IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

A Review on Different Methods to Prevent Black Hole Attack in MANET

Pranjul Sarathe[1*], Neeraj Shrivastava

[1]Dep. Of CSE, IES IPS Academy, Indore, India
[2]Dep. Of CSE, IES IPS Academy, Indore, India

Available online at: www.ijcseonline.org

Accepted: 15/Jun/2018, Published: 30/Jun/2018

Abstract- Mobile ad hoc networks (MANET) are dynamic, decentralized and infrastructure less network, where at any given point of time nodes can join or leave the network. Due to the property of flexibility and simplicity MANET are widely used in military communication, mobile conferencing and emergency communication. As Ad-hoc networks are autonomous mobile nodes, they form a temporary based network which has no fixed infrastructure. Every node in the network is autonomous hence they act as host as well as router. Due to this nature of MANET, where any node can join or leave the network without any permission, security is the main challenge in such networks. One of the major security issues in MANET is Black hole attack. It occurs when a malicious node referred as black hole joins the network. during the process of discovering route this node acts as if it has route to the destination and takes all the packets into it and does not forward to the desired destination, Instead it drops all the packets. In this paper, we have surveyed on few of the techniques and methodologies for detecting and preventing black hole attack in MANET using AODV routing protocol.

Keywords: MANET, AODV Routing Protocol, Ad hoc network, Black hole

1. INTRODUCTION

Wireless unintended networks area unit cluster of autonomous nodes that may be self-managed with no infrastructure. MANET is a unit spontaneous and dynamic in nature therefore any node can be part of or leave the network at any given time. Unintended networks area unit are temporary networks that area unit established in situation wherever no fastened infrastructure is needed [2][4]. The nodes act as host and router they exchange and forward packets for his or her communication. MANET use routing protocols for such communication, they'll be either proactive routing protocol(table driven routing protocol) within which routing data of nodes area unit changed sporadically like DSDV- destination sequenced distance vector,[3]

OLSR- optimized link state routing protocol. reactive routing protocol(on-demand routing protocol) within which route is established and nodes exchange data only required like AODV- unintended on demand distance vector, DSR- dynamic source routing[3] . With the exception of nodes acting as host they conjointly act as router in discovering nodes and forwarding packets to the right node within the network. As wireless unintended networks don't have any fastened infrastructure they're a lot of receptive attacks. One in all the key attacks is that the part of attack. The malicious node absorbs all the packets in it sort of a hole which sucks in everything, thus it's named as part attack. Within the AODV routing protocol the method of route discovering is completed by the intermediate nodes that area unit liable for finding recent path to the destination by causation discovery packets to the neighbor nodes. Malicious node does not fallow this process instead it immediately responds to the source node with false information stating it has the fresh path to the destination. Source node then sends all its packets to the destination via this malicious node assuming it has the route. Black hole attack occurs when this malicious node drops all the packets and does not send packets to the desired destination node.

1.1 AODV ROUTING PROTOCOL

AODV is a reactive routing protocol in this network generates route to start the communication. It does not maintain any routing information or does not participate in any periodic routing table exchange [1]. It does not have to keep track of the route information neither discover the route until the two nodes needs to communicate with each other. In the below figure, AODV route discovery process is explained [5].

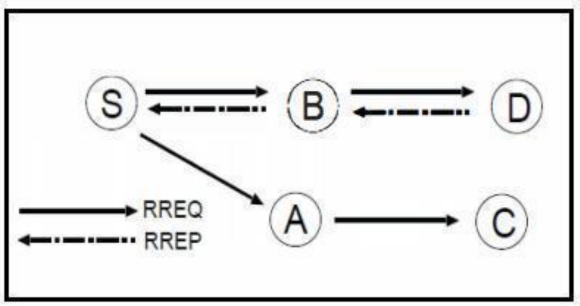


Fig.1. AODV route discovery process

In the figure 1, node S is the source node trying to establish route to the destination node D, if S does not have route information about D in its table it simply broadcast route request packets RREQ to all its neighbor nodes. When node A and B receive RREQ packet it checks in its respective routing table for the fresh route to the destination. If it has the route for destination it reply back to the source node using RREP packet and the source node send packets via the intermediate node by changing the route table information in its node.

If the intermediate node does not have a fresh path to the destination it simply broadcast the RREQ packet to its neighbor nodes and this is done until the destination node D receives RREQ packet. When node D receive RREQ packet it sends back reply using RREP packet hence a connection is established between node S and node D. In case when source node S receives multiple RREP's it selects the one with higher destination sequence number and if all the RREP's have same destination sequence number it considers the one with lower hope count value.

1.2 BLACK HOLE ATTACK

A black hole attack is a kind of denial of service attack in which a malicious node absorb all packets itself by falsely claiming a fresh route to the destination and drop them without forwarding them to the destination [2]. In this kind of attack the faulty node advertise itself for having a fresh route and shortest path to the destination without even checking its routing table information.

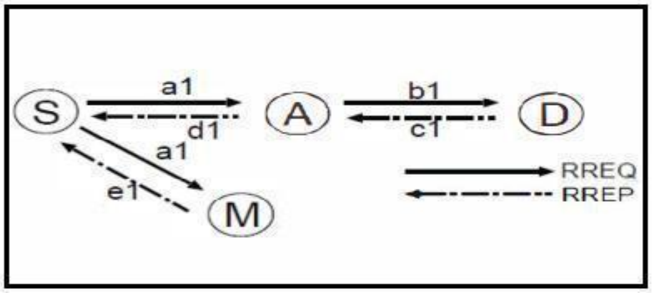


Fig.2. Black hole attack

In the figure 2, S is the source node which wants to send packets to D the destination node. Every node has two types of packets to be sent to the destination, one is routing packet and other is data packet. When node S wants to send data packets to node D it sends the route request packets also called as (RREQ) to its neighboring nodes.

Let us assume that nose M is faulty node, after getting the RREQ packet from S it immediately reply back stating that it has fresh path to the destination without even checking its routing table. Once node S has got the (RREP) route reply packet from M it sends all data packets to M thinking it has the shortest and fresh path to the destination. But node M does not forward packets to the destination and drops all packets. Node M replies back with minimal hope count value and highest destination sequence number so source node S sends all its packets to the malicious node M. With this attack all the data packets are falsely taken from the source node and are dropped without sending to the destination.

Two types of black hole attack

1. **Internal black hole attack**

Here the faulty node is present inside the network. It takes part actively in the communication of source and destination. This is called as internal attack because the malicious node belongs to the network internally [1]. This attack is more severe as the malicious node actively takes part in the network.

2. **External black hole attack**

Here the faulty node stay outside the network and deny access to network traffic. This attack can become internal attack when it takes control of internal malicious node and control it to attack other nodes in the network[1].

Rest of the paper is organized as follows, section 1 contains the introduction of AODV protocol and black hole attack. Section 2 contains literature survey and table of different used techniques. Section 3 contains performance parameters. Section 4 contains comparative analysis. Section 4 contains conclusion and section 5 contains references.

2. LITERATURE SURVEY

K. Madhuri et al. [1] used 20, 50 and 100 nodes for single malicious node and 2 malicious node and analyzed the effect of black-hole attack during passing the data packets and used Intrusion detection system (IDS) that will prevent the attack and increase the packet delivery ratio, throughput and reduce the packet drop rate.

S. R. Deshmukh et al. [2] proposed secure routing mechanism in which source node send RREQ and when RREQ is received by other nodes it checks for route to destination is present or not, if there is no route so it will forward RREQ to destination node and if route is present

then node will generate RREP with validity value and send back
sender node receives RREP and check if validity value = = 1 it will update route table and forward RREP to source node and then data is successfully send to destination.

G. Bendale and S. Shrivastava [3] proposed threshold estimation and black-hole detection and prevention algorithm in which firstly initiated the network and start the route discovery process using RREQ and RREP as always attacker discover in first route now calculate threshold value and broadcast it in entire network threshold value is used for route validation if route is secure then communication is started between nodes and if route found is not secure then start next route selection. it also has compared traditional AODV and measured performance. It provided good packet delivery ratio, less end to end delay and throughput.

A. siddiqua et al. [4] proposed a secure knowledge algorithm in which before forwarding packet to neighbours it compares the value such as fm which contains information about recently transmitted packet and rm which contains information about node related to recent packet which is stored in knowledge table if values are different, nodes are black-hole, algorithm is used to prevent trusted node from becoming a black-hole node by broadcasting black-hole node ID to other nodes.

C. B. Dutta and U. Biswas [5] proposed algorithm is multipath AODV and the attack scheme is energy aware. here attacker wants to damage more than one path in single attempt, it looks for a node through which multiple paths are available so less number of malicious nodes are involved that will consume less energy and attacker optimizes energy and can perform the task for the long duration of time. It causes increasing end to end delay and reducing packet delivery ratio as compared to traditional AODV.

V. Gaikwad and L. Regha [6] has proposed new technique used cooperative cluster agents for detecting cooperative black-hole attack by collecting node ID's and if any node ID matches to the Id present in block table, system immediately drop this node id and broadcast an alert notification in the network by applying this method system is avoiding cooperative black-hole attack and used DRI(data routing information)and SRT-RRT(senders-receivers packet record tables)as an input to cooperative security agents.

S. jain and Dr. A. khuteta [7] used base node which sends dummy RREQ in the network and waits for reply, authentic nodes don't send reply. but malicious node will send RREP without checking its route table, after receiving all replies base node create a block message for this node and broadcast it in the network. Block message has two fields one is ID of Base node and second is ID of Black-hole node when neighbour nodes receive bloc notification, It extract the black-hole node Id and add it in blacklist.in future work more than one BN can be used. It will increase the performance of the system.

In the below table1, shows the different black-hole detection and prevention methods, and their performance based on different parameters like PDR, throughput, E2E delay and packet drop ratio.

s.no.	Author name	Method used	No. of nodes	Performance	Research gap
1.	C. B. Dutta and U. Biswas (2014)	Multiple alternative path is damaged in single attempt and less power Consumption using multipath AODV.	100,120	Under the proposed energy aware black-hole attack PDR is decreasing and end to end delay is increasing.	Extra memory is required.
2.	V. Gaikwad and L. Regha (2015)	Cooperative security agents are used to Prevent Cooperative black-hole attack.	Not Defined	After using Algorithm throughput and PDR is increasing.	If mobility of node increases performance degrades and network load also increases.
3.	S. jain and Dr. A. Khuteta (2015)	Base node is Used To send fake RREQ and using a block table which contains two fields base node ID and malicious node ID and the method is useful to detect black-hole attack	10,50	Energy and delay is reduced by using Proposed method PDR has improved.	If no. of nodes are increasing than performance is decreasing.
4		Analysis of black-hole attack with two malicious node.	100	PDR- 9, throughput-430 kbps and packet drop ratio is 1119	It has only analyzed on two parameters PDR and Throughput.
5.	S. R. Deshmukh, P. N. Chatur and N. P. Bhople	Validity value is implemented in RREP message	100	Proposed method not Required Additional	Extra memory is required for extra header bits

	(2016)	and packet size is 512 byte is used.		memory and Large processing, it improves the performance of system.	
6.	G. Bendale and S. Shrivastava (2016)	Proposed two algorithm one for threshold estimation and second is for black-hole detection and prevention.	100	Under the attack Conditions Proposed Mechanism increased packet delivery ratio, throughput and produced less end to end delay.	Increased Routing Overheads effects the performance of system.

3. PERFORMANCE PARAMETER

i. **Packet Delivery Ratio(PDR)**

PDR is the proportion of the total amount of packets reached the receiver and amount of packet sent by the source it can be calculated by given formula in eq1:

$$PDR = \frac{\text{Total amount of data packet received (Receiver)}}{\text{Total amount of packet Sent (Source)}} * 100………(1)$$

ii. **Throughput**

It is the ratio of successfully received packet to the simulation time. and it can be estimated By given eq2:

Throughput = Packet Received / simulation Time………………………(2)

iii. **End To End Delay**

This parameter can be defined as the time taken by packets to reach from source to destination. It can be calculated by given formula in eq3:

E2E Delay = Receiving Time – Sending Time………………….(3)

iv. **Residual Energy**

It is the remaining amount of energy or power after the complete communication process has been done. Energy can be calculated by formula given below in eq4:

Residual Energy = Initial Energy of Node - Energy Consumed during Communication………(4)

4. COMPARATIVE ANALYSIS

We analyze the work of Balachandra and Nisha P. shetty in “Interception of Black- Hole Attacks in Mobile AD-HOC Networks” [10] and K.Madhuri, N.Kasi Viswanath and P.Usha Gayatri in “Performance Evaluation of AODV under

Black Hole Attack in MANET using NS2" [1]. In "Interception of Black- Hole Attacks in Mobile AD-HOC Networks" [1] they simulated using NS-2.34 in Linux operating system. The basic network set up initiated with 20 number of nodes and it varies up to 100 nodes. It uses an area of 800 × 800 meter flat space, mobility model is Random Way Point Model, node speed is 0.50 m/sec and pause time is 10 seconds.

It uses Constant Bit Rate (CBR) as a traffic model. Time duration for the simulation is 200 Seconds. Three cases are taken for the simulation, SAODV with and without black hole attackers and extended SAODV protocol. Below table and graphs shows the results obtained.

Table:2. Experimental Results[10]

PARAMETERS	*SAODV*	*SAODV-ATT*	*EXTENDED SAODV*
Packet Delivery Ratio	*97.60%*	*29.33%*	*99.66%*
Throughput	*39.50%*	*10.43%*	*50.60%*
End to End Delay	*32.50%*	*55.25%*	*21.77%*

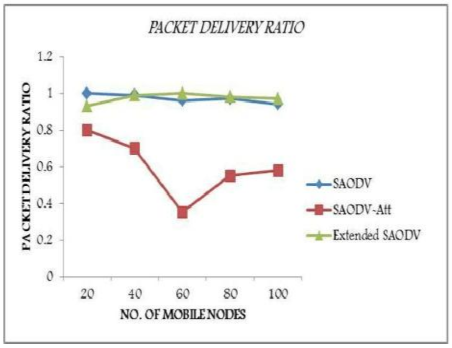


Fig.3. Packet Delivery Ratio VS. Number if Mobile nodes[10]

In the above figure packet delivery ratio has been analyzed with respect to various nodes.

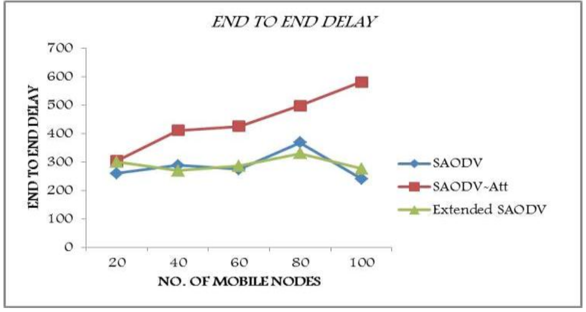


Fig.4. Delay VS. Number if Mobile nodes[10]

In the above figure end to End Delay has been analyzed with respect to various nodes.

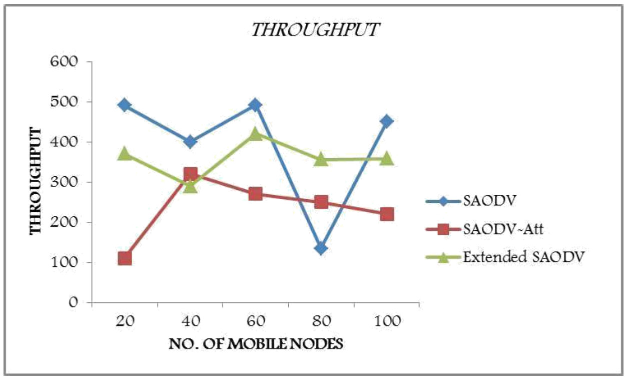


Fig.5. Throughput VS. Number of Mobile nodes[10]

In the above figure Throughput has been analyzed with respect to various nodes.

In "Performance Evaluation of AODV under Black Hole Attack in MANET using NS2" [1] they analyze the effect of Black hole attack while routing the data Packets using AODV for various network parameters like Packet Delivery ratio, Packets dropped and Throughput for 20, 50 and 100 nodes with 2 malicious nodes in the network. Below table and graphs shows the results obtained.

Table:3. PDR in the Presence of One and Two Malicious Nodes[1]

No of nodes	PDR for single malicious node	PDR for 2 malicious nodes
20	40.02	21.2
50	4.19	1.04
100	11.70	9

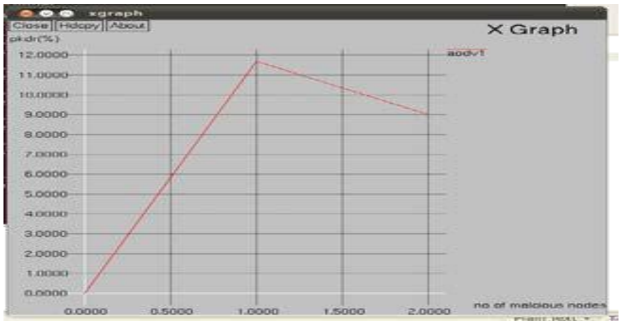
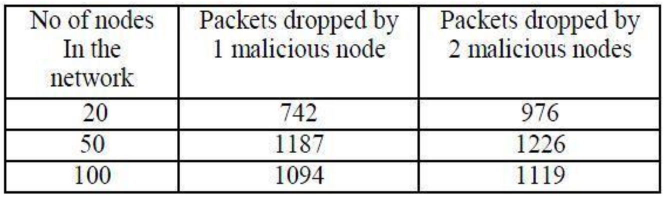


Fig.6. PDR for 100 nodes in the presence of two malicious nodes.[1]

Table:4. Packet Dropped by one and two malicious nodes[1]



No of nodes In the network	Packets dropped by 1 malicious node	Packets dropped by 2 malicious nodes
20	742	976
50	1187	1226
100	1094	1119

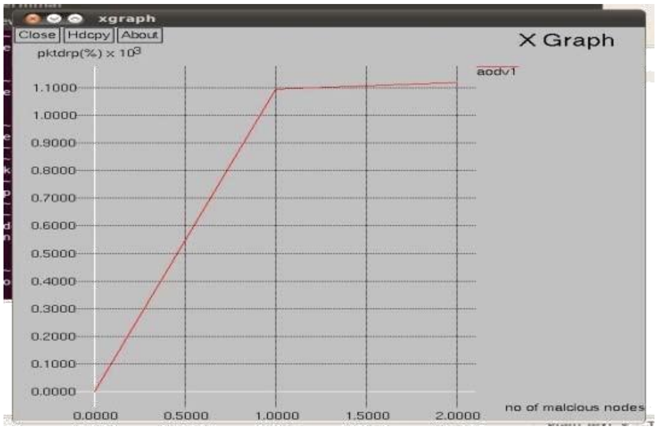


Fig.7. Packets dropped by two malicious nodes for 100 nodes[1]

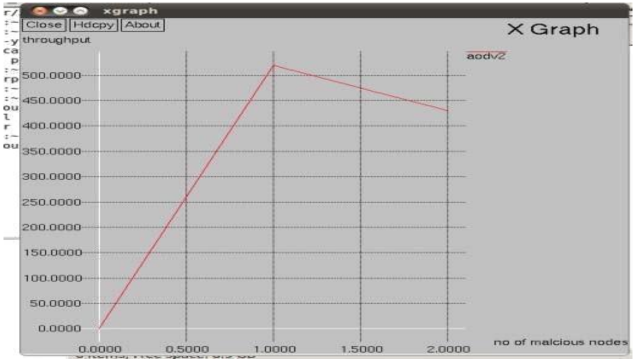
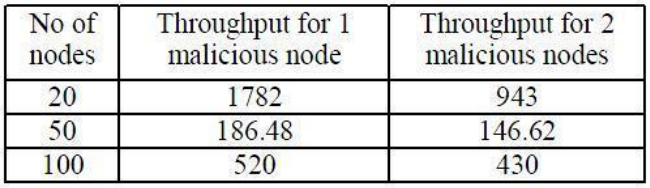


Fig.8. Throughput for 100 nodes in the presence of two malicious nodes[1]

Table:5. Throughput in the presence of one and two malicious nodes.[1]



No of nodes	Throughput for 1 malicious node	Throughput for 2 malicious nodes
20	1782	943
50	186.48	146.62
100	520	430

5. CONCLUSION

A Black Hole attack is one among the most important security issues in MANETs. During this a malicious node impersonates a destination node by sending false RREP to the source node and collects all the packets in it and drops them. In AODV routing protocol the main security threat that degrades the performance is the black hole attack. These methods have benefits like higher packet delivery or support multiple black hole attack at the same time. All of these methodologies have some or the opposite drawbacks, either it might be having higher overhead, higher packet loss, doesn't support cooperative black hole attack or increased end to end delay. Primarily based on the above performance comparisons, it can be concluded that Black Hole attack affects network negatively. Thus there is a desire for perfect detection and elimination of black-hole mechanism that relies on cluster organization of network. This supports cooperative black hole attack and additionally offers way to facilities the server node to overcome the failure. Thus providing security for Black hole attack and Efficient in detection and prevention are the future need for Ad hoc networks.

6. REFERENCES

[1] K. Madhuri, N. K. Viswanath and P.U. Gayatri "Performance Evaluation of AODV under Black Hole Attack in MANET using NS2", IEEE International Conference On ICT and Business Industry & Government (ICTBIG), pp. 1-3, Nov. 2016.

[2] S.R. Deshmukh, P.N. Chatur and N.B. Bhople "AODV-Based Secure Routing Against Black-hole Attack in MANET", IEEE International Conference On Recent Trends in Electronics, Information & Technology, pp. 1960-1964, ISSN:978-1-5090-0774, May 2016.

[3] G. Bendale and S. shrivastava "An Improved Black-hole Attack Detection and Prevention Method for Wireless Ad-hoc Network", IEEE International Conference on ICT in Business & Government, pp. 1-7, ISSN: 978-1-5090-5515, Apr. 2016.

[4] A. Siddiqua, K. Sridev and A. A. Khan Mohammad "Preventing Black-hole Attacks in MANET Using Secure Knowledge Algorithm" IEEE International Conference On Signal Processing and Communication Engineering System, Jan2015, pp. 421-425.

[5] C. B. Dutta and U. Biswas "An Energy Aware Black-hole Attack for Multipath AODV ", IEEE International Conference On Business and Information Management, pp. 142-147, ISSN: 978-1-4799-3264-1, Jan. 2014.

[6] V. Gaikwad(Mohite) and L. Ragha "Security Agents for Detecting and Avoiding Cooperative Black-hole Attacks in MANET", IEEE International Conference On Applied and Theoretical Computing & Communication Technology, pp. 306-311, ISSN: 978-1-14673-9223, Apr. 2015

[7] S. Jain and Dr. A. Khuteta "Detecting and Overcoming Black-hole Attack in Mobile Ad-hoc Network", IEEE International Conference On Green Computing and Internet of Things, pp. 225-229, ISSN: 978-1-4673-7910, Jan. 2015.

[8] L. Mejaele and E. O. Ochola "Effect of Varying Node Mobility in the Analysis of Black Hole Attack on MANET Reactive Routing Protocol", IEEE Information Security for South Africa(ISSA), pp. 62-68, ISSN: 978- 1-5090-2473, Aug. 2016.

[9] H. Kaur and A. singh "Identification and Mitigation of Black Hole Attack in wireless Sensor Networks",IEEE International Conference On Micro-Electronics and Telecommunication Engineering, pp. 616-619, Sept. 2016.

[10]Balachandra and N. p. Shetty " Interception of Black-Hole Attacks in Mobile AD-HOC Network" IEEE International Conference On Inventive Computation Technology(ICICT), pp. 1-5, volume-3, ug. 2016.

[11] B. Singh, D. Srikanth and C.R. Suthikshn kumar, “mitigating effects of Black hole Attack in Mobile Ad- hoc Networks: Military Perspective”, IEEE International Conference On Engineering and Technology, pp. 810-814, ISSN: 978-1-4673-9916, March 2016.

[12] A. Dorri and H. Nikdel “A New Approach for Detecting and Eliminating Cooperative Black hole node in MANET”, IEEE Conference On Information and Knowledge Technology, pp. 1-6, ISSN: 978-1-4673-7485-9, May 2015.

[13] H. Moudni, M. M. Mouncif and B. El Hadadi “Modified AODV Routing Protocol to Improve Security and performance against Black Hole Attack”, IEEE International Conference On Information Technology for Organizations Development, pp. 1-7, ISSN: 978-1-4673-7689, Apr. 2016.

[14] F. Thachil and K. C. Shet “A Trust Based Approach for AODV protocol to Mitigate Black-hole attack in MANET”, IEEE International Conference in Computing Science, pp. 281-285, Sept.2012.

[15] R. Yerneni and A. K. Sarje “Secure AODV Protocol to mitigate Black Hole Attack in Mobile Ad-hoc Networks”, IEEE International Conference on Computing Communication and Networking Technologies(ICCCNT), pp. 1-5, July 2012

Authors Profile

Miss P. Sarathe completed bachelor of engineering in computer science from RGPV University Bhopal, India and my CGPA is 7.56 with honors in 2016. I have done minor project in PHP and the topic was “Bhopal Darshan”, and I have completed my major project and the name was “Emergency Call” it was a women safety app in which you only have to press volume button of your mobile and message and call will reach to your selected contacts with your location. Currently I am pursuing ME from IES IPS Academy Indore.

Mr. N. Shrivastava is Associate Professor at IES IPS Academy Indore, He did his M. Tech from Maulana Azad national institute of technology Bhopal in 2009. Currently he is pursuing ph.D. from Maulana Azad national institute of technology Bhopal. His research work focuses on image processing, ad-hoc network, algorithm etc. he published around 20 international journal and 10 international conferences. 10 years of Teaching and research experience