International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 3
ISSN: 2454-4248
155 – 161

Performance Evaluation of DSR, AODV and SAODV Routing Protocol in MANETs

Dalip
Maharishi Markandeshwar (Deemed to be University)
Mullana, Ambala (Haryana) India
dalipkamboj@mmumullana.org

Deepika, Natasha Gupta and Ashima Mehta
Maharishi Markandeshwar (Deemed to be University)
Mullana, Ambala (Haryana) India
Dronacharay College of Engineering, Haryana (India)
deepika.kalyan@mmumullana.org,natasha.gupta@mmumullana.org, *ashimamehta03@gmail.com*

***Abstract*—** There have been various privileged routing protocols developed for mobile ad hoc networks. Mobile ad hoc networks are support to several security threats due to its dynamic and changeable topology and self configurable features. In this paper, Dynamic Source Routing (DSR) routing protocol was selected as the core of the whole environment simulations. SAODV (Secured Ad hoc On Demand Vector routing) is one of the advanced existing privileged mechanisms, which provide security to AODV using digital signature and hash chain techniques. There have been various secure routing protocols proposed for the mobile ad hoc network. Protocols are used two standard techniques like simulation and security analysis. The performance of these protocols is evaluated using GlomoSim simulator on different performance metrics such as Packet Delivery Fraction (PDF), Average End-to-End Delay and Throughput. To minimize the processing overhead, delays and to maximize the routing throughputs still need further optimization in secure routing protocols (such as SAODV)

.Keywords- *Simulation experiments, Security, Ad hoc Network, Routing protocol, DSR, AODV and SAODV*

*****

I. INTRODUCTION

Today, a wireless technology is an emerging field for research [1]. The wireless equipments and service providers are available to the end user at low cost. The cost of installation of wireless network is less as compared to wired networks. Networks which support ad hoc architecture are called wireless mobile ad hoc networks [1]. This network is known as self-forming and self-healing because these networks do not required human intervention. It is possible that nodes may have lost connectivity with each other if they move out from their transmission range. It is also possible in some applications nodes may lose the connectivity with other nodes that causes run out of battery or may be destroyed. In mobile ad-hoc network the network is reestablished without any human intervention. Routing plays a vital role in wired or wireless networks [1]. Routing protocols in wired networks are not required to manage the mobility of nodes within the system. They do not minimize the communication overhead so it is cause of required high bandwidths. In ad-hoc network each device acts as a router. This can be broadly classified into three categories: table driven routing protocol [2], reactive or on-demand driven routing protocol and hybrid routing based on the routing information update mechanism.

In the table driven routing protocols, every node maintains the network topology information in the form of routing tables by periodically exchanging routing information. Routing information is generally flooded in the whole network. Whenever a node requires a path to a destination, it runs an appropriate path-finding algorithm on the topology information it maintains. For example DSDV [5], WRP [6], CGSR [7], STAR [8], OLSR [9], FSR [10], HSR [10] and GSR [11]. The Reactive or On-demand routing protocols do not maintain the network topology information. They obtain the necessary path when it is required, by using a connection establishment process. Hence these protocols do not exchange routing information periodically. For example DSR [12], AODV [13], ABR [14], SSA [15], FORP [16], PLBR [17]. The Hybrid routing protocols combine the best features of the above two categories. Nodes within a certain distance form the node concerned, or within a particular geographical region, are said to be within the routing zone of the given node. For routing within this zone, a table-driven approach is used. For example CEDAR [18], ZRP [19] and ZHLS [20].

The above protocols do not provide any security mechanism against basic security services wiz authentication, confidentiality, integrity, authentication, non-repudiation and availability. Many protocols have been introduced to provide basic security services. For example SAODV [21], SAR [23], A-SAODV [24], MS-AODV [25], RAODV [26], TAODV [27], SRPM [3], SecureAODV [4] and CBRP [22]. The performance analysis of various routing protocols with security mechanisms is presented here. The performance comparison of routing protocols such as Dynamic Source Routing (DSR), Ad hoc On Demand Distance Vector (AODV) and Secure Ad-hoc on Demand Distance Vector (SAODV) routing are discussed in this paper. SAODV is secure routing protocol uses public key cryptography to secure the information delivery. It also provides integrity and authenticity of routing messages (RREPs, RREQs, and RERRs).

This paper is discussed as follows. The information about base routing protocol DSR is shown in section II (A). The information about the routing protocol AODV is presented in section II (B). The secure routing protocol SAODV information is presented in section II (C). The section II (D) provides the comparison of DSR, AODV and SAODV. The section III describes the Experimental setup and Results. The conclusion of the paper is describes in section IV.

II. RELATED WORKS

A. Dynamic Source Routing (DSR)

The dynamic source routing of packets [12] between source and destination is uses by DSR. The routes are generated when

 ISSN: 2454-4248
155 – 161

required. To create and maintain the routes there is a no need of periodic routing traffic. When the data packets are originated by a node the source routing puts all the hops in the header of packets. It is divided into two mechanisms route discovery and route maintenance. When there are no routes to destination route discovery is used by nodes to discover them. For route discovery, information is caught from adjacent host by protocol when required without any periodic router advertisement. In case of route broken due to failures or movement of node, route maintenance is needed to discover either a different existing (less optimal) route or the node may initiate route discovery for discovering a new route. It provides a number of potential advantages over conventional routing protocols such as distance vector in an ad hoc network.

B. Ad hoc on demand distance vector (AODV)

AODV is an improvement on DSDV [5]. The creation feature of this system requires minimum number of broadcasts. For route finding, a reactive [13] approach is used in this system as establishment of a route is done only when source node need to transmit data packets. For identification of path, destination sequence is used by the system. Storage of information regarding the upcoming node corresponding to each data transmission occur in source node and intermediate node when no route is available for required destination, source node send the route request packet in network. Updating in the path information is done only when the last destination sequence number stored at node is lesser then the current packet received. After receiving the RREQ by intermediate node, either forwarding or preparing route reply (RREP) to confirm the valid route to destination by doing comparison of sequence number at intermediate node, validity of route is checked. If BcastID-SrcID pair, indicates multiple times receiving of RREQ, then the duplicate copies are discarded. A timer is set to delete this entry in case RREP is not received before the time expires. In this way, active path is stored at intermediate [29] node because source routing of data packets is not employed by AODV like DSR [12]. As RREP packet is received by node, information about the last node from which the packet was obtained is also stored so that data packet is forwarded to next node which is the next hop towards the destination. AODV protocol has two phases: Route discovery and route maintenance. In route discovery phase, when intermediate node receives RREP packet, it may forward RREQ packet or prepare route Route Reply (RREP) packet. When a valid route to destination is available in that Cache the (SId,BId) pair is used to avoid duplicate copies to verify a particular RREQ. For transmission RREQ packet previous node address and its BId is also entered by each intermediate node. In route discovery two message formats is there. Route Request (RRQ) Message Format and Route Reply (RREP) Message Format. The step by step procedure of route discovery is given below.

Algorithm 1: Route Discovery algorithm for AODV

1. Route Request (RREQ) is broadcasted by the Source node'S' to all its neighbours.
2. Neighbour nodes check the RID (ROUTE-ID) after receiving the Route Request (RREQ).
3. It discards the packet if Route Request (RREQ) packet has been already received by the neighbour node.
   Otherwise, a reverse path is established between the source and the neighbour node.
4. In case if node is not the destination or having no path to the destination, then
   repeat step 1 and onwards (neighbour node in place of source node)
5. When destination node or node having path to the destination is find by the Route Request (RREQ) packet, the destination node unicast the Route Reply (RREP) towards the source node.
6. When the Route Reply (RREP) packet reach to the source node following the path of intermediate nodes, the route is established in the reverse way i.e. from the destination to the source
7. The route is established, and the data packets can be sent through the established route.

In to the route maintenance phase whenever a node finds out a link break (via link layer acknowledgements or HELLO messages), it broadcasts an RERR packet (in a way similar to DSR) to notify the source and the end nodes. RERR message is used by nodes for invalidating routes they are aware of when links supporting those routes break. This could happen due to node movements, increased link error rate, and so on. When a node loses connectivity to one of its neighbors, it sends a RERR message to other nodes that make use of the path through the "lost" neighbor. The RERR message contains the list of destinations that have become unreachable. The RERR may be broadcast or unicast to the affected nodes.

Security Issues in AODV

In this section, we analyze the security threats and describe the requirements for AODV routing protocol to mitigate these threats. Several attacks can be launched against the AODV and DSR routing protocol:

Wormhole Attack: The wormhole attack is a severe type of attack in which two colluding malicious nodes can tunnel packets through a "tunnel" or vertex cut in the network. **Black hole attack:** In this type of attack, a node advertises a zero metric for all destinations causing all nodes around it to route packets towards it. The AODV protocol is vulnerable to such an attack. **Message dropping attack:** Into the message dropping attack both attackers and selfish nodes can intentionally drop some (or all) routing and data messages. **Message tampering attack**: In this type of attack, an attacker can alter the content of routing messages and forward them with falsified information.

C. Secure Ad hoc on demand distance vector Routing (SAODV)

A secure version of AODV [13] is called Secure AODV (SAODV). There are several security principles such as integrity, authentication, and nonrepudiation of routing data. There are two schemes for securing AODV. The first scheme involves nodes signing the messages e.g. Route Request

 ISSN: 2454-4248
155 – 161

(RREQ), Route Reply (RREP). This allows other nodes to verify the originator of the message. This scheme can be used for protecting the portion of the information in the RREQ and RREP messages that does not change once these messages are created. However, RREQ and RREP messages also contain a field (namely the hop count) that needs to be changed by every node. Such mutable information is ignored by the creator of the message when signing the message. The second scheme of SAODV [21] [31] is used for protecting such mutable information. This scheme leverages the idea of hash chains. Signing routing messages implies that the various nodes need to possess a key pair that makes use of an asymmetric cipher. In addition, nodes in the network also need to be aware of the authentic public keys of the other nodes. Two mechanisms are used to authenticate the AODV routing data: hash chains and signatures. In SAODV [28] signatures when calculating signatures, Hop Count field is always zeroed, because it is a mutable field. In the case of the Signature for RREP field of the RREQ Double Signature Extension, what is signed is the future RREP message that nodes might send back in response to the RREQ. To construct this message it uses the values of the RREQ and the Prefix Size (the RREP field that is not derivable from the RREQ but not zeroed when computing the signature. The SAODV Hash Chains are used in SAODV to authenticate the hop count of the AODV routing messages (not only by the end points, but by any node that receives one of those messages). Every time a node wants to send a RREQ or a RREP it generates a random number (seed). Selects a Maximum Hop Count. Maximum Hop Count SHOULD be set to the TTL value in the IP header, and it SHOULD never exceed its configuration parameter NET_DIAMETER. The Hash field in the Signature Extension is set to the seed. The Top Hash field is set to the seed hashed Max Hop Count times. Every time a node receives a RREQ or a RREP it verifies the hop count by hashing Max Hop Count - Hop Count times the Hash field, and checking that the resultant value is the same than the Top Hash. If the check fails, the node SHOULD drop the packet.

Algorithm 2: Route Discovery algorithm for SAODV
1. The Route Request (RREQ) is broadcasted by the source node.
2. Hash function is used to signs all non mutable fields by sender.
3. Sender signs mutable field such as Hop count with its private key.
4. RREQ is broadcasted to all neighbour.
5. The RREQ is received by the intermediate node.
6. Node verifies the signature with its public key.
7. If (node address is equals to destination address)
{
Then RREP is generated.
Unicast RREP to the neighbour which is in the Reverse path for the source node.
}
Else if (node address not equal to destination address)
{
Then node is an intermediate node of the route.
}

8. If (both verify messages are equal)
{
Then RREQ message is accepted.
}
Else if (both verify messages are not equal)
{
Then RREQ message is rejected.
}

D. Comparison of DSR and AODV and SAODV

TABLE I. A COMPARISON BETWEEN DSR, AODV AND SAODV ON THE BASIS OF THEIR FEATURE

Protocol Feature	DSR	AODV	SAODV
Destination sequence numbers	*Not used*	*Used*	*Used*
Secure	*Not Secure*	*Not Secure*	*Secure*
Routing mechanism	*Source routing – Multiple route caches for each destination*	*Table driven – one entry per destination. Sequence numbers used for*	*Table driven – one entry per destination. Sequence numbers used for*
Route storage mechanism	*Using route caches*	*Using routing tables*	*Using routing tables*
Timers	*Not Used*	*Used*	*Used*
Multiple Route caches	*Yes*	*No*	*No*
Link Layer acknowledgements	*Not Required*	*Required*	*Required*

III. EXPERIMENTAL SETUP AND RESULTS

A. Simulation Model and Parameters

The network simulator Glomosim [30] is used for experimental study. For the experimental setup we use the 40 and 80 nodes. This paper shows the performance comparison between DSR, AODV and SAODV using different performance metrics. Table II shows the simulation parameters and their values for DSR, AODV and SADOV simulation.

TABLE II. SIMULATION PARAMETER VALUES

NUMBER OF NODES	*40, and 80*
SIMULATION-TIME	*20, 40, 60, 80 and 100 in second*
SEED	*1*
TERRAIN-DIMENSIONS	*1500*1500*
NODE-PLACEMENT	*UNIFORM*
RADIO-FREQUENCY	*2.4e9 heltz*
RADIO-BANDWIDTH	*2000000 bits per second*
RADIO-TX-POWER	*8.0 dBm*
MAC-PROTOCOL	*802.11*
NETWORK-PROTOCOL	*IP*

ISSN: 2454-4248
155 – 161

B. Performance Metrics

Three performance metrics for the best simulation results such as Packet Delivery Fraction (PDF), Average End-to-End Delay and Throughput are used here.

Packet Delivery Fraction (PDF): It is a ratio of the data packets delivered to the destinations to those generated by the Constant Bit Rate (CBR) sources. The PDF denoted by P and calculated as follow:

$$P = \frac{\sum_{i=1}^{n} N_i^s}{\sum_{i=1}^{n} N_i^r} \times 100$$

where N_i^s are the number of application data packets sent by the sender and N_i^r are number of application data packets received by the receiver, respectively for the i^{th} application, and n is the number of applications.

Average End-to-End Delay: This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times. The average end-to-end delay of the application data packets, denoted by D, is calculated as follow:

$$D = \frac{\sum_{i=1}^{n} d_i}{n}$$

where d_i is the average end-to-end delay of data packets of i^{th} application and n is the number of CBR applications.

Throughput: It is equal to the average performance of all nodes during simulation. It is a calculation of bits per second processed by each node. The throughput, denoted by T, is calculated as follow:

$$T = \frac{\sum_{i=1}^{n} \left(N_i^s + N_i^r \right)}{n}$$

Where N_i^s are the numbers of application data packets sent by the sender and N_i^r are number of application data packets received by the receiver, respectively for the ith application, and n is the number of applications.

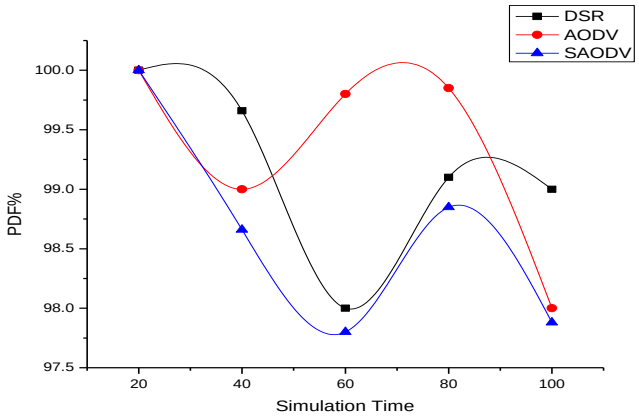

Figure 1: Packet Delivery Fraction (in percentage) for 40 nodes

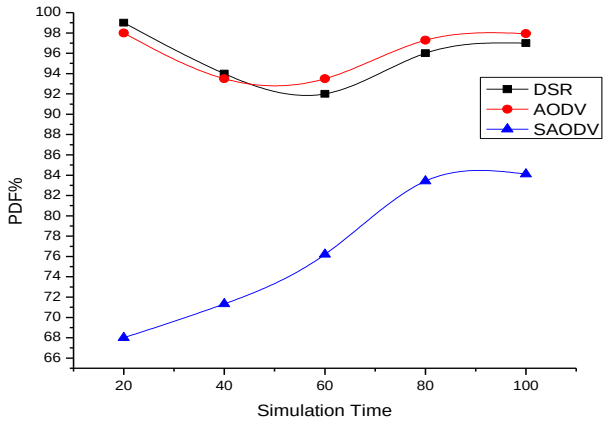

Figure 2: Packet Delivery Fraction (in percentage) for 80 nodes

DISCUSSION

From the Figure 1, the result shows that AODV outperform as compare to SAODV and DSR in PDF percentage. It means that AODV produce more PDF% compared to SAODV in total runtime of the simulations. It is quite clear that at simulation time 20 DSR, AODV and SAODV decreased but after simulation time 40 only AODV increased. In Figure 2, PDF percentage of DSR and AODV is higher as compared to SAODV.

ISSN: 2454-4248
155 – 161

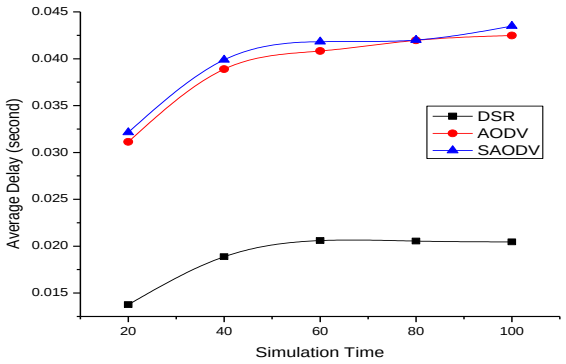

Figure 3: Average End-to-End Delay for 40 nodes

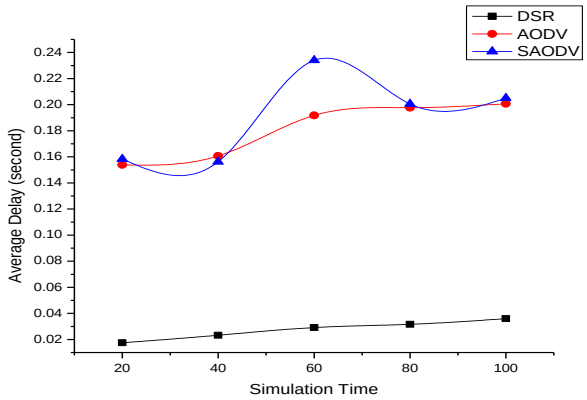

Figure 4: Average End-to-End Delay for 80 nodes

DISCUSSION

From the simulation result it has been observe that in Figure 3 and Figure 4 SAODV produce large average end-to-end delay compared DSR, AODV. It shows that while increasing the number of nodes the average delay was increased in case of SAODV. It indicates that security counter measures have negative effect on performance of routing protocols.

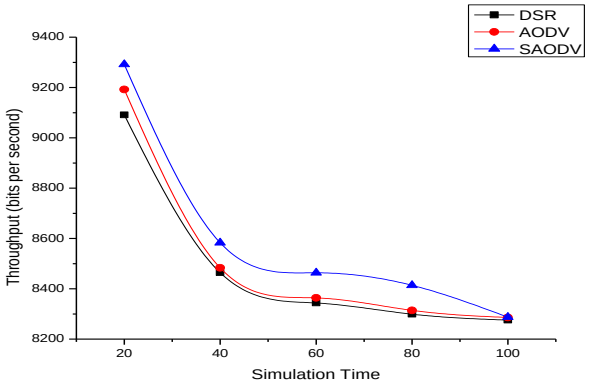

Figure 5: Throughput (bits per second) for 40 nodes

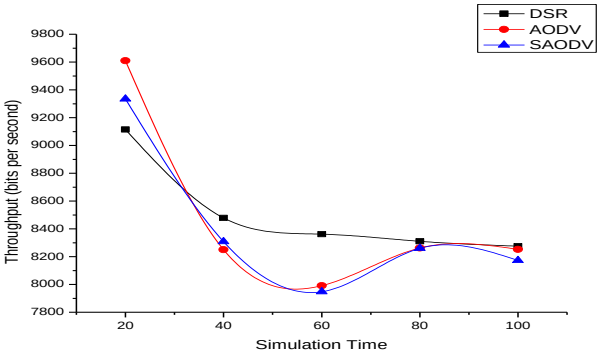

Figure 6: Throughput (bits per second) for 80 nodes

DISCUSSION

It is quite clear that the throughput of SAODV is higher then the DSR and AODV in Figure 5 due to overhead of security counter measure, but in Figure 6 at simulation time 40 to 80 the throughput of DSR is higher then the AODV and SAODV.

IV. CONCLUSIONS

The performance comparisons between DSR, AODV and SAODV routing protocols under the different simulation environments is presented here. On the basis of different performance metrics evaluate the performance of these protocols in best possible way. The expected results are obtained after performing the simulation experiment. Secured ad hoc routing protocols are a necessity for securing the routing of data. To have security in the routing, one should sacrifice the performance of the data transmission. SAODV routing protocol have major impacts on the performance by using the security techniques like digital signature and hash chains. So it will use more processing power and time. Secure routing protocols available today such as SAODV still need further optimizations to minimize the processing overhead, delays and to maximize the routing throughputs.

REFERENCES

[1] Farooq anjum and Petros Mouchtaris,"Security for wireless ad hoc networks," John Wily, 2007.

[2] C.Siva Ram Murthy and B. S. Manoj,"Ad hoc wireless networks: Architecture and Protocols". Prentice Hall Publishers, ISBN 013147023X, May 2004.

[3] S. Khan and K.K. Loo,"SRPM Analysis in the Presence of Sinkhole attack in Hybrid Wireless Mesh Networks," In International Journal of Research and Reviews in Ad Hoc Networks Vol. 1, No. 1, March 2011.

[4] Suman Deswal and Sukhbir Singh,"Implementation of Routing Security Aspects in AODV," In International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010.

[5] C. E. Perkins and P. Bhagwat,"Highly Dynamic Destination-Sequenced Distance-vector-Routing (DSDV) for Mobile Computers," SIGCOMM, UK, pages 234-244, 1994.

[6] S. Murthy and J.J. Garcia-Luna-Aceves,"An Efficient Routing Protocol for Wireless Network", In ACM Mobile Networks and Applications Journal, Special Issue on Routing in Mobile Communication Networks, vol. 1, no. 2, pages 183-197, October 1996.

[7] C. C. Chiang, H. K. Wu, W. Liu, and M. Gerla,"Routing in Clustered Multi-Hop Mobile Wireless Netwroks with Fading Channel," Proceedings of IEEE SICON 1997, pp. 197-211, April 1997.

[8] J.J. Garcia-Luna-Aceves and M. Spohn,"Source-Tree Routing in Wireless Networks," Proceedings of IEEE ICNP, Pages 273-282, October 1999.

[9] T. Clausen and P. Jacquet, eds,"Optimized Link State Routing Protocol (OLSR)," IETF RFC 3626, October 2003.

[10] A. Iwata, C. C. Chaing, G. Pei. M. Gerla, and T.W. Chen,"Scalable Routing Strategies for Ad Hoc Wireless Networks," In IEEE Journal on Selected Areas in Communications, vol. 17. no. 8, pp. 1369-1379, Augest 1999.

[11] T.W. Chen and M.Gerla,"Global state Routing: A New Routing Scheme for Ad Hoc Wireless Networks," Proceeding of IEEE ICC 1998, pp. 171-175, June 1998.

[12] D. Johnson and D. Maltz.,"Dynamic source routing in ad-hoc wireless networks routing protocols," In Mobile Computing, pages 153-181. Kluwer Academic Publishers, 1996.

[13] C.E.Perkins and E.M.Royer,"Ad hoc On-Demand Distance Vector Routing," Proc. 2nd IEEE Workshop of Mobile Comp. Sys. and Apps., pages 90-100, Feb. 1999.

[14] C.-K. Toh.,"Associativity-based routing for ad-hoc mobile networks," WirelessPersonal Communications, 4(2):103-139, 1997.

[15] R.Dube, C.D.Rais, K.Y. Wang and S.K. Tripathi,"Signal Stability-Based Adaptive Routing for Ad Hoc Mobile Networks," IEEE Personal Communications Magazine, Pages 36-45, February 1997.

[16] W. Su and M.Gerla,"IPv6 Flow Handoff in Ad Hoc Wirless Networks Using Mobility Prediction," Proceeding of IEEE GLOBECOM, Pages 271-275, December 1999.

[17] R.S. Sisodia, B.S. Manoj, and C. Siva Ram Murthy,"A Preferred Link-Based Routing Protocol for Ad Hoc Wireless Networks," In Journal of Communication and Networks, vol. 4, no. 1, pp. 14-21, March 2002.

[18] P. Sinha, R. SivaKumar, and V. Bharghavan,"CEDAR : A Core Extraction Distributed Ad Hoc Routing Algorthm," In IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1454-1466, Augest 1999.

[19] Z. J. Haas,"The Routing Algorithem for the Reconfigurable Wireless Networks, " Proceedings of ICUPC 1997, vol. 2. pp. 562-566, October 1997.

[20] M. Joa-Ng and I. T. Lu,"A Peer-to-Peer Zone Based Two Level Link State Routing for Mobile Ad Hoc Networks, " IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1415-1425, Augest 1999.

[21] Manel Guerrero Zapata,"Secure Ad hoc On-Demand Distance Vector (SAODV) Routing," draft-guerrero-manet-saodv-06.txt, September 5, 2006.

[22] Seyed Amin Hosseini Seno, Rahmat Budiarto andTat-CheeWan,"A Secure Mobile Ad hoc Network Based on Distributed Certificate Authority," In King Fahd University of Petroleum and Minerals 2010, 15 January 2011.

[23] R. Kravets, S. Yi, and P. Naldurg,"A Security-Aware Routing Protocol for Wireless Ad Hoc Networks," In ACM Symp. On Mobile Ad Hoc Networking and Computing, 2001.

[24] R Alekha Kumar Mishra and Bibhu Dutta Sahoo,"A Modified Adaptive-Saodv Prototype For Performance Enhancement In Manet," In International Journal Of Computer Applications In Engineering, Technology And Sciences (Ij-Ca-Ets), Volume 1 : Issue 2 , Page: 443, April '09 – September '09.

[25] Tamanna Afroze, Saikat Sarkar, Aminul Islam and Asikur Rahman," More Stable Ad-hoc On-Demand Distance Vector Routing Protocol," In 978–1–4244–2800–7/09/$25.00 ©2009 IEEE.

[26] Sandhya Khurana, Neelima Gupta and Nagender Aneja ,"Reliable Ad-hoc On-demand Distance Vector Routing Protocol," In Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06) 0-7695-2552-0/06 $20.00 © 2006 IEEE.

[27] Xiaoqi Li, Michael R. Lyu, and Jiangchuan Liu ,"A Trust Model Based Routing Protocol for Secure Ad Hoc Networks," In IEEEAC, 0-7803-8155-6 © 2004 IEEE.

[28] Alekha Kumar Mishra andBibhu Dutta Sahoo," A Modified Adaptive-SAODV Prototype for Performance Enhancement in Manet," In International Journal of Computer Applications in Engineering, Technology and Sciences (ij-ca-ets), April '09 – September '09.

[29] Rakesh kumar, Siddharth Kumar, Sumit Pratap Pradhan and Varun Yadav," Modified route-maintenance in AODV Routing protocol using static nodes in realistic mobility model," In International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 4 Apr 2011.

[30] X. Zeng, R. Bagrodia and M. Gerla,"Glomosim: A library for parallel simulation of large-scale wireless networks," In Proceedings of the 12th Workshop on Parallel Distributed Simulations, 1998.

[31] Dalip Kamboj, Pankaj Kumar Sehgal and Rajinder nath," Performance evaluation of secure routing in Ad-hoc network environment", Recent Advance in Information Technology, IEEE International Conference, ISM Dhanbad, Jharkhand, March 15-17, 2012.

APPENDIX

A. AODV MESSAGE FORMATS

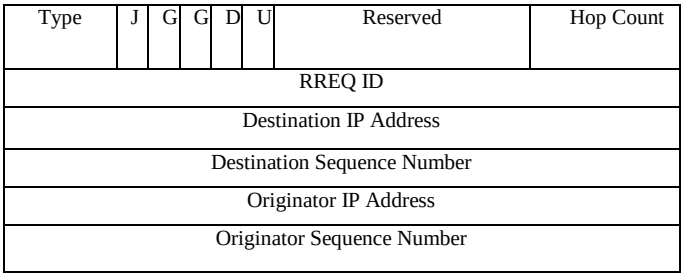

Figure 7: Route Request (RREQ) message format
Mutable fields: Hope Count

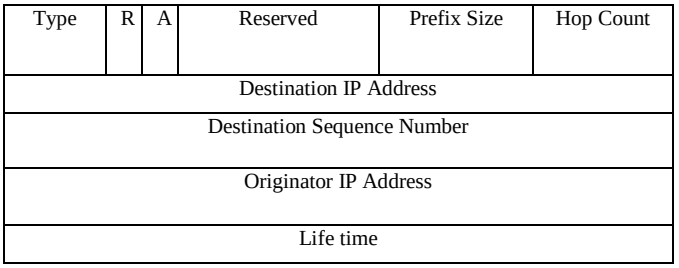

Figure 8: Route Reply (RREP) message format
Mutable fields: Hope Count

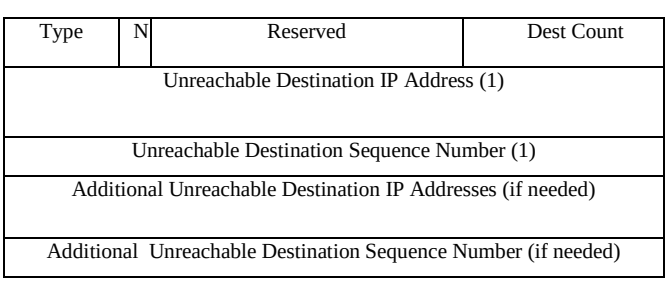

Figure 9: Route Error (RERR) message format

 ISSN: 2454-4248
155 – 161

Mutable fields: None

B. . SECURE AODV EXTENSIONS

Type	Length	Hash Function	Max Hop Count
Top Hash			
Sign Method	H	Reserved	Padd Length
Public Key			
Padding (optional)			
Signature			
Hash			

Figure 10: RREQ (Single) Signature Extension

Type	Length	Hash Function	Max Hop Count
Top Hash			
Sign Method	H	Reserved	Padd Length
Public Key			
Padding (optional)			
Signature			
Hash			

Figure 11: RREP **(Single) Signature Extension**

Type	Length	Hash Function	Max Hop Count
Reserved			Prefix Size
Top Hash			
Sign Method	H	Reserved	Padd Length
Public Key			
Padding (optional)			
Signature for RREP			
Signature			
Hash			

Figure 12: RREQ Double Signature Extension

Type	Length	Hash Function	Max Hop Count
Top Hash			
Sign Method	H	Reserved	Padd Length
Public Key			
Padding (optional)			
Signature			
Old Lifetime			
Old Originator IP address			
Sign Method 2	H	Reserved	Padd Length 2
Public Key 2			
Padding 2 (optional)			
Signature of the new Lifetime and Originator IP address			
Hash			

Figure 13: RREP Double Signature Extension