International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013
ISSN 2229-5518

The Secure Dynamic Source Routing Protocol in MANET to authenticate the node

Mr. Vivek R. Shelk
M-Tech, II Year
MIST, Bhopal,(M.P.)
Email Id: vvkshelke@gmail.com

Mr. Sumit Sharma
M-Tech II Year
MIST, Bhopal,(M.P.)
Email Id:sumit_sharma782022@yahoo.com

Prof. Rahul Deshmukh
Assistant Professor
MIST, Bhopal,(M.P.)
Email Id: rahul.deshmukh30@yahoo.com

Abstract— The *Dynamic Source Routing* protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two mechanisms of *Route Discovery* and *Route Maintenance*, which work together to allow nodes to discover and maintain *source routes* to arbitrary destinations in the ad hoc network. The use of source routing allows packet routing to be trivially loop-free, avoids the need for up-to-date routing information in the intermediate nodes through which packets are forwarded, and allows nodes forwarding or overhearing packets to cache the routing information in them for their own future use. All aspects of the protocol operate entirely *on-demand*, allowing the routing packet overhead of DSR to scale *automatically* to only that needed to react to changes in the routes currently in use.

Index Terms— Dynamic Source Routing, Adhoc Network, Routing protocol, MANET, MD5, WSN, Wormhole Attack.

---

1. INTRODUCTION

Mobile Ad hoc Networks (MANETs) are the special type of wireless network, where mobile nodes or terminals are connected through wireless interfaces forming a temporary network without any fixed infrastructure or a centralized administration. Mobile ad hoc networks are open to a wide range of attacks due to their unique characteristics like open medium, dynamically changing topology, absence of infrastructure, resource constraint (memory, bandwidth, computation power etc.) and trust among nodes. The principle behind mobile ad hoc networking is multi-hop relaying, which means messages sent by source to destination are forwarded by the other nodes if destination node is not directly reachable. In other words, an ad hoc node in MANET operates as not only end terminal but also as an intermediate router. Data packets sent by a source node may be reached to destination node via a number of intermediate nodes. Thus, multi-hop scenario occurs. In the absence of a security mechanism, it is easy for an attacker to insert, intercept or modify the messages. This means that unprotected MANETs are vulnerable to many attacks

[8] such as wormhole attack [9], black hole attack [10] including node impersonation, message injection, loss of confidentiality etc. On the other hand, nodes in MANETs are totally independent from any centralized device and they are free to move anywhere. This causes suddenly appearance and disappearance of the nodes and moving of nodes from one place to another place also increases the probability to compromise. Another issue in mobile ad hoc networks is that the nodes are resource constraint. Nodes are totally dependent on battery power and have limited memory and bandwidth. Therefore, security requirements such as authentication, integrity, availability, confidentiality, and non-reputation should be guaranteed during the communication between source and destination. In this paper, the focus is on securing on-demand routing protocol for MANETs, specifically the dynamic source routing (DSR) protocol. We proposed a protocol to secure the source routing in mobile ad hoc networks. The objective of proposed protocol is to authenticate the source and destination and

intermediate nodes in route list of route request (RREQ) message and detecting any kind of modification or fabrication in route lists from attacker's side and identifying a fake

RREQ by a malicious node. Proposed protocol for mobile ad hoc networks allows intermediate nodes to authenticate its predecessor node, and then forward the RREQ message. Finally destination node authenticates all the nodes that make up route.

1.2 Objective and Scope

When we are in position to send the data packets an Ad-Hoc network is established. But problem in such network is that it broadcast the data packet it is sent to all the nodes in the network. In such case there is possibility of misuse of data and data loss.

To prevent the data packets from such problem of misuse of data and data loss apply some encryption and decryption technique on DSR protocol for security.

It aims towards suggesting, designing and implementing a highly efficient security solution for mobile ad hoc networks by establishing secure routing.

The proposed protocol should be built upon such a platform that it is not only efficient in terms of meeting the security requirements like message integrity, data confidentiality and end to end authentication but is also cost effective and applicable in practical environment.

1.3 Features:

A mobile ad hoc network has following features:

Autonomous Terminal

In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. In other, since there is no background network words, besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.

Distributed Operation

For the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.

Multihop Routing

Basic types of ad hoc routing algorithms can be single hop and multihop, based on different link layer attributes and routing protocols. Single-hop MANET is simpler than multihop in terms of structure and implementation, with the cost of lesser functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes

Light-weight Terminal

In most cases, the MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

1.3 Characteristics

MANETs are new paradigm of networks, offering unrestricted mobility without any underlying infrastructure. Basically, ad hoc network is a collection of nodes communicating with each other by forming a multi-hop network. Following are the characteristics of a MANET [,]:

Dynamic Topologies

Nodes are free to move arbitrarily. The network topology may change randomly and have no restriction on their distance from other nodes. As a result of this random movement, the whole topology is changing in an unpredictable manner, which in turn gives rise to both directional as well as unidirectional links between the nodes.

Energy Constrained Operation

Almost all the nodes in an ad hoc network rely on batteries or other exhaustive means for their energy. The battery depletes due to extra work performed by the node in order to survive the network. Therefore, energy conservation is an important design optimization criterion.

Bandwidth Constraint

Wireless links have significantly lower capacity than infrastructures networks. Throughput of wireless communication is much less because of the effect of the multiple access, fading, noise, interference conditions. As a result of this, congestion becomes a bottleneck in bandwidth utilization.

Limited Physical Security

MANETs are generally more prone to physical security threats than wireless networks because the ad hoc network is a distributed system and all the security threats relevant to such a system are pretty much present, as a result, there is an increased possibility of

eavesdropping, spoofing, masquerading [3], and denial-of- service type attacks.

1.4 Applications

Because ad hoc networks are flexible networks that can be set up anywhere at any time, without any infrastructure, including pre-configuration or administration, people have come to realize the commercial potential and advantages that mobile ad hoc networking can bring.

This section describes some of the most prevalent applications for ad hoc wireless networks. The self-configuring nature and lack of infrastructure inherent to these networks make them highly appealing for many applications, even if it results in a significant performance penalty. The lack of infrastructure is highly desirable for low-cost commercial systems, since it precludes a large investment to get the network up and running, and deployment costs may then scale with network success. Lack of infrastructure is also highly desirable for military systems, where communication networks must be configured quickly as the need arises, often in remote areas. Other advantages of ad hoc wireless networks include ease of network reconfiguration and reduced maintenance costs. However, these advantages must be balanced against any performance penalty resulting from the multi-hop routing and distributed control inherent to these networks.

Data Networks

Ad-hoc wireless data networks primarily support data exchange between laptops, palmtops, personal digital assistants (PDAs), and other information devices. These data networks generally fall into three categories based on their coverage area: LANs, MANs, and WANs. Infrastructure-based wireless LANs are already quite prevalent, and deliver good performance at low cost. However, ad hoc wireless data networks have some advantages over these infrastructure-based networks. First, only one access point is needed to connect to the backbone wired infrastructure: this reduces cost and installation requirements. In addition, it can be inefficient for nodes to go through an access point or base station. Wireless MANs typically require multi-hop routing since they cover a large area. The challenge in these networks is to support high data rates, in a cost-effective manner, over multiple hops, where the link quality of each hop is different and changes with time. The lack of centralized network control and potential for high-mobility users further complicates this objective. Military programs such as DARPA's GLOMO (Global mobile information systems) have invested much time and money in building high-speed ad hoc wireless MANs that support multimedia, with limited success [2]. Wireless WANs are needed for applications where network infrastructure to cover a wide area is too costly or impractical to deploy. For example, sensor networks may be dropped into remote areas where network infrastructure cannot be developed. In addition, networks that must be built up and torn down quickly, e.g. for military applications or disaster relief, are infeasible without an ad hoc approach.

Home Networks

Home networks are envisioned to support communication between PCs, laptops, PDAs, cordless phones, smart appliances, security and monitoring systems, consumer electronics, and entertainment systems anywhere in and around the home. Such networks could enable smart rooms that sense people and movement and adjust light and heating accordingly, as well as "aware homes" that network sensors and computers for assisted living of seniors and those with disabilities. Home networks also encompass video or sensor monitoring systems with the intelligence to coordinate and interpret data and alert the home owner and the appropriate police or fire department of unusual patterns, intelligent appliances that coordinate with each other and with the Internet for remote control, software upgrades, and to schedule maintenance, and entertainment systems that allow access to a VCR, set-top box, or PC from any television or stereo system in the home [ ].

Device Networks

Device networks support short-range wireless connections between devices. Such networks are primarily intended to replace inconvenient cabled connections with wireless connections. Thus, the need for cables and the corresponding connectors between cell phones, modems, headsets, PDAs, computers, printers, projectors, network access points, and other such devices is eliminated. The main technology drivers for such networks are low-cost low-power radios with networking capabilities such as Bluetooth. The radios are integrated into commercial electronic devices to provide networking capabilities between devices. Some common uses include a wireless headset for cell phones, a wireless USB or RS232 connector, wireless cards, and wireless set-top boxes.

Sensor Networks

Wireless sensor networks consist of small nodes with sensing, computation, and wireless networking capabilities, as such these networks represent the convergence of three important technologies. Sensor networks have enormous potential for both consumer and military applications. Military missions require sensors and other intelligence gathering mechanisms that can be placed close to their intended targets. The potential threat to these mechanisms is therefore quite high, so it follows that the technology used must be highly redundant and requires as little human intervention as possible. An apparent solution to these constraints lies in large arrays of passive electromagnetic, optical, chemical, and biological sensors. These can be used to identify and track targets, and can also serve as a first line of detection for various types of attacks. Such networks can also support the movement of unmanned, robotic vehicles.

In the absence of a security mechanism, it is easy for an attacker to insert, intercept or modify the messages. This means that unprotected MANETs are vulnerable to many attacks [8] such as wormhole attack [9], black hole attack [10] including node impersonation, message injection, loss of confidentiality etc. On the other hand, nodes in MANETs are totally independent from any centralized device and they are free to move anywhere. This causes suddenly appearance and disappearance of the nodes and moving of nodes from one place to another place also increases the probability to compromise. Another issue in mobile ad hoc networks is that the nodes are resource constraint. Nodes are totally dependent on battery power and have limited memory and bandwidth. Therefore, security requirements such as authentication, integrity, availability, confidentiality, and non-reputation should be guaranteed during the communication between source and destination.

The focus is on securing on-demand routing protocol for MANETs, specifically the dynamic source routing (DSR) protocol. I proposed a protocol to secure the source routing in mobile ad hoc networks. The objective of proposed protocol is to authenticate the source and destination and intermediate nodes in route list of route request (RREQ) message and detecting any kind of modification or fabrication in route lists from attacker's side and identifying a fake RREQ by a malicious node. Proposed protocol for mobile ad hoc networks allows intermediate nodes to authenticate its predecessor node, and then forward the RREQ message. Finally destination node authenticates all the nodes that make up route. Fig 1.1 shows the simple MANET structure.

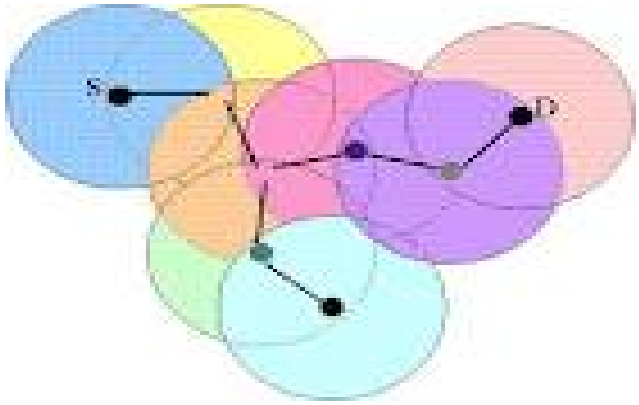


Fig 1.1 MANET structure

2. DYNAMIC SOURCE ROUTING

Dynamic Source Routing (DSR) is an on demand source routing protocol in MANETs. In DSR, when a source S wants to send message(s) to a destination D, S initiates the route discovery process. S generates a route request (RREQ) message and broadcasts it to it's the neighbors. A RREQmessage has unique request identifier and a record field. The purpose of the record field (initially empty) is to record the ids of the intermediate nodes from source to destination. When a node receives RREQ message, it first checks is it the intended destination or does it have a route to destination D in its cache. If so, it returns back a route reply (RREP) message to source. Otherwise it appends its identifier to the RREQ packet and rebroadcasts it. RREQ packet is rebroadcasted, until it reaches to destination D. When D receives RREQ packet, it generates a RREP message and sends back to S via the path obtained by reversing the order of nodes in route
list. Thus a path is establish between S and D. Whenever node cannot deliver apacket to the next node over the chosen route due to link break or any other reason, it unicasts a route error (RERR) message back to the source. Due to open medium and multi hop scenario, an attacker can easily capture the packet or inject the forge route control message in network. The success of DSR Protocol depends on the assumption that all the nodes are cooperative. An attacker can exploit this assumption and

may advertise malicious routing information such as it has less number of hops to the destination known as Black Hole attack [10]. Another attack malicious node can broadcast a forge route request (RREQ) packet to jam the network, if there is no authentication. An attacker can perform denial of service (DoS) attack by flooding several wastage packets into networks. Furthermore, attacker can inject, drop or modify the packets in between source and destination nodes. Many of the security solutions to secure the routing in MANETs have been proposed. Some research papers which, focus on secure routing in mobile ad hoc networks are discussed below: P. Papadimitratos and Z. Haas [3] proposed a securerouting protocol (SRP). SRP is based on a pre-share key between source and destination nodes. In SRP, a source node generates RREQ message and broadcasts it to its neighbors. When destination node receives RREQ message it verifies the source node and establish the route. Drawback of SRP is that it does not authenticate intermediate nodes. Author of [6] have shown the attack against the SRP protocol. In SRP protocol, an attacker can disrupts the normal functioning of this routing protocol in between source and destination nodes. Y.C. Hu, A. Perrig, and D. B. Johnson [4] proposed a secure routing protocol Ariadne. Ariadne protocol uses message authentication code (MAC) to maintain the message integrity and digital signature for authentication. In Ariadne protocol, the source node generates the route request (RREQ) message and appends a hash value to RREQ message. Each intermediate node appends its identifier, digital signature and per hops value. When destination node receives RREQ packet it verifies source node and intermediate nodes, then sends back RREP message. Drawback of Ariadne is that it vulnerable to an active 1-1 attack [4], where an attacker could delete the node's signature to forge a nonexistent route. L. Buttyan and I. Vajda [6] proposed a new protocol EndairA. They enhanced the security of Ariadne protocol proposed in [4] against active 1-1 attack [4] by providing security by appending the signature of source, destination and intermediate nodes. But EndairA protocol is vulnerable to active 0-1 attack [4] which is called Man in the Middle(MITM) attack. J. Liu, F. Fu, J. Xiao and Y. Lu [5] proposed EndairALoc protocol. The authors of [5] have shown that the. EndairA [6] protocol is vulnerable to Man in the Middle (MITM) attack. EndairALoc protocol uses the pair wise pre-shared symmetric keys to construct the message authentication code (MAC) rather than public keys, randomly generated request identifier and location information of nodes in RREQ message. EndairALoc protocol provides the security against MITM attack. This protocol is vulnerable to reply attack. An attacker can capture a valid RREQ message and can do modification in randomly generated request identifier, and then broadcast it, which may consume more resources of nodes unnecessarily. Instead of these secure routing protocols, many more solutions and approaches [2], [11], and [12] are proposed. These protocols are vulnerable either to active attack or passive attack. In this paper, we proposed a secure protocol that authenticates source, destination and intermediate nodes that make up the route from source to destination. MAC function provides the message integrity and confidentiality can be achieved by message encryption

2.1 PREVIOUS WORKS

Many of the security solutions to secure the routing in MANETs have been proposed. Some research papers which, focus on secure routing in mobile ad hoc networks are discussed below:

P. Papadimitratos and Z. Haas [3] proposed a secure routing protocol (SRP). SRP is based on a pre-share key between source and destination nodes. In SRP, a source node generates RREQ message and broadcasts it to its neighbors. When destination node receives RREQ message it verifies the source node and establish the route. Drawback of SRP is that it does not authenticate intermediate nodes. Author of [6] have shown the attack against the SRP protocol. In SRP protocol, an attacker can disrupts the normal functioning of this routing protocol in between source and destination nodes. Y.C. Hu, A. Perrig, and D. B. Johnson [4] proposed a secure routing protocol Ariadne. Ariadne protocol uses message authentication code (MAC) to maintain the message integrity and digital signature for authentication. In Ariadne protocol, the source node generates the route request (RREQ) message and appends a hash value to RREQ message.

Each intermediate node appends its identifier, digital signature and per hops value. When destination node receives RREQ packet it verifies source node and intermediate nodes, then sends back RREP message. Drawback of Ariadne is that it vulnerable to an active 1-1 attack [4], where an attacker could delete the node's signature to forge a nonexistent route. L. Buttyan and I. Vajda [6] proposed a new protocol EndairA. They enhanced the security of Ariadne protocol proposed in

[4] against active 1-1 attack [4] by providing security by appending the signature of source, destination and intermediate nodes. But EndairA protocol is vulnerable to active 0-1 attack [4] which is called Man in the Middle (MITM) attack. J. Liu, F. Fu, J. Xiao and Y. Lu [5] proposed EndairALoc protocol. The authors of [5] have shown that the. EndairA [6] protocol is vulnerable to Man in the Middle (MITM) attack. EndairALoc protocol uses the pair wise pre-shared symmetric keys to construct the message authentication code (MAC) rather than public keys, randomly generated request identifier.

3.PROPOSED SECURE ROUTING PROTOCOL

In our protocol, when a node wants to communicates, it initiates route discovery process by generating a RREQ message. Source appends its digital signature (DS) to the message. Neighbors of source first verify the signature of source and make the decision accordingly. We added a one way hash function to the RREQ message to maintain the integrity of message. Therefore, deletion of a node from or any kind of modification in route list of RREQ message can be detected. Destination sequence number [12]in the protocol is added to make the loop free routing and to check the freshness
of route control packet. Assume that S is the source node trying to discover a route to destination D and route from S to D exist via intermediate node M and N.

A. Assumptions are

1) The nodes which are within range of each other are neighbors.
2) All the nodes in network have their own public and private key pair generated by any key management system for mobile ad hoc networks.
3) Public key of nodes are known to others nodes in network.

B. Notations are

1) LI Life time (maximum number of hop) of a packet 'I'.
2) Seq Destination sequence number.
3) DSA Digital signature of node A.
4) hA Hash value appended by node A to the message.
5) A *, node A broadcast a message.
6) B, node A sends a message to node B.

C. Operation of proposed protocol and format of RREQ and RREP messages

1.) S-> * RREQ <Seq, S, D, LREQ, < >, DSs, hS>
2.) M-> * RREQ <Seq, S, D, LREQ-1, <M>, DSs, DSM, hM>
3.) N-> * RREQ <Seq, S, D, LREQ-2, <M, N>, DSs, DSM, DSN, hN>
4.) D-> N: RREP <Seq, S, D, <M, N>, DSs, DSM, DSN, DSD, hD>
5.) N-> M: RREP <Seq, S, D, <M, N>, DSs, DSM, DSN, DSD, hD>
6.) M-> S : RREP <Seq, S, D, <M,N>, DSs, DSM, DSN, DSD, hD>

D. Description

The operations of protocol are shown above. A source S initiates route discovery by generating route request (RREQ) message. RREQ contains the address of source and
destination, Seq, LREQ, route list of intermediate node which makes the route from source to destination (initially empty), digital signature of source DSS, and a hash value hS. Life time of a packet refers to maximum number of hop which a packet can travel. On each broadcast, life time would be reduced by one automatically. If life time is reached to zero, packet would be discarded. Source produced the hS using one way hash
function.

hS = H(S, D, Seq, LREQ) ……...(1)

When a neighbor of S, M receives the RREQ message, it verifies the signature of source node. If source node is genuine node, M checks Seq and compare with Seq stored in its cache. If Seq is less M discards the packet. Otherwise, it appends its identifier to route list and digital signature DSM to the message and replaces the hS by hM and then rebroadcasts

hM = H(hS, M, LREQ-1)……(2)

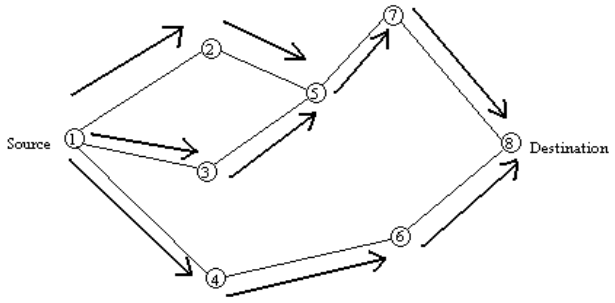
Similarly, node N verifies signature of source and node M and checks Seq, and then appends its identifier to route list and digital signature DSN to the message, replaces the hM by hN and finally rebroadcasts.

hN = H(hM, N, LREQ-2)...…….……(3)

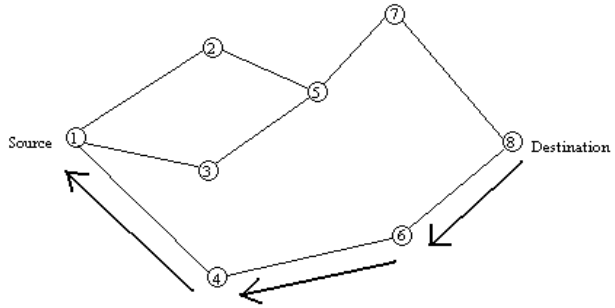
Finally, when destination node D receives the RREQ message, it verifies all the signatures contained in RREQ packet, compares Seq with previously stored Seq in its cache. If source and all the nodes in route list are genuine and packet is not outdated, the destination node, it computes:

hD = H(N, LREQ-2, H(M, LREQ-1, H(S, D, Seq, LREQ)))…(4)

and compares the value of hD with hN. If both values are same, the message integrity is verified. Otherwise message is discarded. If all the verifications are successful, the destination D creates a route reply (RREP) message and sends back to the source S via the path obtained by reversing the route list in RREQ packet. Route Reply (RREP) message contains Seq, addresses of source and destination, route list, hD, and signature of all the nodes from source to destination. Each intermediate node verifies the signature of destination D and Seq to check the freshness of message. On receiving RREP message at source, S verifies signature of all the nodes in route
list and Seq. Source S computes:
h = H (N, LREQ-2, H (M, LREQ-1, H (S, D, Seq, LREQ)))….. (5)
and compares with hD to check the integrity of route list. If both values are same, S accepts RREP. Otherwise discards. S calculates the values of LREQ-1 and LREQ-2 on the basis of route list. After successful completion of all verifications, a route from S to D is established.



(a) Propogation of Route Request (RREQ) Packet



(b) Path taken by the Route Reply (RREP) Packet

Fig. 3.1 Path selection of DSR protocol

3.1 ADVANTAGES AND DISADVANTAGES

This protocol uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach. In a reactive (on-demand) approach such as this, a route is established only when it is required and hence the need to find routes to all other nodes in the network as required by the table-driven approach is eliminated. The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead. The disadvantage of this protocol is that the route maintenance mechanism does not locally repair a broken link. Stale route cache information could also result in inconsistencies during the route reconstruction phase. The connection setup delay is higher than in table-driven protocols. Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility. Also, considerable routing overhead is involved due to the source-routing mechanism employed in DSR. This routing overhead is directly proportional to the path length.

4. CONCLUSION

The Dynamic Source Routing protocol (DSR) provides excellent performance for routing in multi-hop wireless ad hoc networks. In this paper, I have proposed a protocol to secure on demand source routing in MANETs that fulfills the security requirements. Our protocol uses one way hash function to maintain the integrity of message. Therefore, deletion of a node from or any kind of modification in route control packet can be detected. Using Public Key Cryptography (PKC), nodes can negotiate the session key for secure communication that fulfills the requirement of confidentiality. Source, destination and intermediate nodes in route list authenticate others nodes by verifying signature. Security analysis results show that protocol provides the security against many attacks such as reply attack, rushing attack, IP spoofing and man in the middle attack. Our protocol is based on Public Key Cryptography. Asymmetrical algorithms require more calculation than the symmetrical algorithms. Therefore, it consumes much battery power than protocols based on symmetric algorithms.

DSR has very low routing overhead and is able to correctly deliver almost all originated data packets, even with continuous, rapid motion of all nodes in the network. DSR operates *entirely* on demand [12], with *no* periodic activity of *any kind* required at *any level* within the network. This entirely on-demand behavior and lack of periodic activity allows the number of routing overhead packets caused by DSR to scale all the way down to *zero*, when all nodes are approximately stationary with respect to each other and all routes needed for current communication have already been discovered. As nodes begin to move more or as communication patterns change, the routing packet overhead of DSR *automatically* scales to only that needed to track the routes currently in use.

5. REFERENCES

[1] W. Huang, Y. Xiong, and D. Chen, "DAAODV: A Secure Ad hoc Routing Protocol based on Direct Anonymous Attestation", Proceeding of International Conference on Computational Science and Engineering,August, vol-2, pp: 809-816, 2009.

[2] D. Cerri and A. Ghioni, "Securing AODV: The A-SAODV Securing Routing Prototype", IEEE Communication Magazine: Security in Mobile Ad hoc and Sensor Networks, vol-46, pp: 120-125, February, 2008.

[3] P. Papadimitratos, and Z. Haas, "Secure Routing for Mobile Ad hoc Networks", Proceeding of SCS Communication Networks and Distributed Systems Modeling and Simulation, January, 2002.

[4] Y.C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-demand Routing Protocol for Ad hoc Networks", Proceeding of 8th Annual International Conference on Mobile Computing and Networking, (MobiCom 02), September 2002, pp: 12-23,.

[5] J. Liu, F. Fu, J. Xiao and Y. Lu, "Secure Routing for Mobile Ad Hoc Networks", Proceeding of 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, vol-3, 2007, pp: 314-318.

[6] L. Buttyan, and I. Vajda, "Towards Provable Security for Ad hoc Routing Protocols", Proceeding of 2nd ACM Workshop on Security of Ad hoc and Sensor Networks, October 2005, pp: 94-105.

[7] G. Ács, L. Buttyán, and I. Vajda, "Provably Secure On-demand Source Routing in Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, vol-5, November 2006, pp: 1533-1546.

[8] N. Kettaf, H. Abouaissa, P. Lorenz, "An Efficient Heterogeneous Key Management approach For Secure Multicast Communication in Ad hoc networks", Springer, Telecommunication System, vol-37, February 2008, pp: 29-36.

[9] Y.Chun Hu, A. Perrig and David B. Johnson, "Wormhole Attack in Wireless Networks", IEEE Journal on Selected Areas in Communication, vol. 24, February 2006, pp: 370-380.

[10] R.A. Raja Mahmood, A.I. Khan, "A Survey on Detecting Black Hole Attack in AODV-Based Mobile Ad hoc Networks", International Symposium on High Capacity Optical Networks and Enabling Technologies, November 2007, pp: 1-6.

[11] A. K. Shukla, N. Tyagi, "A New Route Maintenance in Dynamic Source Routing Protocol", IEEE International Symposium on Wireless Pervasive Computing, January, 2006.

[12] Q. Niu, "Secure On-Demand Source Routing for Ad hoc Networks", Proceeding of IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 08), October, 2008, pp: 1-4.