Hybridization Optimization Approach For Energy Efficiency on Wireless Sensor Network

Neha Kohli, Er. Sukhpreet Kaur

Computer Science and Engineering, Shaheed Udham Singh College of Engineering and Technology, Tangori

***Abstract*—**Mobile ad-hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. Mobile ad-hoc network consists of spatially distributed autonomous sensor nodes to monitor surroundings at different locations. Security is one of the core issues in mobile ad-hoc sensor networks because packets are having less security in transmission from source to destination which degrades the quality of service. It is desirable to make these nodes as cheap and reliable as possible and rely on their large numbers to obtain high quality results. As the number of packet losses increases the routing error rate increases which must be low. Security is a major challenge for these networks due to their features of open medium, dynamically changing topologies. The black hole attack is a well known security threat in mobile ad hoc networks. Black hole attack is a serious kind of security flaw, where a malicious node advertises itself for having the shortest path between source and destination. Therefore, the network traffic is attracted by the malicious attacker and most of the data is lost when the malicious node found a data packet. In this paper, the deployments of the nodes in the network are performed and convergence set are also evaluated. The attack scenario is implemented by using the hybrid routing optimization (PSO +Firefly) and performance is evaluated in the presence of attack. The proposed approach is also evaluated by using the various parameters such as energy consumption, routing overhead and throughput to increase the lifespan of the network. The proposed secure routing technique is able to provide the efficient results and also able to overcome the routing based attack detection and prevention.

Keywords*—*PSO, Firefly, WSN, Manet, Black hole, Grey Hole

I. INTRODUCTION

Wireless network is the one in which, computer devices communicate with each other without any wire. The communication medium between the computer devices is wireless. When a computer device wants to communicate with another device, the destination device must lay within the radio range of each other. Users in wireless networks transmit and receive data using electromagnetic waves. Recently wireless networks are getting more and more popular because of its mobility, simplicity and very affordable and cost saving installation.

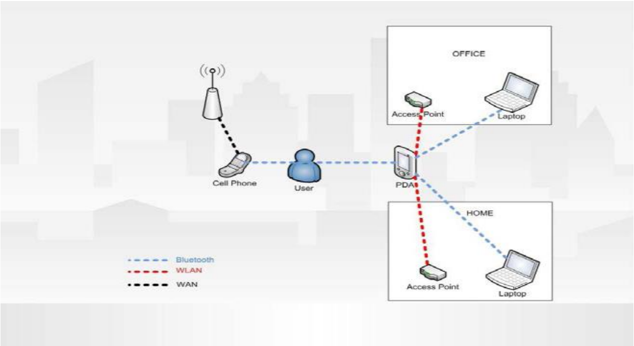

Fig. 1: Communication in Wireless Networks

Wireless networks are getting popular due to their ease of use. Consumer/user is no more dependent on wires where he/she is, easy to move and enjoy being connected to the network.

One of the great feature of wireless network that makes it fascinating and distinguishable amongst the traditional wired networks is mobility. This feature gives user the ability to move freely, while being connected to the network. Wireless networks are comparatively easy to install than wired network. There is nothing to worry about pulling the cables/wires in walls and ceilings. Wireless networks can be configured according to the need of the users. These can range from small number of users to large full infrastructure networks where the number of users is in thousands. Wireless wide area network (WWAN) cover geographically larger area than local area network. The wide area networks almost consist of one or two local area networks. Examples of WWAN are Satellite Systems, Paging Networks, 2G and 3G Mobile Cellular.

A. MANET

A Mobile ad hoc network (MANET) is a collection of autonomous mobile nodes which communicate with one another using wireless links [31]. They cooperate in a distributed fashion to provide network functionality in the absence of fixed network infrastructure. Nodes are typically small, light-weight, and battery powered. They usually have fewer resources and are less capable than a desktop or portable computer. The network topology is dynamic due to node mobility [4]. The autonomy and self-sufficiency of MANETs enables them to be deployed as standalone network which do not require network infrastructure [3]. MANETs can also play an important role in accessing networked services in the Internet. MANETs as edge networks could facilitate internet service access to broader groups of users. For example, emergency responders in a disaster relief scenario may require internet connectivity to communicate with their headquarters or to access resources available on the internet. Since mobile nodes in MANETs communicate over a wireless channel, message security and transmission are indeed a major concern. MANETs are vulnerable to several distinct types of attacks, including blackhole attacks, wormhole attacks, sybil attacks, Denial of Message (DoM) attacks, to name a few [6].

II. ATTACKS ON AD HOC NETWORKS

There are number of attacks which harm the performance of ad-hoc network. In this section some of these attacks will be addressed.

A. *Routing Loop*

By sending forged routing packets an attacker can create a routing loop [10]. This will result in data packets being sent around consuming both bandwidth and power for a number of nodes. The packets will not reach their intended recipient and thus can be considered a sort of denial-of-service attack.

B. *Black Hole*

The setup for the black hole attack is similar to the routing loop attack in which the attacker sends out forged routing packets [6]. It can setup a route to some destination via itself and when the actual data packets get there they are simply dropped, forming a black hole where data enters but never leaves. Another possibility is for the attacker to forge routes pointing into an area where the destination node is not located. Everything will be routed into this area but nothing will leave also creating a sort of black hole.

C. *Grey Hole*

A special case of the black hole attack is an grey hole attack [10]. In this attack the adversary selectively drops some kinds of packets but not other. For example the attacker might forward routing packets but not data packets.

D. *Partitioning*

Another kind of attack is for the attacker to create a network partition in which some nodes are split up to not being able to communicate with another set of nodes. By analyzing the network topology the attacker can choose to make the partitioning between the set of nodes that makes the most harm into the system. This attack can be accomplished in many ways.

E. *Blackmail*

Some Ad Hoc routing protocols try to handle the security problems by keeping lists of possibly malicious nodes. Each node has a blacklist of, what it thinks, bad nodes and thereby avoiding using them when setting up routing paths. An attacker might try to blackmail a good node causing other good nodes to add this node to their blacklists and so avoid it.

F. *Wormhole*

In the wormhole attack an attacker uses a pair of nodes connected in some way. It can be a special private connection or the packets are tunneled over the Ad Hoc network. Every packet that one of the nodes sees is forwarded to the other node which in turn broadcasts them out. This might create short circuits for the actual routing in the Ad Hoc network and thereby create some routing problems. Also, all the data can be selectively forwarded or not using this attack thereby controlling the Ad Hoc network to a large extent. This kind of attack together with a partitioning attack can gain almost complete control over the network traffic.

G. *Rushing*

Many reactive routing protocols keep a sequence number for duplication suppression at every node. An attacker can distribute a large number of route requests with increasing sequence numbers forged to appear to be from other nodes. This way when the actual route request is sent out, many nodes suppress it as a duplicate and thereby disrupt the actual route discovery.

H. *Resourse Consumption*

By injecting extra data packets into the Ad Hoc network, limited resources such as bandwidth and maybe battery power are consumed for no reason. Even more resources might be consumed by injecting extra control packets since these might lead to additional computation. Also, the other nodes might forward control information as it comes in resulting in even more resource.

III. LITERATURE REVIEW

Shobina et al. (2017) objective of research was to avoid and detect black hole attack in MANET. It was basically used for military purpose. The approach started with the detection and separation of malicious node in ADOV routing protocol due to which black hole attacks occurs in MANET. As black hole attack basically utilizes the routing protocol and claims as if it is the shortest path to the destination but it drops the packets to its neighbors.

Kumari et al. (2017) presented the work which gives stress on the security while sending data packets to different routing paths due to black hole attack. As wireless sensor networks are mostly used in form of application. Wireless sensor network consists of very sensible information which was quite a serious problem as the point of security.

Khemariya et al. (2016) analyzed the problem of black hole attack in wireless environment. Black hole attack was considered as the main issue to get degraded wireless communication. They used the technique AOVC routing protocol for surveying the effect of that attack on network. Network simulator (NS2) was used for simulation. It was the serious problem because a malicious node chews all data packets in itself, same way to a hole which sucks in everything in.

Nakum et al. (2016) objective of this research was to remit the impact of black hole and grey hole attacks in AODV network. Security in wireless communication is very important, so that unauthorized access or damage can never happen. Hackers had found wireless network relatively very easy to break. AODV known as ad-hoc demand network is routing protocol used in MANET.

IV. RESEARCH PROBLEM FORMULATION

Mobile ad-hoc network consists of spatially distributed autonomous sensor nodes to monitor surroundings at different locations. Security is one of the core issues in mobile ad-hoc sensor networks because packets are having less security in transmission from source to destination which degrades the quality of service. It is desirable to make these nodes as cheap and reliable as possible and rely on their large numbers to obtain high quality results. As the number of packet losses increases the routing error rate increases which must be low. Consequently many protocols have been proposed in order to minimize the losses or overheads in the network. The efficiency of mobile ad-hoc networks strongly depends on the secure routing and protocol used. So this thesis will work on the secure routing in MANET in which several simulations will be conducted to analyse the performance including the power consumption and overall network performance like packet delivery ratio, energy consumption, throughput, routing overhead. As we know that MANET is a network containing of multiple wireless devices, also called nodes, which collaborate in sensing certain sort of physical or conservational conditions. Because of the situation of mobile sensor schemes, all sensor nodes in the network may not have a shortest linking to the base position. Therefore, they use multi-hop broadcasting in order to interconnect. They have very limited consumption of energy, computational influence and memory sharing

A. Research objectives

A Mobile Ad Hoc network is a self-configuring networks consisting of mobile nodes without any fixed infrastructure. These wireless devices communicate with each other directly if they are in the same network coverage area. If they are out of the coverage range, the communication will require the formation with the help of cooperatives. The objectives of the research work are:

1. To study the various routing protocols and their consequences in routing performance in MANET.

2. To perform deployment of the nodes in the network and evaluation of the coverage set.

3. To implement the attack scenario and evaluate the performance in the presence of attack.

4. To implement hybrid routing optimization approach (PSO + Firefly) to mitigate the effect of attack and evaluate the performance in terms of energy consumption, routing overhead and throughput to increase the lifespan of the network.

V. RESULT & DISCUSSION

Mobile ad hoc network deals with dynamic and multi hop strategies, unorganized infrastructure that consists of IP service and autonomous procedure and tasks. Battlefield circumstances and natural adversities are circumstances where it is very dangerous and most difficult task to organize the network. MANET provides explanation for various situations. It includes mobile nodes which are to deployed in the configurations for the creation of the network and communicate through wireless connectivities. Security is the key issue in MANET. Various intruders intrude and obtain black hole nodes to generate such fake route which direct to the destinations and will able to achieve high packet losses. So this proposed approach deals with the hybrid optimization algorithms using PSO and Firefly to mitigate the effect of the black hole attack and increase the lifetime of the network to achieve less packet losses Algorithms used in the proposed approach are given below.

A. Particle swarm optimization

Particle Swarm Optimization (PSO) is a simplified algorithm that optimizes the problem in an iterative manner which will provide global best solutions from the number of solutions. It deals with free space search operations over the particle's position and velocity and can seek vast spaces to get best optimized solution. So, PSO is generally considered for the sake of optimization which is popularly known as routing optimization.

```
For every particle j = 1, ..., swarm do
Set the particle's location with a consistently dispersed random vector Xi
Set the particle's best recognized location to its initial location Pi
If f (Pi) <f (gb) then
    1. Update the swarm's finest known position: gb
    2. Set the particle's speed: vi
    3. While a finishing is not encountered do
       For each particle ij= 1, ..., Swarm do
       For each measurement d = 1, ..., n do
    4. Evaluate fitness function
    5. Update the particle's speed: vi, Update the particle's location: xi, Update the best known location: gb
```

Where gbis the resultant global best optimize solution which is done in the iterative manner.

B. Firefly Optimization algorithm

It is also one of the efficient algorithm which is used to achieve optimizations and having less error rate probabilities while reducing the randomness of the firflies and achieving high link stability. The steps of the algorithm are discussed below:

1) Objective function: f (x) , x = (x 1 , x 2 , . . . , x d)

```
 2) Generate an initial population of fireflies x i ( i = 1 , 2 , , n)
 3) Formulate light intensity I so that it is associated with f(x )
 4) Define absorption coefficient $\gamma$
  While (t < MaxGeneration)
     for i = 1 : n (all n fireflies)
        for j = 1 : n (n fireflies)
           if ( I j > I i )
              Vary attractiveness with distance r via $\exp^{(-\gamma r)}$
              move firefly i towards j;
              Evaluate new solutions and update light intensity;
           end if
        end for j
     end for i
     Rank fireflies and find the current best;
  end while
end
```

C. The Proposed approach is divided into various steps

Step 1: Nodes Location evaluations

Step 2: Nodes Deployment in the network to create the network

Step 3: Coverage Area Evalaution

Step 4: Generation of the fake route through black hole node.

Step 5: Identification of the black hole node

Step 6: Perform Hybrid optimization approach using PSO and firefly and mitigate the effect of attack in the network

Step 7: Performance evalautions in terms of the energy consumption, throughput, packet deliveries to increase the lifespan of the network.

The result explanation of the proposed approach is discussed below:

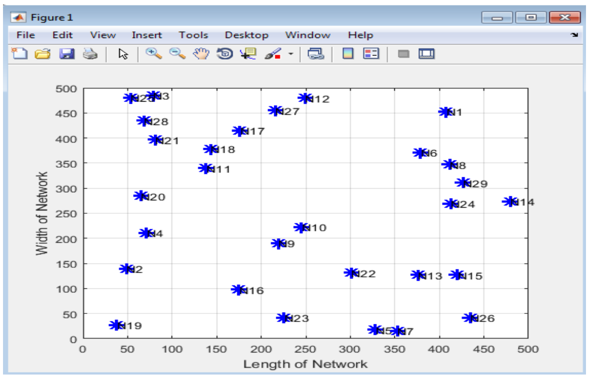

Fig. 2: Network Creation

Figure 2, deals with the network creation in which the nodes are deployed in the network with their ids as shown in the figure. The nodes are deployed using evaluation of x and y locations which will further work as a processing unit

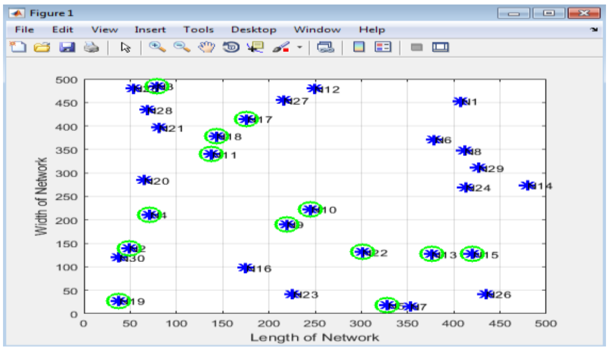

Fig. 3: Nodes with maximum energies

The figure 3 shows the nodes which are marked in the green are the nodes having maximum energy than the average energy and shows that these nodes are having high probability to perform better in the further routing process

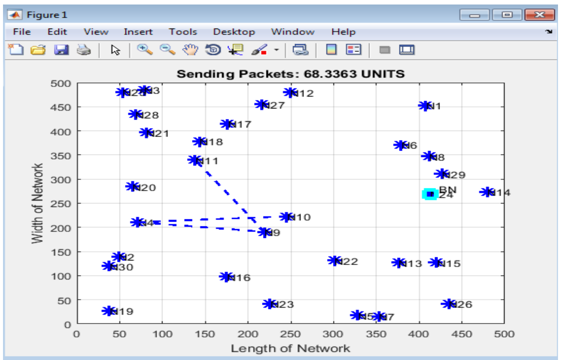

Fig. 4: Routing through fake route

The figure 4, shows the routing nodes which fake nodes are obtained by the intruder in the network and shows that the packets are transferring through the fake route in the network from the source node to the destination node

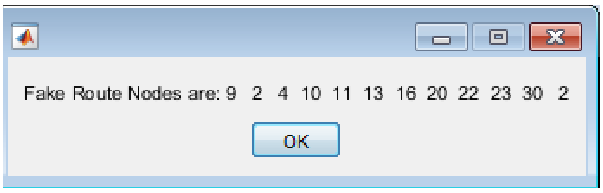
Fake Route Nodes are: 9 2 4 10 11 13 16 20 22 23 30 2

Fig. 5: Fake route node ids

The figure 5, shows the fake route node ids which are shown in the network through which the packets are transferring from source to the destination. The source node is 9th node and the destination node is 2nd node.

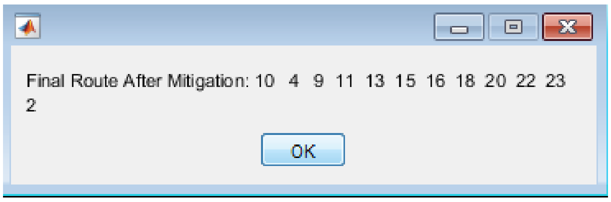
Final Route After Mitigation: 10 4 9 11 13 15 16 18 20 22 23
2

Fig. 6: Final Route

The figure 6 shows the final route nodes which are shown in the message box after the mitigation. The nodes are obtained after the optimization process through which the route packets will be sending with less packet drop probability and less error rates

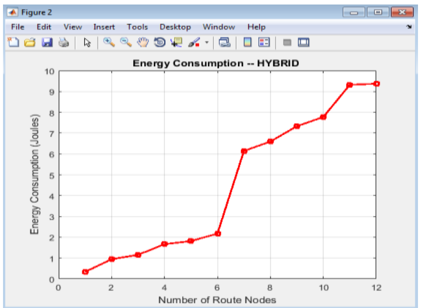

Fig. 7: Energy Consumption

The figure 7 shows the energy consumption of the network which shows that the route nodes are taking that much of energy consumption to successfully transmit the packets from source to the destination and shows that the proposed hybrid approach is able to achieve less energy consumption for achieving high accuracy and less packet drop probabilities.

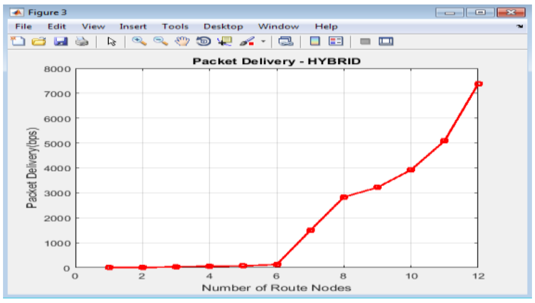

Fig. 8: Packet delivery rate

The figure 8 shows the packet delivery rate in a successful manner in bits per second and shows that the proposed approach is able to achieve high packet deliveries with less error probabilities of packet drops with less energy consumptions. The packet delivery must be high to increase the lifetime of the network

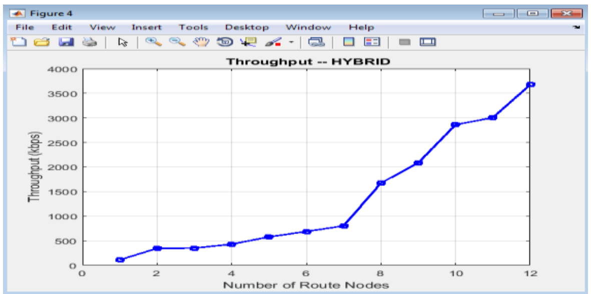

Fig. 9: Throughput (Kbps)

The figure 9 shows the throughput of the network and shows that throughput of the proposed approach is high which shows that the overall performance of the network increases with low overhead and shows that the mitigation of the attack decreases with the use of hybrid approach.

TABLE I. Proposed Approach Table Performance

Parameter	Proposed
Throughput	3600 Kbps
Packet delivery	7500 bps
Energy Consumption	9.5 Joules

TABLE II. Performance Comparison

Parameter	Base	Proposed
Throughput	300 Kbps	3600 Kbps
Packet delivery	6600 bps	7500 bps

VI. CONCLUSION & FUTURE WORK

MANET is a collection of wireless hosts that can be rapidly deployed as a multi-hop packet radio network without the aid of any established infrastructure or centralized administrator. Such networks can be used to enable next generation battlefield applications, including situation awareness systems for maneuvering war fighters, and remotely deployed unmanned micro-sensor networks. MANETs have some special characteristic features such as unreliable wireless media (links) used for communication between hosts, constantly changing network topologies and memberships, limited bandwidth, battery, lifetime, and computation power of nodes etc. While these characteristics are essential for the flexibility of MANETs, they introduce specific security concerns that are absent or less severe in wired networks. MANETs are vulnerable to various types of attacks. MANET is vulnerable to various types of attacks. One such serious security problem in MANETs is - Black Hole attack. It is an attack where a malicious node sends a forged or fake RREP (route reply) to source node and initiates route discovery and prevent the data traffic from the source node. We proposed an effective and efficient routing against black hole attack. The proposed method adds a negligible overhead as single bit used to confirm the legitimacy of route. Proposed method is adjustable with other on–demand routing protocols. The research work has evaluated the performance of the system present in the attack. For the purpose, we have implemented hybrid routing optimization approach (PSO + Firefly) to mitigate the effect of attack and evaluated the performance in terms of energy consumption, routing overhead and throughput to increase the lifespan of the network.

Future scope

MANET is vulnerable to various types of attacks. The Major issues on the MANETs are - Black Hole attack. It is an attack where a malicious node sends a forged or fake RREP (route reply) to source node and initiates route discovery and prevent the data traffic from the source node. As a future scope of work, the proposed security mechanism may be extended so that it can defend against other attacks like resource consumption attack and packet dropping attack. Adapting the protocol for efficiently defending against gray hole attack- an attack where some nodes switch their states from black hole to honest intermittently and vice versa. In future we also can make effective optimization algorithm to reduce the effect of black hole attack in MANET.

VII. References

[1] K. Shobina, N.M. Prabhu, ”Modified AODV routing protocol to detect and avoid the black hole attack in MANET” in International journal of innovative research in science, engineering and technology, vol. 6, pp. 2319-8753, February 2017.

[2] K.M.Kumari, S.Samreen,” Secure and Reliable Black Hole detection Attack and to increase the Network Lifetime in Wireless Sensor Networks,” International Journal of Innovative Research in Science, engineering and Technoogy,Vol.6, August 2017.

[3] A.P.Reddy, N.Satyanarayana,” Energy Efficient Stable Multi Path Routing in MANET,” In proceedings of Springer, 2016.

[4] S.R. Deshmukh,P N Chatur,N.B.Bhople,”AODV-based secure routing against blackhole attack in MANET,” proceedings of IEEE, 2016.

[5] P.Khemariya,U.K.Purohit,U.Barahdiya,”Performace study of Improved AODV against Black Hole Attack in wireless Environment, “international Journal of Engineering Research and Modern education, Vol.1, 2016

[6] S.Shrivastava,C.Agrawal, A.jain,”An IDS scheme against Black Hole Attack to Secure AOMDV Routing in MANET,” International Journal on Ad Hoc Networking Systems (IJANS) Vol. 5, January 2015

[7] A.Nakum, J.H.Joshi,”An Enhance Approach to Mitigate the Impact of Black Hole and Gray Hole Attacks in AODV Routing Protocol,” International Journal of Innovative Research in Computer and Communication Engineering, Vol.4,April 2016.

[8] M.Puray,P.Palod,” Black Hole Attack in MANET:A Study” International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Vol 5, March 2016.

[9] A.Aldaej, T.Ahamad,” AAODV (Aggrandized Ad Hoc on Demand Vector): A Detection and Prevention technique for MANETS,” International Journal of Advanced Research in Computer Science and Applications, Vol 7, 2016

[10] H.Gupta,H.Aggarwal, ”Simulation to Detect and Removal of Black Hole in MANET” International Journal of Electronics and Communication Engineering (SSRG-IJECE) , April 2015.

[11] K.Kamboj,V.Singla,” Secure AOMDV Protocol in MANET,” International journal of Emerging Research in Management and Technology, Vol.4, July 2015.

[12] T.M.Mahmoud, A.A.Aly, O.M.M,” A Modified AODV Routing Protocol to Avoid Black Hole Attack in MANETS,” International Journal of Computer application, Vol.109, January 2015,

[13] N.Gupta,K.Kishore,”An implementation of secure Wireless Network for avoiding Black hole attack,” International Journal of Computer applications, Vol.112, February 2015.

[14] Monika, S. Gupta, ”Detection Prevention of Black Hole and Gray Hole Attack in MANET using digital signature techniques,” International Journal of Engineering and Computer Science Vol.4, pp. 13268-13272, 2015.

[15] S.Behzad, R.Fotohi, F.Dadgar,” Defense against the Attacks of the Black Hole, Gray Hole and Wormhole in MANETs Based on RTT and PFT,” International Journal of Computer Science and network Solutions.Vol.3, March2015.

[16] S.Sharma, U.K.Singh,K.C.Phuleriya, D.N.Goswami,” SCAODV: A protocol To Prevent Black Hole Attacks in Mobile Ad Hoc Networks,” International Journal of Computer Science and Communication, Vol.6, April-Sept 2015.

[17] T.Nandhini, V, Sandhya, R, Kundhavai, ”Detection of Grouped Malicious Nodes to Avoid Black Hole Attack in Mobile Ad-Hoc Network,” International Journal for Innovative Research in science and Technology, Vol.1, Dec 2014.

[18] G. Wahane, A.Kanthe,”Technique for detection of Cooperative Black Hole attack in MANET” IOSR journal of computer science, pp. 59-67, 2013.

[19] Jyoti, R.Kushwah,” Performance Analysis of Black Hole attack in MANET,” International Journal of Computer Science and Information Technologies, Vol. 5 pp. 5225-5230 , 2014.

[20] D.Geetha, B. Revathi,”AOMDV Rountingh Based Enhanced Security for Black hole attack in MANETs,” in International conference on research Trends in Computer Technologies,2013.

[21] J.Kumar, M.Kulkarni,D.Gupta ,”Effect of Black Hole Attack on MANET Routing Protocols,” I. J. Computer Network and Information Security,Vol.5, pp. 64-72, April 2013.

[22] R. Kesavan, V.T Bai,”Avoidance of Black Hole Attack in Virtual Infrastructure for MANET,”in Internatuional journal of Computer Applications, Vol.50, July 2012.

[23] S. Agrawal, S. Jaiswal, Study to Eliminate Threat of Black Hole of Network Worms in MANET International Journal of Scientific and Research Publications, Volume 2, September 2012.

Neha Kohli obtained her Bachelor of Technology degree in Computer Science and Engineering from Swami Parmanand College of Engineeering, Punjab Technical University, Kapurthala. Her research interest include MANET.