*IRACST – Engineering Science and Technology: An International Journal (ESTIJ), ISSN: 2250-3498, Vol.2, No. 5, October 2012*

# A Novel Approach for Secure Routing in MANETs

C. Sreedhar
Associate Professor, CSE Dept.,
G. Pulla Reddy Engineering College,
Kurnool.

Dr. S. Madhusudana Verma
Professor, OR & SQC Dept.,
Rayalaseema University,
Kurnool.

Dr. N. Kasiviswanath
Professor & HOD, CSE Dept.,
G. Pulla Reddy Engineering College,
Kurnool.

***Abstract*—Mobile Ad-hoc Network (MANET) is a collection of mobile nodes that can communicate with each other using multi-hop wireless links without requiring any fixed infrastructure and centralized management. In this paper, we propose a novel security mechanism for Ad-hoc On-Demand Distance Vector (AODV) routing protocol. The widely accepted AODV routing protocol designed to accommodate the needs of such self-organized networks do not address possible threats aiming at the disruption of the protocol itself. The assumption of a trusted environment is not one that can be realistically expected. Hence, several efforts have been made towards the design of a secure and robust routing protocol for ad-hoc networks. Blackhole attacks pose a severe threat for normal communication in MANETs. In blackhole attacks, a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. In this paper, secure communication among nodes in MANETs is provided by calculating the Threat value parameter (Tvp) at the network layer. We have compared our proposed solution with AODV and Secure AODV (SAODV) in normal situation as well as in the presence of malicious nodes. The simulation results demonstrate the performance impact of security implementations into the original AODV after the implementations of SAODV and our proposed solution.**

***Keywords-component; MANETs, secure routing, blackhole attacks, AODV.***

## I. INTRODUCTION

Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self configuration ability, they can be deployed urgently without the need of any infrastructure. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols. Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed for MANETS, i.e. AODV, OLSR, DSR etc [1].

Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats.

MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS) [2], selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from. A MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

## II. ROUTING SECURITY IN MANETS

Security always implies the identification of potential attacks, threats and vulnerabilities of a certain system. Janne Lundberg [3] discussed special types of attacks that can simply be performed against a MANET. Attacks can be classified into *passive* and *active attacks*. A passive attack does not interrupt the operation of a routing protocol, but only attempts to find out valuable information by listening to routing traffic, which makes it very difficult to detect. An active attack is an attempt to modify data, gain authentication, or acquire authorization by inserting fake packets into the data stream or modifying packets transition in the network. Active attack can be divided into external attacks and internal attacks. In *external attack* nodes do not belong to the network. An *internal attack* is one from compromised or hijacked nodes that belong into the network.

Based on this threat analysis and the recognized capabilities of the potential attackers, we will now discuss several specific attacks that can target the function of a routing protocol in an ad hoc network.

**Black Hole:** A black hole [4] is a type of denial of service attack where the intension of the malicious node could be to hinder the path finding process or to intercept all data packets being sent to the destination node.

**Location Disclosure:** Location disclosure [5] is an attack that targets the confidentiality requirements of an ad hoc network. Through the utilize of traffic analysis techniques, or with simpler probing and monitoring approaches, an attacker is able to find out the location of a node, or even the structure of the whole network.

**Replay:** An attacker in replay attack [6] an attacker injects into the network routing traffic that has been captured previously. This attack generally targets the newness of routes, but can also be used to undermine badly designed security solutions.

**Energy consummation**: Energy is a critical parameter in the MANET. Battery-powered devices try to conserve energy by transmit only when absolutely necessary. An attacker can attempt to consume batteries by requesting routes or forwarding unnecessary packets to a node [6].

**Blackmail:** This attack is relevant against routing protocols that use mechanisms for the recognition of malicious nodes and transmit messages that attempt to blacklist the offender. An attacker may fabricate such reporting messages and try to isolate legal nodes from the network [7].

## III. AD-HOC ON-DEMAND DISTANCE VECTOR ROUTING (AODV)

AODV is described in RFC 3561 [8]. It's reactive protocol, when a node wishes to start transmission with another node in the network to which it has no route; AODV will provide topology information for the node. AODV use control messages to find a route to the destination node in the network.

### *A. Route Discovery in AODV*

When a node "A" wants to initiate transmission with another node "G" as shown in the Fig. 1., it will generate a Route Request message (RREQ). This message is propagated through a limited flooding to other nodes. This control message is forwarded to the neighbors, and those node forward the control message to their neighbors' nodes. This process of finding destination node goes on until it finds a node that has a fresh enough route to the destination or destination node is located itself. Once the destination node is located or an intermediate node with enough fresh routes is located, they generate control message route reply message (RREP) to the source node.

When RREP reaches the source node, a route is established between the source node "A" and destination node "G". Once the route is established between "A" and "G", node "A" and "G" can communicate with each other. Fig. 1. depicts the exchange of control messages between source node and destination node.

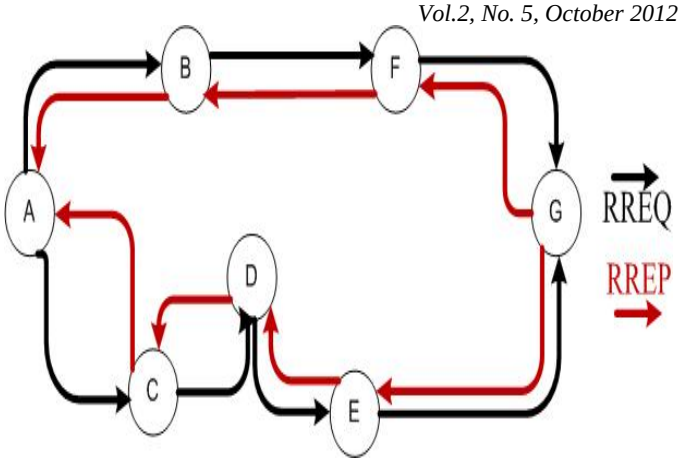


Figure 1. AODV Route Discovery

When there is a link down or a link between destinations is broken that causes one or more than one links unreachable from the source node or neighbors nodes, the RERR message is sent to the source node. When RREQ message is broadcasted for locating the destination node i.e. from the node "A" to the neighbors nodes, at node "E" the link is broken between "E" and "G", so a route error RERR message is generated at node "E" and transmitted to the source node informing the source node a route error, where "A" is source node and "G" is the destination node. The scheme is shown in the Fig.2 below.

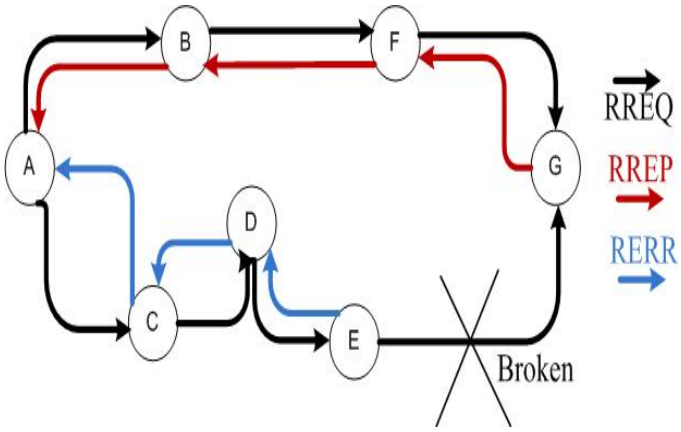


Figure 2. Route Error message in AODV

### *B. Route Discovery Process*

When a source node wants to start data transmission with another node in the network, it checks its routing cache. When there is no route available to the destination in its cache or a route is expired, it broadcast RREQ. When the destination is located or any intermediate node that has fresh enough route to the destination node, RREP is generated [9]. When the source node receives the RREP it updates its caches and the traffic is routed through the route.

### *C. Route Maintenance Process*

When the transmission of data started, it is the responsibility of the node that is transmitting data to confirm the next hop received the data along with source route. The

node generates a route error message, if it does not receive any confirmation to the originator node. The originator node again performs new route discovery process.

## IV. BLACKHOLE ATTACK

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept [10] [11] [12].This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [13]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address [14].

The method how malicious node fits in the data routes varies. Fig. 3 shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost.

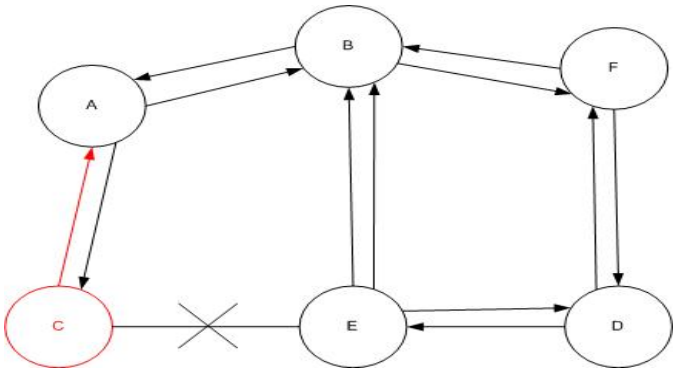


Figure 3. BlackHole attack

There are two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack.

### A. *Internal Blackhole attack*

This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.

### B. *External Blackhole attack*

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET. External black hole attack can be summarized in following points:

1. Malicious node detects the active route and notes the destination address.
2. Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
3. Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
4. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.
5. The new information received in the route reply will allow the source node to update its routing table.
6. New route selected by source node for selecting data.

The malicious node will drop now all the data to which it belong in the route.

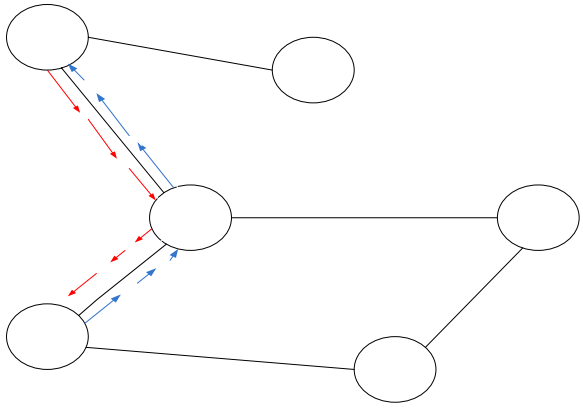

Figure 4. BlackHole attack(Scenario 2)

In AODV black hole attack the malicious node "A" first detect the active route in between the sender "E" and destination node "D" as shown in Fig. 4. The malicious node "A" then send the RREP which contains the spoofed destination address including small hop count and large sequence number than normal to node "C". This node "C" forwards this RREP to the sender node "E". Now this route is

used by the sender to send the data and in this way data will arrive at the malicious node. These data will then be dropped. In this way sender and destination node will be in no position any more to communicate in state of black hole attack.

## V. PROPOSED SOLUTION

The Threat value Parameter (Tvp) is based on the parameters shown in Table 1. The table calculates the overall Tvp, which is required in proposed routing protocol for secure communication among nodes in MANETs and at the network layer, Tvp is calculated. The path is selected in such a way that the node with less Tvp values. The parameter Nsr denotes the number of nodes successfully received RREQ packets from the source node, Nsn denotes the number of nodes not received RREQ packets, Nsp denotes the number of nodes successfully received RREP packets, Nnp denotes the number of nodes not received the RREP packets, Nsd denotes the number of data transmitted successfully from the source node, Nnd denotes the number of nodes not received data. The Query request rate is denoted by the Rr, query reply rate is denoted by the Pr and Dr denotes the data transmission rate.

The Threat value parameter (Tvp) is given by the equation:

$$Tvp=Tq*Rr + Tp*Pr+Td*Dr \quad (1)$$

Where Tvp is the Threat Value parameter and Tq, Tp, Td are time factorial at which route request, route reply and data are sent by the node respectively. Tvp is calculated for each node during routing and is checked against the threshold value. If higher than the threshold value, then there is a possibility for this node to be marked as node with prone to attacks for the current transmission and will not be suitable for further routing and an alternate path is selected for routing.

TABLE I. THREAT VALUE PARAMETER CALCULATION

| S.No | Query Request | Nsr | Query Request rate |
|---|---|---|---|
| 1. | | | Rr |
| | | Nsn | |
| 2. | Query Request | Nsp | Query Reply rate |
| | | | Pr |
| | | Nnp | |
| 3. | Data | Nsd | Data transmission rate |
| | | | Dr |
| | | Nnd | |

### A. Route Discovery

Our proposed solution uses the on-demand principle of route discovery as the routes are discovered only when they are needed. The destination node selects the optimal route after receiving RREQ packets. The source node broadcasts RREQ packet to search available paths to the destination. The fields in RREQ packets are updated at each intermediate node. Route Tvp parameter is incremented to find the total threat value of the route. The destination node unicasts RREP after evaluating the best secure path as given in Fig. 5.

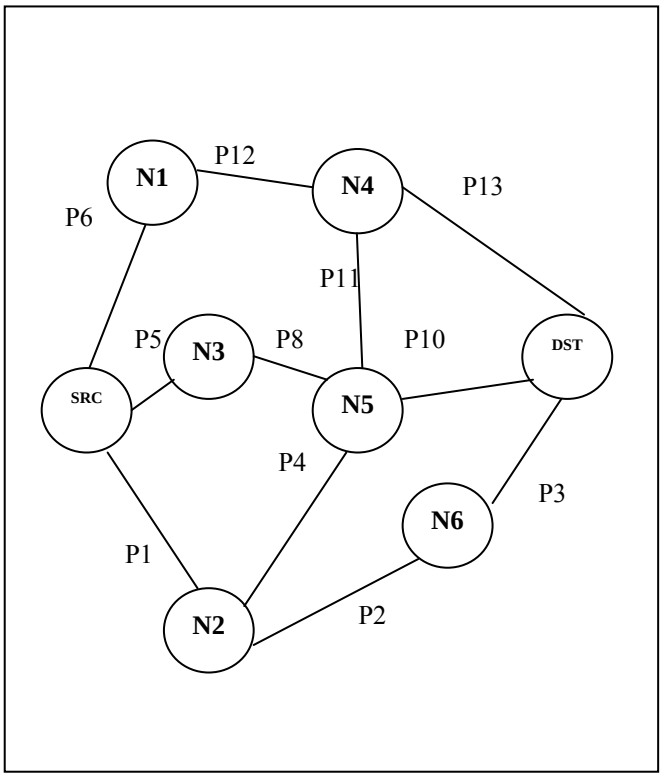


Figure 5. Route Discovery in our proposed solution

In Fig. 5, the available routes from the source (SRC) to destination (DST) are as follows:

Route 1 (R1) : P1→P2→P3

Route 2 (R2) : P1→P4→P9→P3

Route 3 (R3) : P1→P4→P10

Route 4 (R4) : P5→P8→P10

Route 5 (R5) : P6→P7→P10

Route 6 (R6) : P6→P7→P11→P13

Route 7 (R7) : P6→P12→P13

The destination node receives seven RREQ packets, in which the values of lowest Tvp are presented as:

RREQ of R1 : [0.128]

RREQ of R2 : [0.432]

RREQ of R3 : [0.563]

RREQ of R4 : [0.312]

RREQ of R5 : [0.715]

RREQ of R6 : [0.234]

RREQ of R7 : [0.345]

The destination node selects the most secure and best route P3→P2→P1 and unicasts RREP packet to the source node (SRC). In our proposed routing protocol, the route maintenance is done at destination node. Once the route is selected, the destination node starts a timer to make sure the availability of selected route. If the destination does not receive packets from the source, and the timer expires, it is assumed that the route is broken, and the destination node selects another best secure route and again unicasts RREP to the source node.

## VI. SIMULATION ANALYSIS

We conducted extensive simulations to analyze the performance of the proposed solution in both normal and malicious conditions and compare it with SAODV (Secure ad-hoc on demand distance vector) and AODV routing protocols using NS-2.

The nodes used in the simulations were based on IEEE 802.11 with different data rates such as 1, 2, 5.5 and 11 mbps. The application traffic consists of constant bit rate (CBR) with a radio range of 100 m. The source and destination nodes were randomly selected. The packet size used is 512 bytes. The random waypoint mobility model is used. The different parameters used are presented in Table 2.

TABLE II. SIMULATION PARAMETERS

| | |
|---|---|
| Number of nodes | Random initial topology |
| Total simulation time | 600 s |
| Packet Size | 512 bytes |
| MAC protocol | IEEE 802.11b |
| Wireless node Data rate | Variable 1,2,5,5, 11 mbps |
| Radio transmission range(m) | 100 |
| Mobility model | Random waypoint |
| Maximum route request timeout | 30 s |
| Protocols | Proposed solution, SAODV, AODV |

Fig. 6 shows the packet delivery ration against maximum speed for proposed solution, AODV and SAODV. AODV has low packet delivery ratio as compared to proposed solution and SAODV, as both proposed solution and SAODV has multiple routes from the source to the destination and if any route is broken due to mobility, they can still operate. The packet delivery percentage is more than 85% in proposed solution for all the node speeds. This shows effectiveness of proposed solution in discovering and maintaining routes in high mobility for delivering data packets.

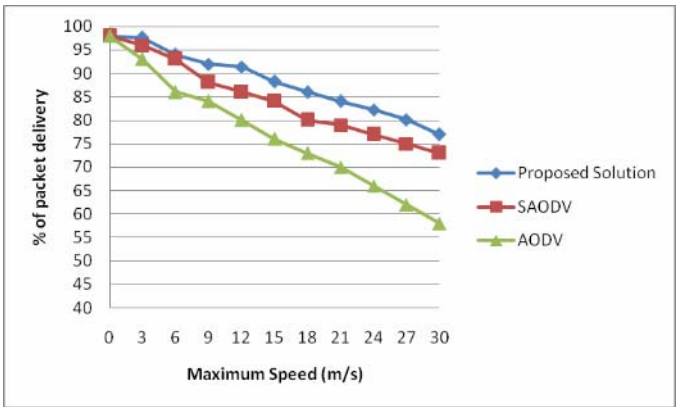


Figure 6. Packet delivery ratio in mobility

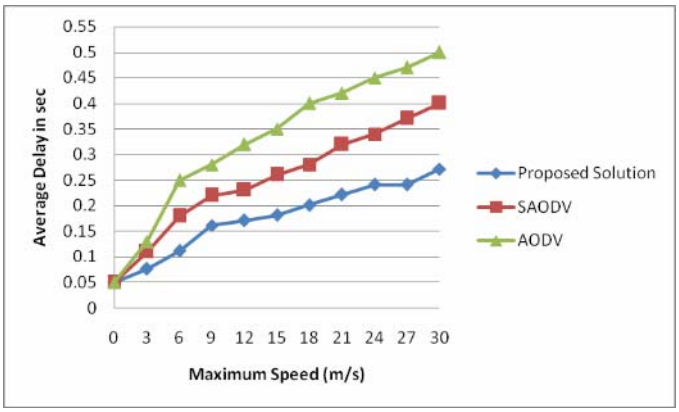


Figure 7. End-to-End delay

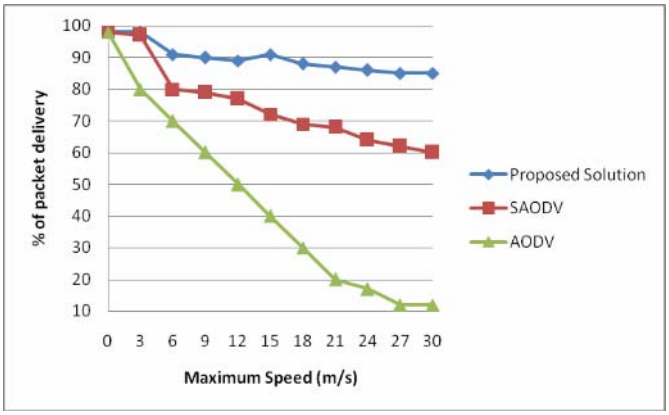


Figure 8. Packet delivery ratio in the presence of malicious nodes

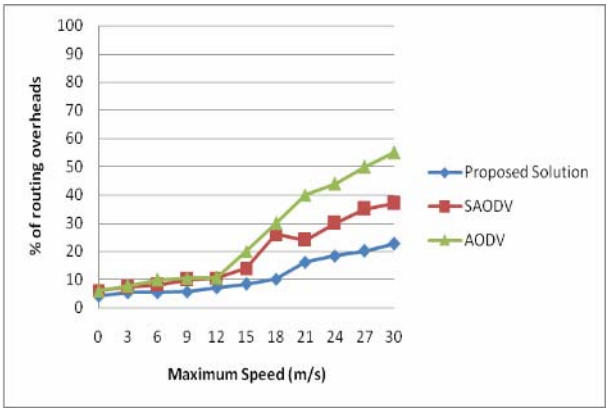


Figure 9. End-to-end delay in the presence of malicious nodes

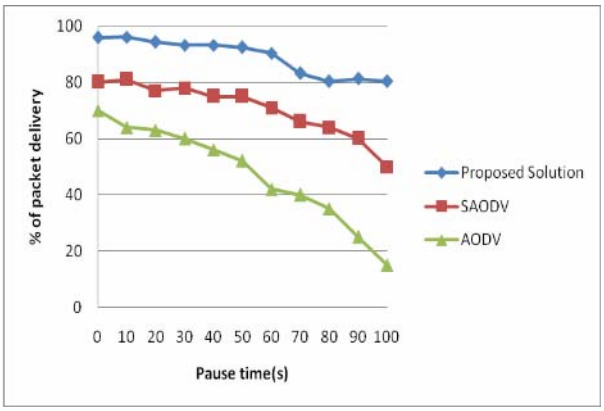


Figure 10. Packet delivery ratio with varying pause time.

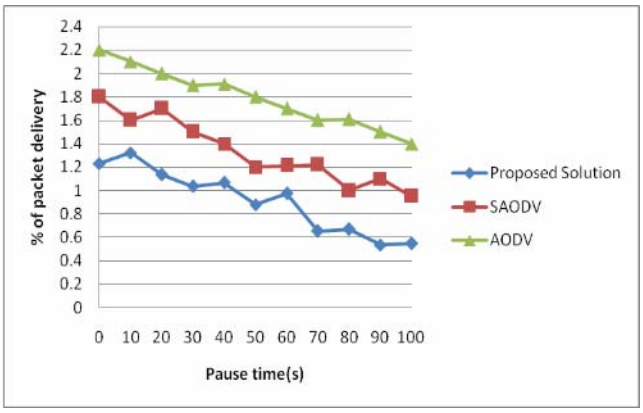


Figure 11. Average end-to-end delay with varying pause time

The average end-to-end delay for a network of 60 nodes is shown in Fig. 7. Smallest end-to-end delay is observed in case of proposed solution. The end-to-end delay is increased quickly with increasing node mobility in AODV due to lack of alternate path. When an active route is broken, AODV initiates route discovery procedure again. SAODV has slight more end-to-end delay as compared to proposed solution due to involvement of cryptographic operations in route discovery.

The packet delivery ratio in the presence of malicious node is shown in Fig.8. The source node sends packets to the destination, in which the malicious node is located near the source node. In AODV, the packet delivery is reduced to 15%, while in SAODV; the packet delivery ratio is dropped to 60%. Here the packet delivery ratio of proposed solution is above 85% in the presence of malicious node near the source.

Fig.9. In AODV, the end-to-end delay is gradually increasing. However, the end-to-end delay remains the same in vase of SAODV and proposed solution as in Fig.7

The end-to-end delay in the presence of malicious node near the source node is shown in following control packets are used: routing request message (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is unicasted back to the source of RREQ, and route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used for detecting and monitoring links to neighbours.

## VII. CONCLUSION

In this paper, various aspects of the proposed protocol are presented in detail such as the route discovery process, route maintenance and route security mechanism used within the route discovery. Comparison of proposed protocol with two different well known routing protocols such as AODV and SAODV is done using ns-2. The comparison covers most of the scenarios such as the packet delivery ratio, average delay and routing overheads with and without malicious nodes.

The performance of the protocol is analyzed according to varying pause time and velocities. Proposed solution is very effective against blackhole attacks. Our future work intends to be in the direction of analyzing the protocol in very large networks with very high mobility in nodes and adapting this protocol for various other security attacks and nodes which are susceptible to packet modification attacks.

## REFERENCES

[1] C.E.Perkins and E.M.Royer, "Ad-Hoc on Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp.90-100, Feb, 1999

[2] C.M barushimana, A.Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad-Hoc Networks", Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.

[3] J. Lundberg, ―Routing Security in Ad Hoc Networks,‖ Helsinki University of Technology, http://citeseer.nj.nec.com/400961.html.

[4] Songbai Lu, Longxuan Li, Kwon-Yan Lam and Lingvan Jia ―SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack,‖ International Conference on Computational Intelligence and Security, pp 421-425 (2009)..

[5] J.-F. Raymond, ―Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems,‖ *Proc. Wksp. Design Issues in Anonymity and Unobservability*, Berkeley, CA, July 2000, pp. 7–26..

[6] J.-F. Raymond, ―Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems,‖ *Proc. Wksp. Design Issues in Anonymity and Unobservability*, Berkeley, CA, July 2000, pp. 7–26..

[7] . L. Zhou and Z. J. Haas, ―Securing Ad hoc Networks,‖ *IEEE Net. Mag.*, vol. 6, no. 13, Nov./Dec. 1999, pp. 24–30.

[8] C.Parkins, E.B.Royer, S.Das, A hoc On-Demand Distance Vector (AODV) Routing. July 2003, [Online]. Available: http://www.faqs.org/rfcs/rfc3561.html. [Accessed: April. 10, 2010] .

[9] V.Mahajan, M.Natue and A.Sethi,"Analysis of Wormhole Intrusion attacks in MANETs", IEEE Military Communications Conference, pp. 1-7, Nov, 2008.

[10] C.Jiwen, Y.Ping, C.Jialin, W.Zhiyang, L.Ning, " An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network",24th IEEE International Conference on Advance Information Networking and Application (AINA 2010), pp. 775-780, April,2010.

[11] Y.F.Alem, Z.C.Xuan, " Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection",2nd International Conference on Future Computer and Communication (ICFCC 2010), Vol. 3, pp. 672-676, May,2010.

[12] S.Sharma, Rajshree, R.P.Pandey, V.Shukla, "Bluff-Probe Based Black Hole Node Detection and Prevention", IEEE International Advance Computing Conference (IACC 2009), pp. 458-462, March, 2009.

[13] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007.

AUTHORS PROFILE

**C. Sreedhar** received B.E (Computer Science & Engineering) and M.E (Computer Science & Engineering) degree. Presently pursuing Doctorate Degree (Ph.D) in Computer Science from Rayalaseema University, Kurnool and working as Associate Professor in Computer Science & Engineering Department in G. Pulla Reddy Engineering College, Kurnool. His research interest includes Wireless networks, Security, Routing Protocols. He has published 7 National/International Journals/Conferences.

**Dr. N. Kasiviswanath** received his B.E. degree in Computer Science & Engineering from Marthwada University, M.S. degree in Computer Science & Engineering from BITS, Pilani and the Ph.D. degree from Rayalaseema University, Kurnool. He has 24 years of teaching experience. He has published 30 research papers in National/International journals/conferences. At present, he is working as Professor and Head of Computer Science & Engineering Department, GPREC, Kurnool.

**Dr. S. Madhusudana Verma** has received M.Sc., in 1986, M.Phil in 1988 and Ph.D in 1994 in the subject of Operations Research and SQC from SVU, Tirupathi. He is a Professor and Controller of the Examination at Rayalaseema University, Kurnool. His research interests are reliability engineering, Queuing theory, statistical Quality Control and Computer Science etc., He has attended 13 National/International Conferences and published 28 research articles in National/International journals and guided for Doctoral and M.Phil degrees.