ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Comparison of Reactive Routing Protocol under Black hole attack for MANET

Shridevi.K, Sudha.S

Assistant Professor, Dept. of Computer Science and Engineering, Secab Institute of Engineering & Technology, Vijayapur, Karnataka, India

Student, Dept. of Computer Science and Engineering, Secab Institute of Engineering & Technology, Vijayapur, Karnataka, India

ABSTRACT: Mobile adhoc network is a set of wireless mobile nodes in which nodes will forward the packets to neighbour nodes and communicate directly by wireless transmission. In this paper, reviews of various routing protocols are discussed. due to the various attacks on the nodes lead to increase in delay and control overhead, Hence to overcome these issue a novel approach(timer based) method is proposed using modified AODV and modified DSR protocol to detect black hole attack. The performance of this novel approach is measured using the matrices such as throughput, delay and packet delivery ratio. Simulation results are carried out using NS-2 Simulator for 50 numbers of nodes.

KEYWORDS: Mobile adhoc Network (MANET), AODV, Dynamic Source Routing (DSR), throughput, delay, packet delivery ratio.

I. Introduction

The type of network as Infrastructure less network is known as Mobile Ad Network (MANET). All nodes are capable of movement and can be connected dynamically in arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the terminals themselves. The entire network is mobile, and the individual terminals are allowed to move with other nodes. In this type of network, some pairs of terminals may not be able to communicate directly to with neighbour nodes and relaying of some messages is required so that they are delivered to their destination. The nodes of these network function as routers, which discover and maintain routes to other nodes in the networks. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices. In any but the most trivial networks (point-to-point links), some mechanism is required for routing the packets from the source to the final destinations. This includes discovery and maintenance of routes along with associated costs.

In an infrastructure less wireless network, the job of routing is assigned to dedicated nodes called access points (AP). A wireless access point normally connects directly to a wired Ethernet connection and then provides wireless connections using radio frequency links for other devices to utilize that wired connection. Configurations of the APs are much less dynamic than end-point nodes. APs are like base stations which keep track of nodes associations/disassociations, authentication etc. and control the traffic flow between their clients as well as between fellow APs. The AP may also be connected to the Internet thereby providing Internet connectivity to its clients.

The Characteristics of MANET are as follows.

Dynamic Topologies: Since nodes are free to move arbitrarily, the network topology may change randomly and rapidly at unpredictable times. The links may be unidirectional or bidirectional.

Bandwidth constrained, variable capacity links: Wireless links have significantly lower capacity than their hardwired counterparts. Also, due to multiple access, fading, noise, and interference conditions etc. the wireless links have low throughput.

Energy constrained operation: Some or all of the nodes in a MANET may rely on batteries. In this scenario, the most important system design criteria for optimization may be energy conservation.

Limited physical security: Mobile wireless networks are generally more prone to physical security threats than are fixed- cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANET provides additional robustness against the single points of failure of more centralized approaches.

Security is essential for wired/wireless network communications. MANET's success depends on its security. The various types of attack in mobile adhoc networks are as follows:

Black hole attack: This is a kind of attack in which a malicious node broadcasts itself to have a legitimate route to the destination node even if the route is unauthentic. Drops the packets by sending false route reply messages to the route request instead of forwarding. A black hole node exploits a routing protocol. In black hole attack, the attacker node may or may not be authorized in the network due to which performance of the network degrades.

Gray hole attack: It is difficult to detect the gray hole attack. Because the nodes can drop the packets partially and behaves as normal honest node. Here the first being first who drop the packets coming from the certain specific node in the network while forwarding all the packets for other nodes.

Worm hole attack: In this attack attacker recives the packets from one location of network and tunnels from other location of the network where the packets will be present in the network. Tunneling between two colliding attackers is referred as wormhole attack.

Man in Middle attack: In this attacker generally makes independent connection with the victims and then relays messages between them, making them believe that they are talking directly to each other over a private connection, when the fact is that the entire conversation is controlled by the attacker. An attacker usually sites between the sender and receiver and sniffs the information being sent between two nodes.

The paper is organized as follows. Section 2 provides an overview of AODV protocol and DSR protocol, section 3 deals with several methodologies for performance measurements in MANET, section 5 presents a Simulation results and finally conclusion of the paper in Section 6.

II. ROUTING PROTOCOLS

An ad-hoc routing protocol is the one which controls the nodes, as nodes will decide which way to route the packets between computing devices in a network. The various kinds of protocols are proposed to deal with routing problem in the MANET. These routing protocols can be classified into two classes as Reactive and Proactive. Reactive protocols are characterized by node acquire and maintain routes on demand. AODV and DSR are two reactive routing protocols. Proactive protocols are characterized by all nodes maintain routes to the destination in the network at all times.

A. Overview Of Aodv Protocol

Route establishment: In the figure shown bellow source node sends packets to destination node. In route establishment AODV builds routes by using RREQ and RREP messages. When source node wants to reach to destination it sends packets as RREQ across the network. The nodes receiving packet will update the information for source node and sends a reply message to source node. When all intermediate nodes have a valid and appropriate route to the destination then the RREP packets are sending to the source by the nodes or by the destination itself. If no valid route is finding by the nodes then the RERR is send to the source node. If source node receives RERR again it will initiate a new route establishment.

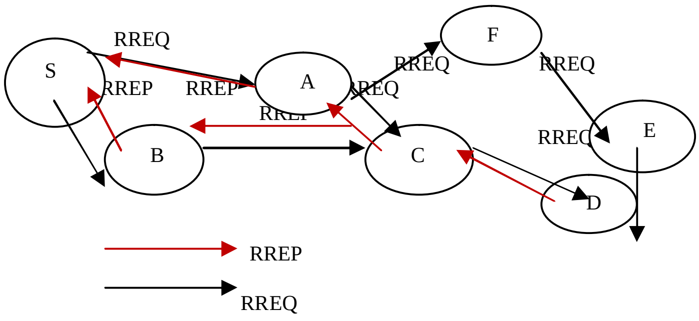


Figure (a). Route request and reply

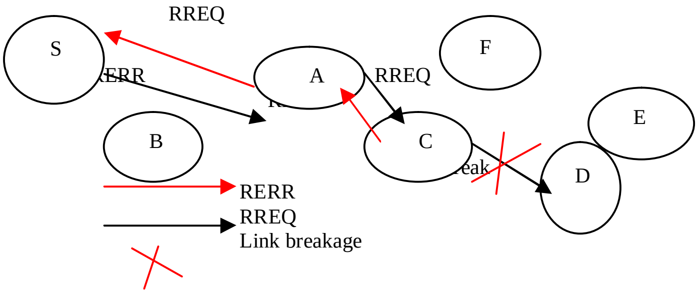


Figure (b). Route error and request
Figure: 2.1 (a) and (b) Route Discovery process

Route maintenance: In the figure 2.2 source node initiates a new route establishment process, destination or intermediate node will moves route error message is sent to source node. When intermediate node receives RERR will update their routing table by routing the distance. If source node receives RERR again it will initiate a new route establishment. In route maintenance there is link between C &D will breaks. Node C will evaluates route to D in route table. Node C creates a route error message. node A receives RERR.then source will also receives RERR message.

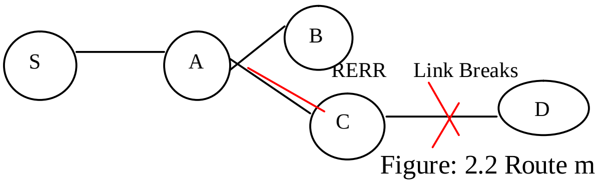
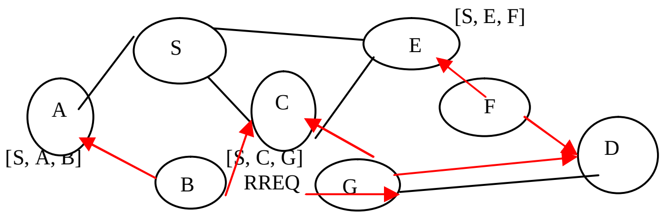


Figure: 2.2 Route maintenance

B. Overview Of DSR Protocol

DSR stands for Dynamic Source Routing and is a type of reactive protocol. DSR is an on demand protocol which is designed for use in multihop wireless network. The network of DSR is self organizing. This protocol has two methods route establishment and route maintenance.

Route establishment: It has two messages as route-request and route reply. In the figure 2.3 when a source node S wants to send message to the destination node D, it initiates route discovery by broadcasting the RREQ packet to its neighbours (S, E, and F). The intermediate nodes (A, E, F) on receive the RREQ packet rebroadcast the packet to its neighbours by appending its id in the route record of the RREQ packet. Similarly other intermediate nodes also forward the RREQ packet to the destination. When the destination node D receives two or more RREQ packets from the same source through different routes, it finds the two best routes based on the no of hopes. The route which has least number of hopes. The route which has least number of hops it becomes primary, and second least number of hops route becomes backup route. The destination node D sends Route Reply (RREP) packet. When source node S receives first RREP packet form destination, it treats this is the primary route and wireless communication is more error prone compared to wired network.



Destination D receives RREQ via G and F.It does not broadcast it further.
Figure: 2.3 DSR Route discovery process

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Route Maintenance: It is used to handle route breaks. When a node encounters a fatal transmission problem at its data link layer, it removes the route from its route cache and generates a route error message. The route error message is sent to each node that has sent a packet routed over the broken link. When a node receives a route error message, it removes the hop in error from its route cache. Acknowledgment messages are used to verify the correct operation of the route links.

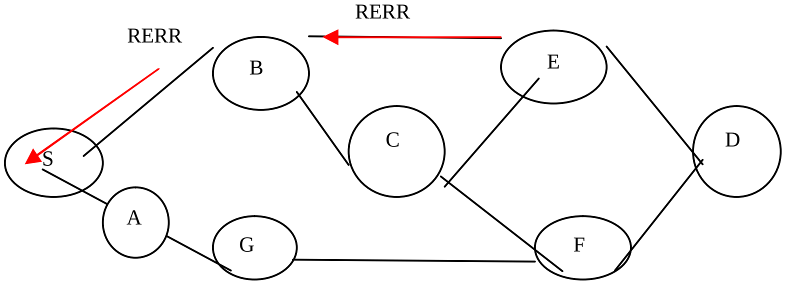


Figure: 2.4 Route Maintenance

III. RELATED WORK

In [1], states that there is a method used as Fidelity table that works on the AODV protocol, which decline one or many black hole nodes in the connection, where the selected or communicating node has been assigned a Fidelity Level which will ensure about the Reliability. When the level of point comes zero value, will be noted or recognized as a black hole node, were to be thrown out for the connection of the network. Drawback of this method is Delay. In [2], presents a method as Timer Expired Table, where sender will have to wait for reply from the neighboring nodes before sending any data packet to destination. Method is to fix the timer in Timer Expired Table when it will get First Request and it will try to collect next requests from neighbor nodes and with the sequence number, store it in CRRT with series number or sequence num at the period when data packet enters. In [3], proposed as the any of node when gets a route-reply packet, it will cross- checks or survey the next step through source to the destination from the correct Path. In the case next hop node does not have path that sent by route reply or not having direct path which got the REP marked as Malicious or attacking node. Drawback of this method is control overhead. In [4], proposed a Trust Based method for AODV Protocol. For AODV malicious nodes are not monitored. In the AODV first Sender will send a Request to destination and search a Path. AODV has contains the three messages as RREP, RREQ and RERR. RREP stands for route reply packets, RREQ stands for route request packets, whereas, RERR stands for route error reply. Here each connection point observes the next node will measure the trust value for the next node then when trust value reaches bellow it will be recognized to black-hole node, will decline from network. In [5] [6], presents the solution for black hole attack in MANET. As it contains the two purposes. It does not change or forward any packet. Here there are two applicable methods. First will be as to search extra or other path for routing as sender to receiver. Sender sends RREQ broadcast, Sender pass packet only when RREP is granted. When sender receives RREP it sends the packet. Other will be use a Packet Series number or sequence num within a Packet Header. The next packet has a higher sequence id value than the current packet. Value node contains update table to find if the packets are send or received by their sequence number. In [7] [8], states about the comprehensive study of AODV, DSDV, TORA and DSR protocols. The study considers the periodic advertisements, on-demand route discovery, hop-by-hop routing and source routing, and the usage of the feedback from MAC layer when there is a failure. In this paper, also evaluated the quality of service with some parameters include packet delivery ratio, average time delay, routing load overhead. The work concludes that DSR is performing better than the other routing protocols at different mobility factors such as the mobility rate and the movement speeds. In [9], analyses the performance of DSR routing protocol using OPNET simulation tool with different sizes of MANET models in which no. of nodes varies. The performance metrics used are average route discovery time, average route length, throughput, data network latency and data loss rate. The result concluded is that DSR is suitable for small scale MANET networks and it is necessary to improve DSR protocol for large scale MANETs. In [10], states that it is focused on the performance analysis of three routing protocols that are AODV, OLSR and DSDV using NS-3 simulation tool. Work analyzed routing protocols on four factors that are normalized routing load, packet delivery ratio, end to end delay, and throughput. with the analysis of routing protocols it showed that the OLSR performs better than AODV and DSDV protocols in terms of normalized routing load, throughput,

DOI: 10.15680/IJIRCCE.2016. 0407060

Packet delivery ratio for 2, 3, 4 mobile nodes. Work also showed that AODV perform better in terms of end to end delay than OLSR and DSDV.In [11] [12], evaluates three routing protocols which are DSDV, AODV and DSR. DSDV has low throughput but also has high routing load compared to AODV and DSR. Both AODV and DSR protocols perform very well. Although in some situations AODV outperforms DSR, DSR has the best performance especially when evaluated based on the Packet delivery ratio, normalized routing overhead and end-to-end delay while varying the number of sources and pause time has been performed average end to end delay. Moreover, changing the packet size doesn't affect the performance of DSDV but affects the performance of AODV and DSR. All protocols perform well when they are evaluated based on the mobility of the nodes. In the above related work there are some drawbacks on AODV and DSR.AODV has less delay, control overhead is less.DSR performance will be better in mobility rate and movement speeds.AODV performance will be better in delay, where the routing load is high in DSR and AODV will perform well.

IV. PROPOSED WORK

In this paper, a novel approach using Timer based concept is proposed to detect the black hole attack. Figure 4.1 shows flowchart for detection of black hole attack.In this work the route is established using modified AODV and modified DSR protocol between source and destination. As the source forwards the encrypted packet the timer is set. When timer expires it checks whether the next hop neighbour has received the packet, if not the trust value is decreased and updated to all the nodes. If the trust value reaches the minimum trust value the node is identified as malicious and updated to all the other nodes in the network.

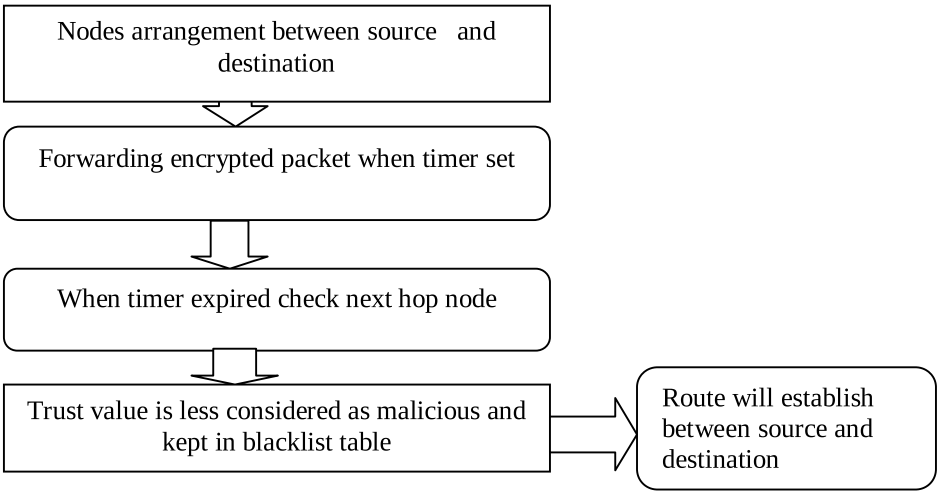

Nodes arrangement between source and destination
Forwarding encrypted packet when timer set
When timer expired check next hop node
Trust value is less considered as malicious and kept in blacklist table
Route will establish between source and destination

Figure: 4.1 Flowchart for detection of black hole attack

V. SIMULATION RESULTS

The simulations are carried out using Network Simulator (Ns-2), for 50 numbers of nodes using performance matrices such as packet delivery ratio, throughput and delay.

Parameter	Value
Total number of mobile nodes	50
Node Speed	0 to 20 m/s
Number of generated Packets	10000
Simulation Time	100 sec
Size of packet	512 bytes
Routing protocol	MAODV and MDSR

Figure: 5.1 Simulation Parameters

Simulations were done varying the speed keeping the pause time constant (0 sec) and then varying the pause time keeping the speed constant (5 m/s).The variation were done respectively varying the routing protocol from DSR to AODV . In all scenarios the Comparison were based on performance metrics as Packet Delivery Ratio, Delay and Throughput.

Packet Delivery Ratio (PDR): The ratio of Data packets delivered to those generated by the sources. The figure 5.11 depicts modified AODV has maximum packet delivery ratio and DSR has lowest.

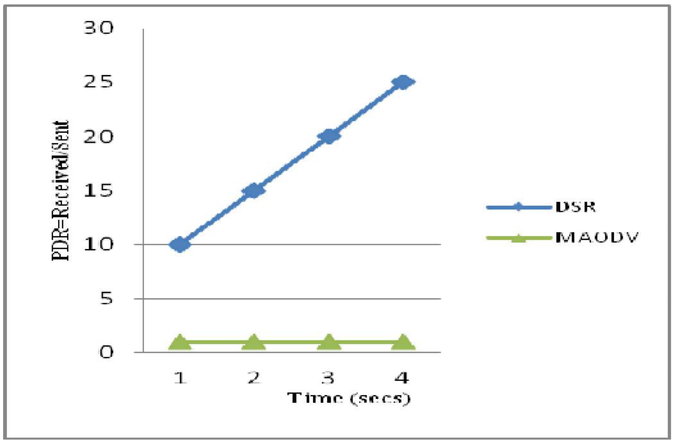


Figure: 5.11 MAODV packet delivery ratio and MDSR packet delivery ratio

Delay: the delay in delivering a packet to the destination which is inclusive of all kinds of delay.

As it can be seen from bellow figure 5.12 delay is highest in DSR followed by AODV having the lowest and most stable delay in mobility. DSR is a on-demand source routing protocol, and this is the major reason for it having a lower delay, AODV on the other hand has only one route per destination in the routing table, which is constantly updated based on sequence number delay does not change with increase in the number of nodes as the source and destination are in the same place moving with same speed, the increased number of nodes only might increase number of hops. Delay decreases with increase with speed, as when it moves more frequently the Routing updates are exchanged more frequently and faster it reaches the destination.

DOI: 10.15680/IJIRCCE.2016. 0407060

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

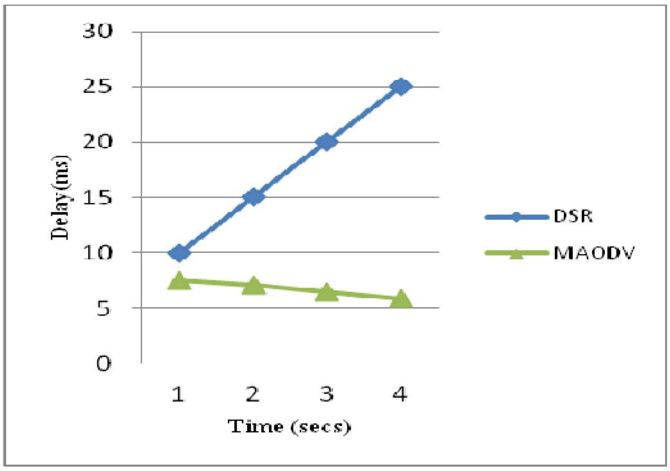


Figure: 5.12. MAODV delay and MDSR delay

Throughput: It is the rate of Packets transported or forwarded to the destination .It is measured in bits or per time slot or data packets per second. Throughput is lowest in DSR followed by AODV having the highest in mobility.

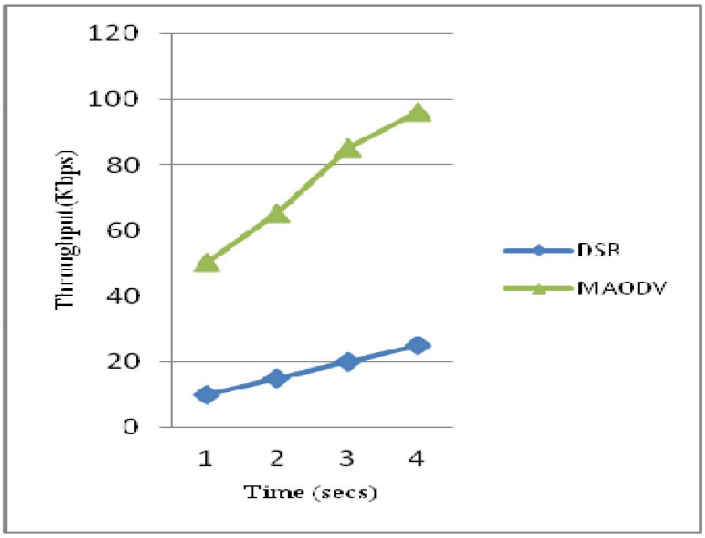


Figure: 5.13 MAODV Throughput and MDSR Throughput

VI. CONCLUSION

In this work a novel approach for (Timer based) method is proposed with modified AODV and modified DSR routing protocols. Proposed method works on Modified AODV routing protocol which is detection of attacker by encrypted packet and trust value updation using timer based method. Simulation results shows that amongst two protocols, AODV has a stable delay despite mobility as it has the feature of On-Demand Routing protocol and also maintains a Routing table and also has higher reliability.DSR has the highest delay and throughput as lowest. As compared with secured AODV and Modified AODV delay is less in modified and SAODV has high. Throughput and packet delivery ratio has maximum in MAODV and SAODV has low.As modified AODV uses one route to the destination, where modified DSR uses multiple routes to the destination.AODV will perform in higher mobility and in DSR will perform in lower mobility. Route discovery process is frequent in AODV and has less frequent route discovery process in

DOI: 10.15680/IJIRCCE.2016. 0407060

DSR.Based on the above simulation scenario, parameter, assumption and results AODV could be considered as an efficient faster routing protocol than DSR.

REFERENCES

1. Er.Kiran Narang, ’A Study Of Different Attacks In MANET And Discussion About Solutions Of Black hole Attack On AODV Protocol’, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 4, pp. 1601-1606 April 2. 2013.
2. Latha Tamilselvan, Dr.V Sankaranarayanan, ’Prevention of black hole attack in MANET’, the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, pp. 21-26, 2007.
3. Hitender Gupta, Harsh Aggarwal, ’Simulation to Detect and Removal of black hole in MANET’, SSRG International Journal of Electronics and Communication Engineering (SSRG-IJECE) EFES, pp. 35-40, April 2015.
4. Sharndeep Kaur, Dr. Anuj Gupta, ’A Novel Technique to Detect and Prevent black Hole Attack in MANET ’, International Journal of Innovative Research in Science, Engineering and Technology Vol. 4, Issue 6, pp. 4261-4267,June 2015.
5. Sharndeep Kaur, Dr. Anuj Gupta, ’A Novel Technique to Detect and Prevent black Hole Attack in MANET’, International Journal of Innovative Research in Science, Engineering and Technology Vol. 4, Issue 6, pp. 4261-4267,June 2015.
6. K.Lalramhluni, Aditya Bakshi, ’Detection of black Hole using Time Difference and Neighbourhood nodes’, IJISET International Journal of Innovative Science, Engineering & Technology,Vol.2, Issue 3, pp.1578-1583 , March 2015.
7. Ammar Odeh, Eman Abdel Fattah and Muneer Alshowkan, ’Performance Evaluation of AODV and DSR Routing Protocols in Manet Networks’, International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, pp. 14-21,July 2012.
8. Charu Sharma, Harpreet kaur, ’Literature Survey of AODV and DSR Reactive Routing Protocols,’ International Journal of Computer Applications (0975 – 8887), pp. 14-17, International Conference on Advancements in Engineering and Technology (ICAET 2015).
9. Charu Sharma, Harpreet kaur, ’Literature Survey of AODV and DSR Reactive Routing Protocols’, International Journal of Computer Applications (0975 – 8887), pp. 14-17, International Conference on Advancements in Engineering and Technology (ICAET 2015).
10. Pooja Sugandhi, Chhaya Nayak, ’A Review of Performance Evaluation & Enhancement of Proactive and Reactive Routing Protocols of MANET’, International Journal for Rapid Research in Engineering Technology & Applied Science ISSN (Online): 2455-4723, Vol 2 Issue 2, pp. 1-6 March 2016.
11. Deepti Sharma, Ankush Goyal, ’Performance Analysis of DSR and OLSR Routing Protocols for Fixed Wireless Sensor Networks (WSN)’, International Journal of Engineering Research and General Science Volume 3, Issue 3, ISSN 2091-2730, May-June, 2015.
12. Naveen Hemrajani, Nidhi Goyal, ’A Review of Comparative study of DSR and AODV Routing Protocols for Mobile AD-Hoc Network (MANET)’, International Journal of Engineering Sciences & Research Technology Hemrajani, 2(6): ISSN: 2277-9655, pp. 1536-1539, June, 2013.

BIOGRAPHY

Shridevi.K is a Assistant Professor in Computer Science and Engineering Department, College of Secab Institute of Engineering Technology, Vijayapur, Karnataka, India.

Sudha.S is a student studying M.TECH in Computer Science and Engineering Department, College of Secab Institute of Engineering Technology, Vijayapur, Karnataka, India.