and OWN ADDRESS →h(rno_hash,own address)→ h''
- Assign h'' to rno_hash
- Insert own address in NODE_LIST
- FORWARD

For all others receiving intermediate node in path:

- Intermediate node Address from which node received RREQ equal to node list last entry.
- NOT EQUAL → DROP
- Generate hash for received RREQ(Excluding field not included by Source) and Compare with Full_hash.
- Not EQUAL →DROP
- Append rno_hash and OWN ADDRESS →h(rno_hash,own address)→ h''
- Assign h'' to rno_hash
- Insert own address in NODE_LIST
- FORWARD

At Destination (D) :

- Intermediate node Address from which destination node received RREQ equal to node list last entry.
- NOT EQUAL ➔ DROP
- Digital Signature (1024 bit key) Verification(PUB$_A$key$_S$) → verification : ok
- Verification FAILS ➔DROP
- Decrypts the Random no with PRV$_B$key$_D$.(64 bit) ➔X
- Hash : h(X) , hashing and Continue appending address from node list and again hashing with previous hash ➔ Times HOP COUNT received➔hop_hash→h[………..''..'.h(X)]
- Compare rno_hash and hop_hash.
- EQUAL ➔ACCEPT else ➔DROP.

Destination Generate RREP:

- Excludes Encrypted_rno field from RREP.
- Hash for all non Mutable field(above Full_hash field) , h(RREP)➔h$_2$'
- Assign h$_2$' to Full_hash field in RREP packet
- Sign above with its private key(1024 bit) PRV$_A$key$_D$ and assign to Signtaure extension.
- Assign rno_hash of RREQ to rno_hash RREP.
- Assign Node_List of RREQ to Node_List of RREP.

For Intermediate Nodes :

- Check Entry after their own entry in Node_List , Compare from receiving address of Intermediate Node.
- NOT EQUAL ➔DROP
- Hash non mutable fields and compare with Full_Hash if Not EQUAL ➔DROP else Forward

For Source:

- Check First entry from Node_LIST and Intermediate node From which RREP received
- NOT EQUAL ➔DROP
- Digital Signature Verification(PUB$_A$key$_D$) ➔ verified : ok
- Verification Fails➔DROP
- Perform Hash of X " random number" followed by entries from NODE_LIST and last hash obtained by hashing ➔TIMES HOP COUNT received ➔Hop_Hash➔h[……''….(X)]
- Compare Hop_hash and rno_hash of RREP
- EQUAL ACCEPT➔Secure Path Established Else ➔DROP

6.2 Security Analysis of Proposed Algo

Suppose a malicious Scenario in which S wants to establish a connection to destination D and intermediate nodes in path are A M B. M is the malicious node.

S➔A➔M➔B➔D

6.2.1 Malicious node Forwards Decrement Hop Count(RREQ)

- Using Message Digest M cannot generate Previous hash.
- Using Encrypted X from Node_list ➔true hash rno_hash field cannot be regenerated.
- If not enter own address then ➔ Detected at next intermediate node.
- Malicious node removes last entry and not enter own address ➔ rno_hash will not come equal at destination.
- If Enter in Node_list and decrement Hop Count ➔ Detected at Destination➔Hop Count time hash at destination .

6.2.2 Malicious node Forward Equal Hop Count(RREQ)

- If not enter own address then ➔ Detected at next intermediate node.
- If Enter in Node_list and forwards same hop count ➔ Detected at Destination➔Hop Count time hash at destination
- If remove any before node entry➔rno_hash change and detected at destination.

6.2.3 Malicious node forwards increment Hop Count(RREQ)

- It Has to enter 2 fake entry including M if not ➔ detected at destination hop count times. It can enter fake values including itself.
- Enter Fake entry after MXY if does ➔Detected at next intermediate node.
- Enter fake Entry before XYM➔Detected when RREP is forwarding towards source at intermediate node, if malicious change node list entry the rno hash will change and this change will be detected at source.

6.2.4 Malicious node Forward Increment, Decrement or Equal Hop count(RREP)

- If Malicious node forward Equal, increment or decrement hop count ➔ detected at source hop count time hash at destination.
- If it changes Node_list value to make respective hop value acc to node list items then Rno_hash will change which cannot be regenerated by intermediate nodes and thus will be detected at source.

6.2.5 Malicious node Generate fake RERR.

- Protected by Signature Extension so can be detected when it generate fake RERR

6.2.6 Malicious node Changing nonmutable field.

- Non Mutable field are protected by Full_hash at intermediate nodes, and if Full_hash is compromised by malicious node then false packet can be detected at destination by signature verification.

The proposed algorithm secure all three types of attacks on hop count which is very much attracted to malicious node to execute various attacks like rushing attack. Proposed SE-AODV secure non-mutable information by hash method at intermediate nodes and digital signature verification at destination.

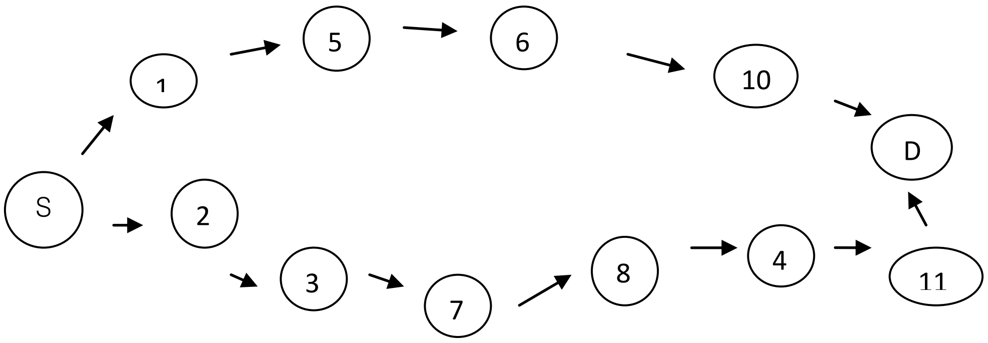

Fig 2: Sample Topology

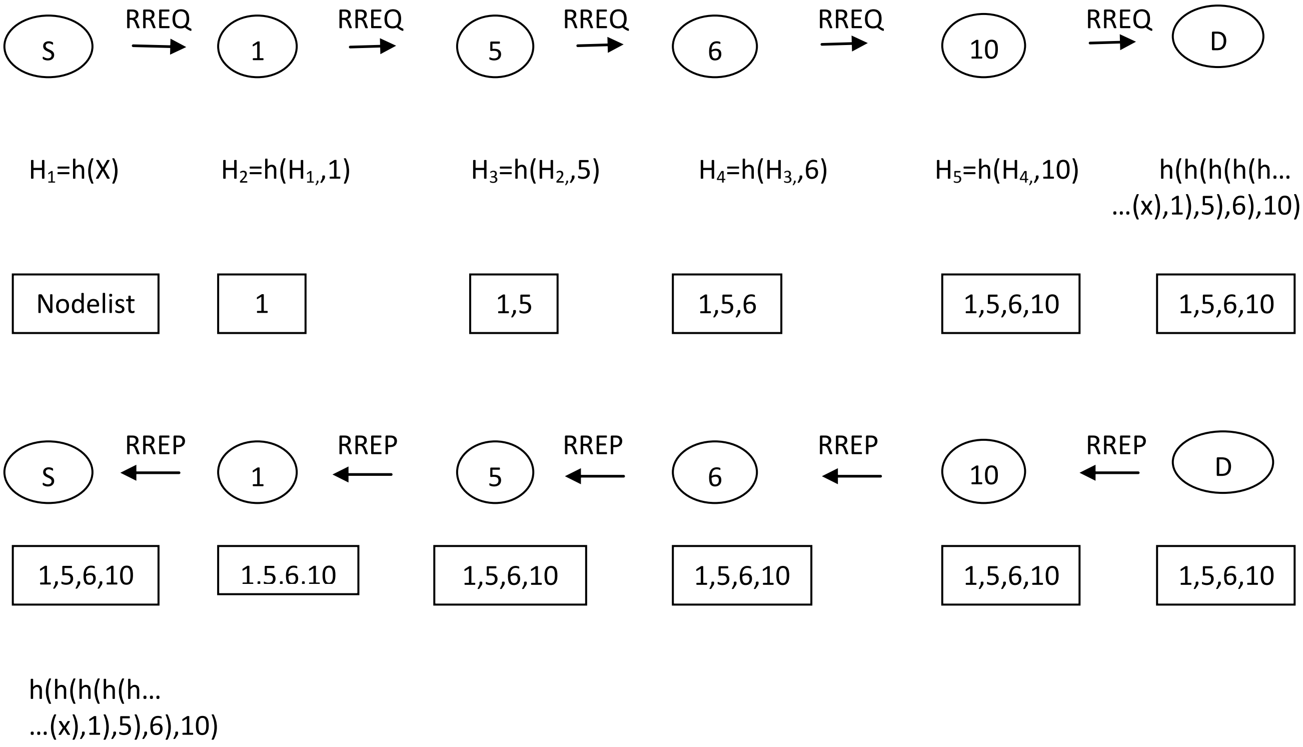

Fig3 : Securing Mutable information

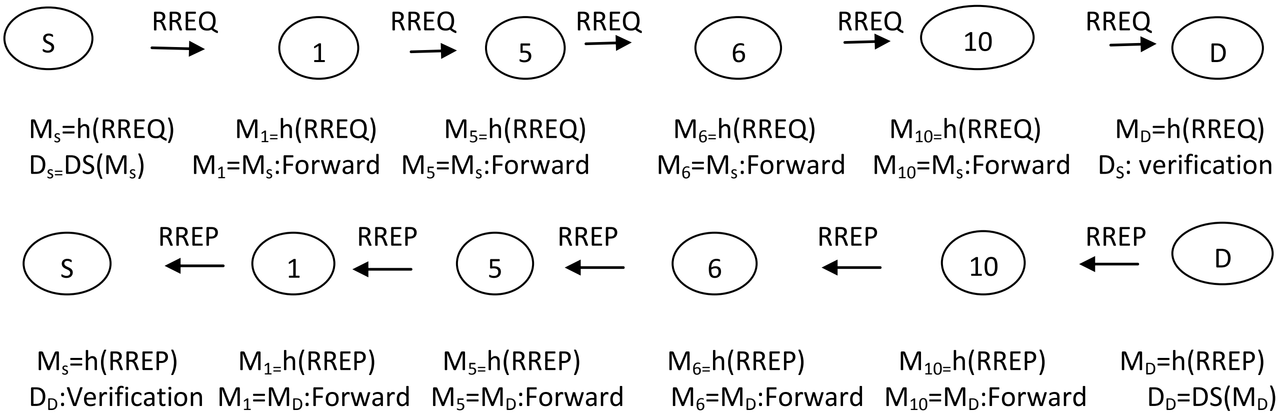

Fig 4: Securing Non-Mutable information

7 RESULTS

Same key size is followed for SAODV and proposed algorithm of 1024 bit for digital signature.

7.1 Non Malicious Scenario

Table 2. Parameters of Scenario

Nodes	12
Pause Time	1.0
Max Speed	5.0
CBR Traffic	10
Simulation time	200,400,600,800,1000
Area	1200 X 1200
Movement pattern	Non-random

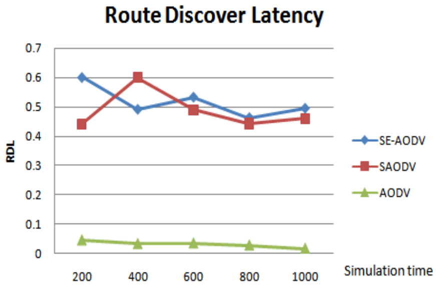

Fig 5 : Route Discovery latency

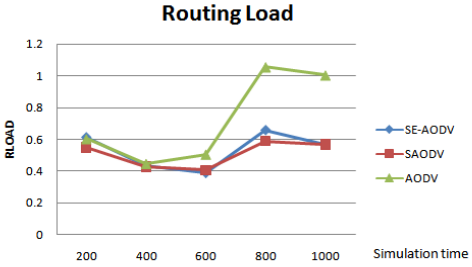

Fig 6 : Routing Load

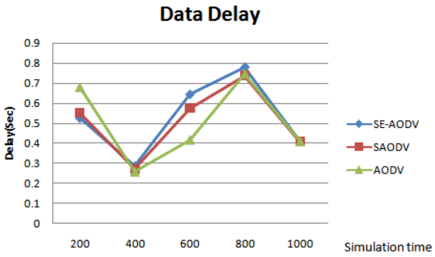

Fig 7 : Data Delay

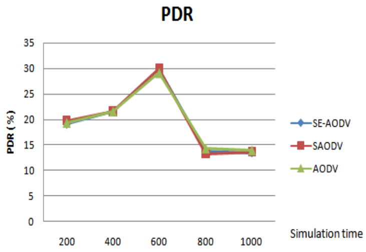

Fig 8 : PDR

From above Graph of non malicious scenario we can conclude that PDR comes out same for AODV SAODV and proposed SE-AODV. The slight increase in route discovery latency and data delay which is due to the more secure approach and routing overhead which result in slight increase which is reasonable tradeoff for security.

7.2 Malicious Scenario

Table 3 : parameters for Malicious Scenario

Nodes	10
Pause Time	3.0
Max Speed	5.0
CBR Traffic	10
Malicious Node	0%,10%, 20%, 30%,40%
Area	500 X 500
Movement pattern	Non-random
Simulation Time	200 sec

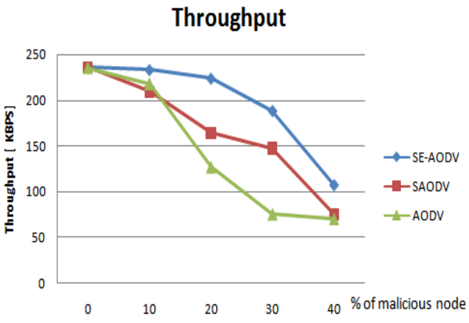

Fig 9 : Throughput

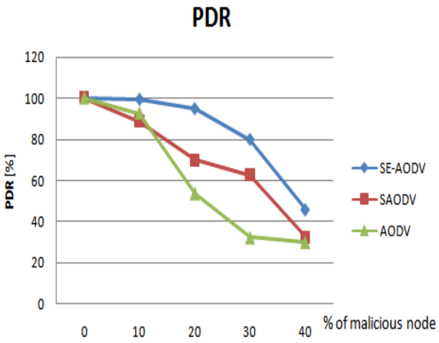

Fig 10 : Packet Delivery Ratio

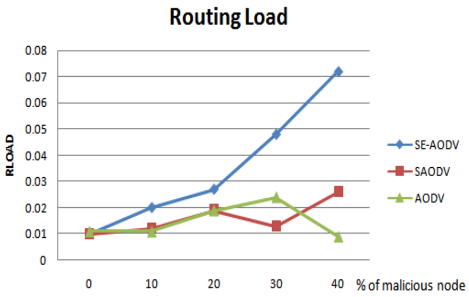

Fig 11 : Routing Load

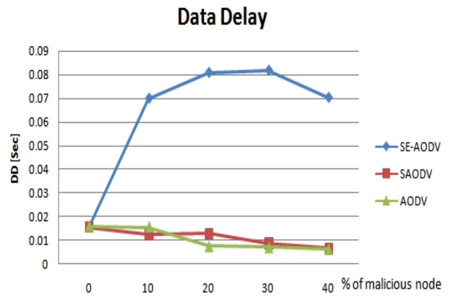

Fig 12 : Data Delay

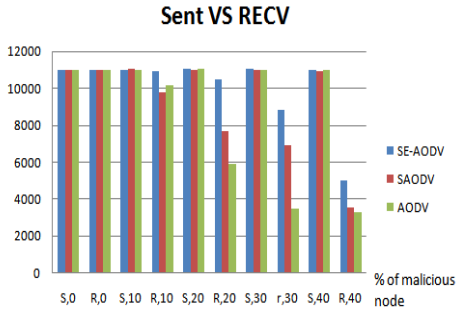

Fig 13 : Sent vs Recv packets

8.0 CONCLUSION

From above graph in malicious scenario it can be easily conclude that when there is increase of malicious node in any scenario proposed SE-AODV proves to be more Secure with that delivering a high throughput, PDR and high number of receive packets as compared to SAODV. As in SAODV a malicious node can come in path through loopholes of hop count security in SAODV, our approach proves to be more secure as it provide a alternate malicious free path to source.

Table4 : Comparison SAODV vs SE-AODV

Attack	SAODV	SE-AODV
Intermediate Nodes Verify Control Message	Yes	yes
Prevent From decrease Hop Count	Yes	yes
Prevent From same Hop Count Value	No	Yes
Prevent from Increase Hop Count value	No	Yes
Prevent From Route Modification attack	No	Yes
Prevent From Rushing attack	No	Yes
Detect Malicious Node	No	Yes

9. FUTURE WORK

The proposed scheme covered many attacks but for further giving more advance shape to this work a intrusion detection system for MANET can be designed which can focus on NODE_LIST field of control packet, a trackback IP approach can be designed which can policy drive malicious node for further connection in network. As this approach can detect nodes increasing hop count, malicious node can be detected which don't want to come in path for other's connection, a intrusion system can isolate these nodes from network and increase of the network performance.

10. REFERENCES

[1] Songbai, L., Longxuan, L., Kwok-Yan, L. and Lingyan, J. 2009. SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack, IEEE.

[2] Sanzgiri, K., LaFlamme,D., Dahill, B. and Levine, B.N. 2005. Authenticated Routing for Ad Hoc Networks, IEEE.

[3] Mao, L. and Ma, J. 2008. Towards Provably Secure On-Demand Distance Vector Routing in MANET, International Conference on Computational Intelligence and Security.

[4] Zapata, M.G. 2006. Securing and Enhancing Routing Protocols for Mobile Ad hoc Networks, Master Thesis. Technical University of Catalonia Universitat Polit`ecnica de Catalunya Barcelona.

[5] Wu, B., Chen, J., Wu, J. and Cardei, M. 2006. A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks, Springer

[6] Hu, Y. and Perrig, A. 2005. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc. Springer

[7] Weng, J. 2008 Security Issues in Mobile Ad Hoc Networks.

[8] Pirzada, and Donald, M. 2005. Secure Routing with the AODV Protocol. IEEE Asia-Pacific Conference on Communications, Perth, Western Australia, pp.57-61.

[9] Wang, W., Lu, Y. and Bhargava, B. 2003. On Security Study of Two Distance Vector Routing Protocols for Mobile Adhoc Networks. IEEE International Conference on Pervasive Computing and Communications (PerCom'03).

[10] Jin L., Zhang, Z. and Z. 2006. Performance Comparison of the AODV, SAODV and FLSL Routing Protocols in Mobile Adhoc Networks, 5th Workshop on the Internet, Telecommunications and Signal Processing (WITSP2006).

[11] Alaa, S., Dalghan, Mohamad, M., Gamloush, Raji M. Z., and Yasser, M. Shaer, "Securing Mobile Adhoc Networks.

[12] Lin, Y., Hamed M.R., Vincent, W.S., and Wong, 2005. Experimental Comparisons between SAODV and AODV Routing Protocols, WMuNeP'05,, 1-59593-183-X/05/0010, Montreal, Quebec, Canada, ACM.

[13] Cerri, D. and Ghioni, A. 2008. Securing AODV: The A-SAODV Secure Routing Prototype. Communications Magazine, IEEE, Vol.-46, Issue. 2, pp. 120-125, February 2008.