A Hybrid and Secure Clustering Technique for Isolation of Black hole Attack in MANET

VeerpalKaur
M.tech. Research Scholar (Computer Science &Engg.)
Punjabi University Guru Kashi Campus, Talwandi Sabo, Bathinda, Punjab, India.

Simpel Rani
Associate Professor (Computer Science &Engg.), Yadavindra College of Engineering,
Punjabi University Guru Kashi Campus, TalwandiSabo,Bathinda, Punjab, India.

ABSTRACT-A mobile ad hoc network (MANET) is a collection of independent nodes that communicate with each other through a multi-hop radio network and keep up connections in a decentralized manner. Security remains a major challenge for thesetypes of networks due to their features of open medium, dynamically change in topologies, reliance on cooperative algorithms, absence of centralized monitoring points, and lack of clear lines of defense. Most of the routing protocols for MANETs are thus vulnerable to many types of attacks. Ad hoc on-demand distance vector routing (AODV) is a very efficient routing algorithm. However, it is insecure to the well-known black hole attack, where a malicious node falsely claims that have a best path to a destination node during the route discovery process. This attack becomes more serious when more than one malicious nodes present within network, called multiple black hole attack. In this paper, a defense mechanism hybrid and clustering is presented against to multiple black hole nodes in a MANET.The exploratory results will show that proposed strategy detects and isolate the malicious nodes from the network proficiently. It will enhance network effectiveness as far as expand throughput, reduce the packet loss and delay of the network. The NS-2.33 simulator instrument will be utilized as a part of it.

Keywords- Mobile ad-hoc network (MANET), Blackhole Attack, Malicious node, Routing protocols, clustering.

1. INTRODUCTION

The type of network that provides communication across various devices without the need of any a wire within it is known as a wireless network. There is a requirement of radio waves and microwaves for providing communication within the devices which present within the wireless networks. Wireless networks classify in to two types one is Infrastructure networks and another is infrastructure-less or Ad-Hoc networks.In infrastructure networks used a central controller which is also known as access point (AP). The communication between all the nodes is done through the access point. Which networks that do not have any central controller or access point for communication is called the infrastructure-less networks. Mobile ad-hoc networks are self-configuring and infrastructure less in nature. With the help of wireless links, the different mobiles are connected with each other. There is a limited bandwidth and node mobility of the mobile ad hoc networks. Thus, the various factors like as energy efficiency of the nodes, topology changes and unreliable communication are to be considered and analyzed in a proper manner within the network [1] [17].

The transformation of data from source to destination is done with the help of routing protocols. Routing protocols classify in to three categories, Reactive, Proactive and Hybrid protocols. In Reactive Protocols there is a route established from source to destination as per the need. The various reactive routing protocols are AODV (Ad-hoc On Demand Distance Vector), DSR (Dynamic Source Routing) etc.In proactive routing protocols route is predefine between the source and destination within a network. A routing table is maintained by each node which present within the network. There are various proactive routing protocols like as DSDV (Destination Sequence Distance Vector) etc. The hybrid routing protocol is the type of protocol that is combination of proactive and reactive routing protocols. The example of hybrid type of routing protocol is the ZRP (Zone Routing Protocol).Security is main concern in all types of communication networks, But ad-hoc networks face the major challenge due to their infrastructure-less and independent nature [1] [4] [16].

1.1 AODV Routing Protocol

In AODV protocol route is established from source to destination as per the demand of the network. As shown in figure 1 the three control messages are present within this protocol which is the route request (RREQ), route reply (RREP) and the route error (RERR) [29].In case where is a requirement to establish a route to destination node, the route request packets are sent by the source node in initially to the nearby nodes.The adjacent node replies back to the source node with the route reply message when there is a path available from source to destination across it.

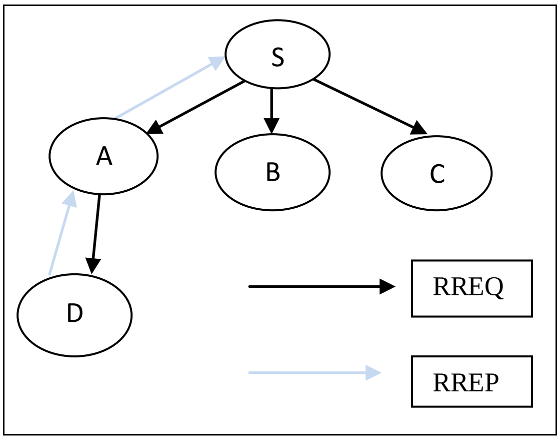


Fig 1:General Working ofAODV protocol

The best path is choosing within the network on the basis of the minimum hop counts and maximum sequence number within the network. The sequence number is also a very important factor for selecting the appropriate path.

1.2Attacks in Mobile Ad-hoc Networks:

There are two important concepts in MANET security: security services and various Attacks.Security Services refer to procedures that make a network more secure. where attacks are use weaknesses of network to break the security of services, some serious attacks in MANETs are like Black hole attack, Worm hole attack, Routing attack, Eavesdropping attack, Man in Middle attack, Denial of service, Jamming attack etc [6].

a). Routing Attacks: The most commonly attacks found in the mobile ad hoc networks are the routing attacks. The attacks trigger within the network due to the presence of the malicious nodes. The traffic of the network can be routed to other nodes when routing attack is trigger. The destination node is free here [5].

b). Eavesdropping Attack: A passive type of attack in which the malicious nodes detect within the traffic of network is known as eavesdropping. The attacker collects the secret information such as the passwords or private keys from the network.

The permanence of active attacks can be caused due to the presence of passive attacks [5], [6].

c). Black hole Attack: In a black hole attack a malicious node attract the data packets by declare a falsely, fresh path to reach destination. But it absorbs the data packets and not forward packets to destination. In cooperative black hole attack malicious nodes work together in a team [4].

d). Wormhole attack: This type of attack can be occur within or outside the network by the malicious node is known as a wormhole attack. In wormhole attack packets are received from the one end of the network and the rest of the traffic is sent to another side. There is delay of other services within the network when the wormhole attack is occurring [4].

e). Jamming Attack: An active type of attack in which abundant packets are sent to specific node by the malicious nodes is known as jamming attack. Such abundant packets are not capable to be handled by the node. The network will be blocked in such type of condition [4], [5].

f). Man-in-the-Middle Attack: When the two parties that is exchanging information between each other, and the third party (attacker) lies between them this type of attack is called the man-in-middle attack. Any information being exchanged amongst them can be detected by the attacker. There is a need to get hold on the information being transferred between two parties. There might be many other attacks occurring possibility increase within the network in this attack scene after the information is extracted once [7].

g). Denial-of-Service Attack: The required services cannot be accessed by the legal nodes in the denial-of-service attack. The Large no. of burst packets is sent with respect to the legal nodes in this scenario by showing illegal sources as legal ones. The services are disturbed due to the overcrowding within the network. The network performance measurement parameters such as throughput and bandwidth get decreases which degrade the overall performance of the network [6], [7].

1.3 Black Hole Attack in AODV protocol

In a black hole attack a malicious node attract the data packets by falsely claim, it have a fresh path to reach destination [8, 9]. But it absorbs the data packets and not forwards them to destination [1].Here an example, which shows a fired black hole attack within a network, is shown in Figure 2. Where S is a source node and D is a destination node, Nodes 1,2,3,4 and 5 are act as the intermediate nodes and 4(B1) and 5(B2) Nodes are act as malicious nodes. When source node wants to send a data packet to Destination then it send RREQ message to all neighbor nodes. Here the malicious nodes also part of the network and receives the RREQ message. Then malicious nodes immediately send the RREP message that reach at destination through B1.

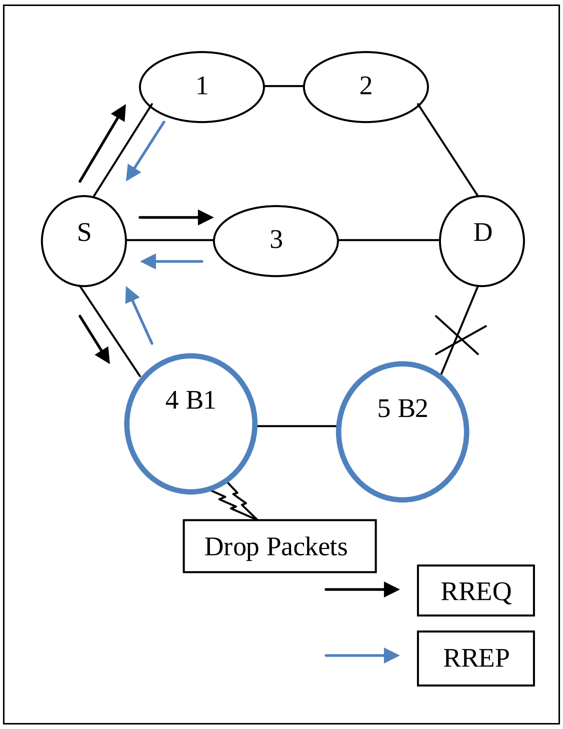


Fig 2: Black hole Attack

When source node receives the RREP starts the data packets send to B1 continously.B1 drops the data packet, instead send it to destination. Thus the data packet is absorbed and never reaches to destination. 5(B2) also react same as 4(B1),so when the malicious nodes are more than one called multiple black hole attack. When the multiple black hole attack is trigger the situation is very critical.

2. Literature Survey

Sen et al. [1] proposed a technique to detect the cooperative black hole attack in MANETs. In technique used two concepts to modify the AODV protocol. One is DRI (data routing information) table and another one is cross checking. Each node maintains a DRI table. In DRI table have information about true or false values [1]. In cross checking when source node (SN) broadcast a RREQ message to find a short and Secure path, then intermediate nodes transmits RREP to provide information about its DRI table. BY using this mechanism delivery ratio is increased 38% to 55%. Resulting an average improvement of 17%, but performance is decreased.

Ren et al. [2] described a technique to detect black hole attack by using packet exchange recording in disruption tolerant networks. In this technique, two tables RRT (receiving record table) and SRT (self-record table) used to keep the record of exchanged packets.RRT have the packet exchanged record of that node which sends the RREP and SRT have packet exchange record of that node which sends the RREQ.by using this technique detect insider attack efficiently with high detection rate and low positive rate.

Esmaili et al. [3] proposed a scheme to analysis the performance of AODV protocol by using OPNET simulator, under black hole attack. In this paper discuss two approaches to secure MANET. First is the securing ad-hoc routing by using various protocols like DSR (dynamic source routing), DSDV (destination sequence distance vector), ARAN (authenticated routing certificate process), TRP (real time transfer protocol) etc. Second one is, intrusion detection system provide a mechanism in which each intermediate node sends back the next hop information with RREP massage. By using this approaches packet delivery ratio is increased but PDR reduces the remarkably in presence of black hole attacks.

Mohite and Ragha [4] described mechanism to detect cooperative black hole attack by using cooperative security agents. In mechanism take three concepts, first is SRT and RRT Tables, second one is data routing information and third is cooperative security agents by using the combination of three methods, malicious nodes detect effectively and mitigate the negative impact caused by black hole and cooperative black hole attack.

Al-Shurman et al. [5] proposed two techniques to detect the black hole attack. First technique is based on RREP packet arrives from more than two nodes. This method is secure but longer time delay. Second technique is based on send RREP with record of Last-packet sequence numbers. Second method is fast, reliable and reduces the overhead in network. But this method is not secure because sometimes malicious node can listen to channel and Update their tables.

3. Proposed Methodology for Isolation of Multiple Black hole Attack

The wireless mobile networks is the decentralized type of network due to which malicious nodes enter the network which trigger various type of active and passive attacks. The blackhole attack is the active type of attack which is triggered by the malicious nodes. The proposed technique is based on to detect malicious nodes which are responsible to trigger blackhole attack in the network. The proposed technique consists of following steps for the detection of malicious nodes:-

STEP1: In the initial step, the route request packets are flooded by the source node within the network. For checking the time taken for receiving the route reply packets, the timer is initiated by the source node.

STEP2: Each route reply packet is checked by the source. The node that responds in least time duration and has the highest sequence number is checked and selected.

STEP3: The node that responds in least time duration and has exceptionally high sequence number is black listed.

STEP4: The number of packets re-transmitted by individual node is checked by the source node.

STEP5: For each node present within the network, rating is assigned and the node that has highest trust values is chosen to the most trusted or legitimate node.

STEP6: Within the network various clusters are generated. The node that has highest trust value is selected as cluster head. Through the cluster heads, all the network data is transmitted.

4. Algorithm for Proposed Technique

To overcome the problematic issue of black hole attack in mobile ad-hoc networks, a new algorithm has to be implemented using ns-2.35 tool. Its details steps are given below:

i).First Phase: In the first phase, the network is deployed with the finite number of mobile nodes. The malicious are defined in the network which are responsible to trigger black hole attack in the network.

ii).Second Phase: In the second phase of algorithm, the source node floods the network with the RREQ message and set the timer in which it receives route reply packets. The malicious node reply back with the route replies packets in the minimum amount of time. The source node put node id in the blacklist for isolation.

iii). Third Phase: In the last phase of the algorithm, the trust value of each node is calculated on the basis of number of packets forwarded in the network. The malicious node forward the least number of packets due to which it has least trust value. The whole network is divided into fixed size clusters based on node location. The node which has maximum trust is selected as cluster head and node which has least trust is considered as malicious and cannot be involved in the data communication within network.so it's a very

```
STEP 1: Deploy the network with finite no. Of nodes.

STEP 2:  Apply AODV protocol( )

2.1: Source set timer “t” and send route request packets in the network.

2.2: present nodes in the network respond with route reply.

STEP 3:Analyze Route Reply ( )

3.1: source node analyze route reply & check the seq no. & throughput.

3.2: if (Time & Throughput == minimum and sequence np.=maximum)

Then node enter in black list.

STEP 4: Calculate Trust( )

4.1: Check No. Of packets Retransmitted by node.

4.2: Repeat 4.1 until all nodes covered.

STEP 5: Cluster the Network

5.1: Apply location based clustering.

5.2: Node== maximum trust selected as cluster head.

STEP 6: Start communication from cluster head to cluster head.
```

efficient technique to isolate the multiple black hole attack.

5. Simulation

The Proposed scheme will be implemented by using network simulator NS-2.35.We have considered the simulation parameters as shown in the table I.

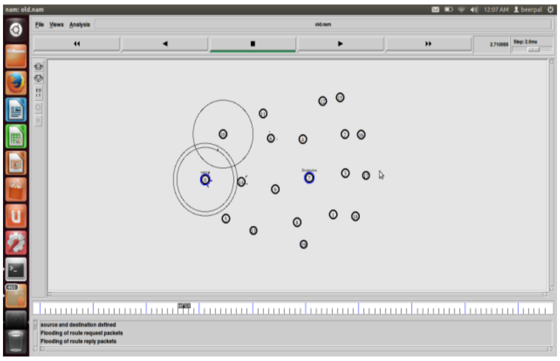
TABLE I: Simulation Parameters

Parameter	Value
Terrain Area	800 m x 800 m
Simulation Time	50 s
MAC Type	802.11
Application Traffic	CBR
Routing Protocol	AODV
Data Payload	512 Bytes/Packet
Pause Time	2.0 s
Number of Nodes	20
Number of Sources	1
No. of Adversaries	1 to 3

SNAPSHOTS:

A). MANET without Black hole Attack

In figure 3. Shows that in the network the node 0 is a source node 7 is destination. Hence the Path between source and destination is 0-14-9.

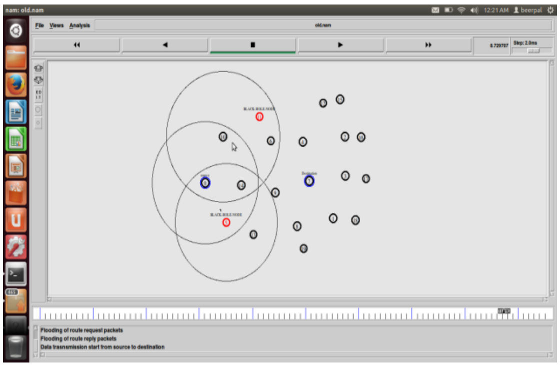


source and destination defined
Flooding of route request packets
Flooding of route reply packets

Fig 3. MANET without blackhole Attack

B). MANET with the Multiple Blackhole Attack

In figure 4 shows that nodes 5 and 11 act as a malicious nodes. Data packets are absorbed by these nodes, due to this network performance will decreased.

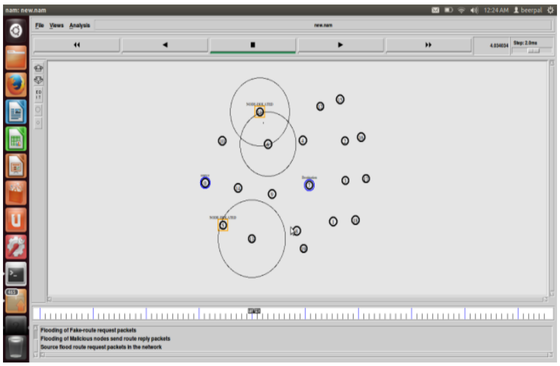


Flooding of route request packets
Flooding of route reply packets
Data trasnmission start from source to destination

Fig 4. MANET with Multiple Blackhole Attack

C). Isolation of Multiple Blackhole Attack

As shown in figure 5, the malicious nodes are isolated with our purposed technique.so that performance of the network is increased in the form of various parameters like as throughput, packet loss and delay.

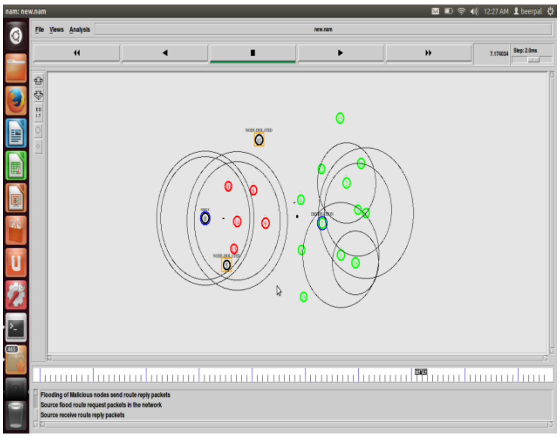


Flooding of Fake-route request packets
Flooding of Malicious nodes send route reply packets
Source flood route request packets in the network

Fig 5. Isolation of Multiple Blackhole Attack

D).Clustering of Network

As shown in the figure 6, location based clustering is performed within the network. Which nodes have the highest trust value will be chosen as the cluster head.



Flooding of Malicious nodes send route reply packets
Source flood route request packets in the network
Source receive route reply packets

Fig 6. Clustering of Network

6. Results and Discussion

- **Graphical Representation of the result of Throughput**

In the figure 7, the old throughput that is denoted by the green line and the existing throughput is shown by the red line and new throughput is shown by the blue line. The time is denoted on x-axis and number of packets on y-axis. The throughput of the new technique is higher as compared to the previous technique.

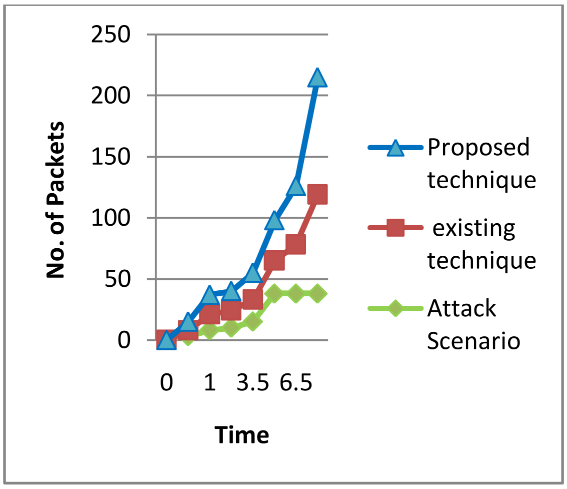


Fig 7.Throughput Graph

- **Graphical Representation of Result of Packet-loss:**

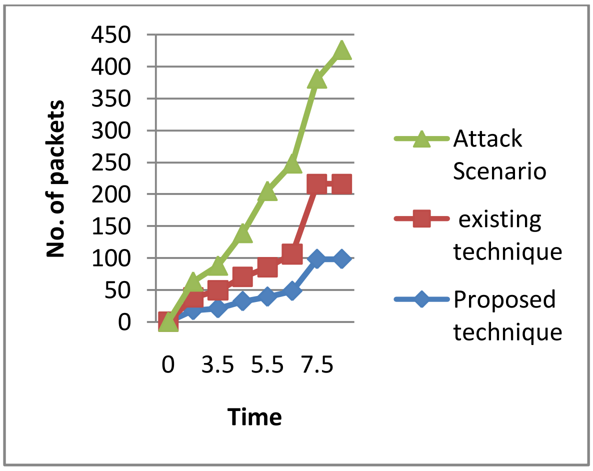


Fig 8. Packet Loss Graph

In figure 8, the packet losses in case of old with green line, existing with red line and new with blue line are shown. The time duration and the number of packets are represented on x-axis and y-axis respectively. As compared to the previous technique, there is packet loss is decrease in the new technique which shows the enhancement in the new method.

- **Graphical Representation of the Result of delay:**

In the figure 9, the earlier delay is denoted by the green line and existing delay represent by the red line and the new delay is represented by blue line. The time duration and the number of packets are represented on x-axis and y-axis respectively. The delay is reduced within the new proposed method in comparison to the earlier method. This shows improvement within the new technique.

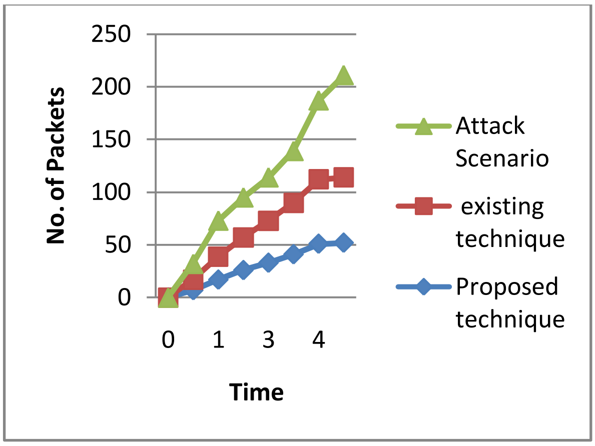


Fig 9. Delay Graph

6. Conclusion and Future Work

In this paper the routing security issues of MANETs are described. The Blackhole attack, which can easily be deployed against MANET and an efficient technique to isolate the multiple balckhole attack, is described. The proposed technique will be based on to analyze the route reply packets in which the nodes reply with the exceptional high sequence number is add into blacklist. To isolate these nodes from the network, technique of clustering will be applied this improvement leads to increase network performance.The future work may be concentrate on the proposed technique can be compared with some other technique of intrusion detection for mobile ad-hoc networks. And also the proposed technique can be applied for the detection of wormhole attack in the network. The malicious nodes which are increasing delay in the network.

References

[1] J. Sen, S. Koilakonda and A. Ukil, 2011. "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks", in Proceedings of 2nd International Conference on Intelligent Systems, Modeling and Simulation, pp. 338-343.

[2] Y. Ren, M. C. Chuah, J.Yang and Y.Chen, 2010. "Detecting Black hole Attacks in Disruption-Tolerant Networks through Packet Exchange Recording", in Proceedings of IEEE International Symposium on World of Wireless Mobile and Multimedia Networks (WoWMoM), pp. 1-6.

[3] H.A. Esmaili, M. R. KhaliliShoja, Hosseingharaee, 2011. "Performance Analysis of AODV under Black hole Attack through Use of OPNET Simulator", World of Computer Science and Information Technology Journal (WCSIT), Vol. 1,No. 2, pp. 49-52.

[4] V. Mohite and L. Ragha, 2012. "Cooperative Security Agents for MANET", IEEE World Congress on Information and Communication Technologies, pp. 549-554.

[5] M. Al-Shurman, S. Yoo and S. Park, 2004."Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, pp. 96-97.

[6] K. Osathanunkul, and N. Zhang, 2011. "A countermeasure to black hole attacks in mobile ad hoc networks", IEEE International Conference on Networking, Sensing and Control (ICNSC), pp.508-513.

[7] P. N. Raj and P.B. Swadas, 2009. "DPRAODV: A Dynamic Learning System against Black HoleAttack in AODV based MANET", IJCSI International Journal of Computer Science Issues, Vol. 2.

[8] L. Tamilselvan and V. Sankaranarayanan, 2008. "Prevention of Co-operative Black Hole Attack in MANET", Journal of Networks, Vol.3, No 5, 13-20.

[9] S. Lu, L. Li, K. Y. Lam and L. Jia, 2009."SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack", International Conference on Computational Intelligence and Security, Vol. 2, pp.421-425.

[10] H. Deng, W. Li and D. P. Agrawal, 2002."Routing security in wireless ad hoc networks", IEEE Communications Magazine, Vol.40, No.10, pp. 70- 75.

[11] R. Kaur and J. Kalra, 2014."Detection and Prevention of Black Hole Attack with Digital Signature", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.4, No. 8.

[12] A.Siddiqua, K. Sridevi and A.A.K. Mohammed, 2015. "Preventing Black Hole Attacks in MANETs Using Secure Knowledge Algorithm", In Proceedings of International Conference on Signal Processing and Communication Engineering Systems (SPACES),pp. 421-425.

[13] T.Manikandan, S.Shitharth, C.Senthikumar and C. Sebastinalbina, 2014."Removal of Selective Black Hole Attack in MANET by AODV Protocol", Vol.3, No. 3.

[14] Pradeep kyasanur, 2005. "Selfish MAC layer Misbehavior in wireless networks", IEEE on Mobile Computing.

[15] Tien-Ho Chen and Wei-Kuan, 2010. Shih, "A Robust Mutual Authentication Protocol for Wireless Sensor Networks," ETRI Journal, Volume 32, Number 5.