Exposure and Mitigation of the Gray Hole Attack from AODV in Mobile Ad hoc Network: An Approach

Ruchi Tiwari
Electronic and Communication Department
Sagar inst. of Research and Technology
Engineering R.G.P.V. Bhopal,
Madhya Pradesh, India

Jyoti Jain
Head of Department, E&C Dept.
Sagar Inst. of Research and Technology
Engineering, Bhopal,
Madhya Pradesh, India

ABSTRACT

Wireless ad hoc network is a collection of mobile nodes and all nodes behave as router or host. Due to its dynamic nature and lack of central authority security is challenging task. The nodes of network may compromise from the various security threats and can leak the personal information. Numerous security threats such as Denial of Service, black hole attack, Gray-hole attack, Worm hole, Sybil attack and jamming may be used by attacker to damage the network security. Gray hole attack is one the security threat which selectively drop the packets. In this paper, proposes an probabilistic approach with IDS (Intrusion Detection System) which detect and mitigate the gray hole attack effectively. The simulation of the propose approach is done in NS2.34 network simulation and comparative analysis is perform among the performance metrics such as Throughput, Packet Delivery Ratio and Routing load etc.

Keywords

Gray hole, Network Security, Network Simulator, PDR, Routing Load.

1. INTRODUCTION

In wireless ad hoc networks all nodes are mobile and can be connected dynamically in an arbitrary manner. As the range of each host in wireless transmission is limited, so to communicate with hosts outside its transmission range, it needs to enlist the aid of its nearby hosts in forwarding packets to the destination. So all nodes of these networks behave as routers and take part in discovery and maintenance of routes. [1]

Wireless networks use some sort of radio frequencies in air to transmit and receive data. Wireless networks are formed by routers and hosts. Basically ad-hoc networks are wireless networks in which nodes are communicated with each other using multi-hop routers. Topology in MANET are created dynamically and maintained by individual nodes comprising the network. In MANET all communication occurs through a wireless medium. MANETs also possess multi hop routing means packets are allowed to forward to the destination through multiple nodes thus each node act as terminal as well as router. Routing is an concept of transferring data from source to destination while maximizing network performance. So it becomes a challenging task in MANETs due to cause of change in topology, network density and limited resources changes paths which were initially efficient but can quickly become inefficient and infeasible.

In these networks, nodes are usually distinguished by their memory resources, limited power, processing speed as well as high degree of mobility. Due to the limited transmission range of wireless network, multiple hops are usually needed for a node to exchange information with any other node in the network.

Thus ad-hoc routing protocols play a significant role in MANET. It is usually possible to establish more than one path between a source and a destination. In an Ad Hoc networks all nodes are mobile nodes and the topology of the network is changing dynamically, which brings great challenges to the security of Ad Hoc Network.

As a result, attackers can take advantage of flaws in routing protocols to carry out various attacks. Black hole and Gray hole attacks are two severe attacks under Ad Hoc networks, which could disturb routing protocol and bring about huge damage to the network’s topology.

Gray hole attack is a certain type of Black hole attack in which a malicious node acts as a normal node for some time and later drops the packets selectively. These malicious nodes properly participate in the route discovery process, when a route is established between sender and destination node they are selectively drop the data packets from some nodes and selectively forward packets from other nodes so it will degrade the network performance and there is need to remove these gray hole nodes from the route. In this paper, mainly focus on detection and prevention of gray hole attack using probabilistic approach and the experimental analysis of this proposed approach is executed in network simulator NS-2.34 and taken comparative analysis of routing load, PDR, and throughput between normal aodv, aodv with attack and with Intrusion detection system.

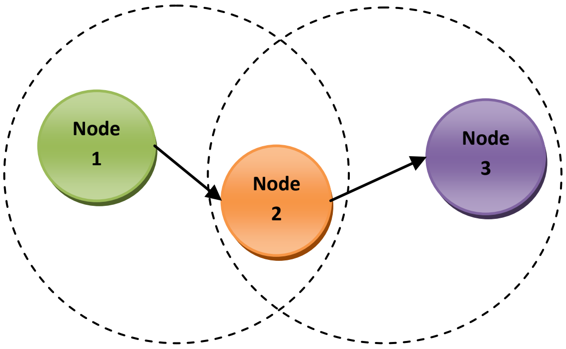

Fig.1: Architecture of Mobile ad Hoc Network

1.1 Characteristics of Wireless Ad Hoc Network

1) Distributed operation: In MANET nodes move continuously, therefore nodes must be scheduled in a distributed fashion for gaining access to the channel. This may required exchange of control information. The control of the network is distributed among the nodes; there is no background network for the central control of the network operations. The nodes involved in a MANET should cooperate with each other and communicate among themselves and , to implement specific functions such as routing and security; each node acts as a relay as needed [2][3].

2) Mobility of nodes: Nodes are mobile most of the time in wireless network. The bandwidth reservation made or control information exchange may end up being of no use if node mobility is very high. Protocol design must take this mobility factor into consideration such that the performance of the system is not significantly affected due to node mobility [3].

2) Multi hop routing: When a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes.

3) Autonomous terminal: Every mobile node is an independent node in MANET which could acts as both a host and a router.

4) Dynamic topology: In MANET nodes are free to move arbitrarily with different speeds; thus, the network topology may change randomly at unpredictable time. In MANET nodes are dynamically establish routing among themselves as they travel around, establishing their own network.

5) Light-weight terminals: In maximum cases, the nodes at MANET are mobile with less CPU capability, low power storage and small memory size.

The rest of paper organized as follow: Section 2 gives brief description about different types of attack. Section 3 describe literature study about the former work done by the different authors to evade the Gray hole attack. Section 4 proposed methodologies and its algorithm. Section 5 describe Experimental setup and result analysis. Last section concluded about the whole paper with future work.

1.2 Physical Layer Attack

Some of the attacks identified at physical layer include eavesdropping, interference, and jamming etc.

1) Eavesdropping: It can also be defined as interception and reading of messages and conversations by unintended receivers. The main goal of such type of attacks is to get the confidential information that should be kept secret during the communication.

2) Jamming: Jamming is a special class of Denial of Services attacks which are initiated by malicious node after determining the frequency of communication. It also prevents the reception of legitimate packets.

3) Active Interference: An active interference is a Denial of Service attack which blocks the wireless communication channel, or distorting communication among the nodes.

1.3 Data Link Layer Attack

The data link layer can classify attacks as follows:

1) *Selfish Misbehaviour of nodes:* The selfish nodes may refuse to take part in the forwarding process or drops the packets intentionally in order to conserve the resources and battery power.

2) Malicious Behaviour of nodes: The main task of malicious node is to disrupt normal operation of routing protocol. The impact of such attack is increased when the communication takes place between neighbouring nodes.

*3) Denial of Service (DoS)***:** A denial of service (DoS) attack is characterized by an attacker to prevent authorized users of a service from using the desired resources and attempts to “flood” a network, thereby preventing legitimate network traffic.

*4) Misdirecting traffic***:** A malicious node advertises and passes fake routing information in order to get secure data before the actual route.

*5) Attacking neighbour sensing protocols***:** To break important links interface malicious nodes generate fake error messages.

1.4 Network Layer Attack

The basic idea behind network layer attacks is to inject itself in the active path from source to destination or to absorb network traffic.

1) Black hole Attack: In this type of attacks, malicious node claims having an optimum route to the node whenever it receives RREQ packets, and sends the RREP with highest destination sequence number and minimum hop count value to original node whose RREQ packets wants to intercept.[6]

2) Gray hole Attack: Gray hole is one of the attacks found in ad hoc network which act as a slow poison in the network side it means we cannot suppose how much data can be lost. In Gray hole Attack [7] a malicious node discarded to precede certain packets and simply drops them. The attacker selectively drops the packets at beginning from a single IP address or a range of IP addresses and forwards the remaining packets. Gray hole nodes in MANETs are very effective. All node maintain a routing table that holds the next hop node information for a route to send packet from source to destination node ,when a source node want to route a packet to the destination node , it uses a particular route if such a route is available in its routing table. If not, nodes initiate a route discovery process by broadcasting Route Request (RREQ) message to its neighboring nodes. By getting the RREQ message, the intermediary nodes bring up-to-date their routing tables in a reverse route to source node. A Route Reply (RREP) message is sent backward direction of the source node after the RREQ query reaches either the objective node itself or any other intermediary node that has a recent route to destination.

The gray hole attack has two significant phases [15].

In primary phases, a malevolent node exploits the AODV protocol to proclaim itself as having a valid route to destination node, with the intension of interjecting or humiliating packets, even though route is fake.

In second phases, the malicious nodes drop the intermittent packets with a certain prospect. The process of finding gray hole is very challenging task. In certain new gray hole attacks the attacker node acts maliciously for the duration until the packets are dropped and then switch to their normal nodes behavior. By these activities it’s very challenging for the network to distinguish such kind of attack. In some cases gray hole attack is also called as node misbehaving attack. The variation of black hole attacks is the gray hole attack, in which the affected nodes drop packets selectively. Both categories of gray hole attacks look for to disturb the network without being detected by the security measures in place [16].

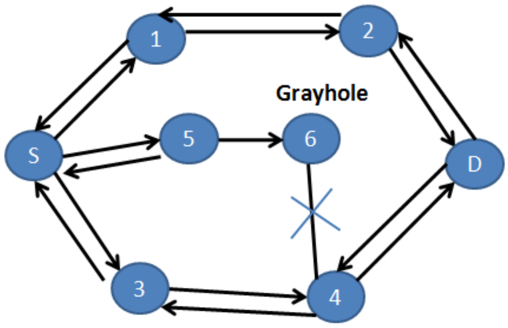

Fig. 2: Gray Hole Attack in MANET

3) Wormhole Attack:
In wormhole attack, malicious node receive data packet at one point in the network and tunnels them to another malicious node. The tunnel present between the two malicious nodes is referred to as a wormhole.

2. RELATED WORK

Most of the previous research on ad hoc networking has been done focusing only upon the efficiency of the network. A number of routing protocols proposed that are excellent in terms of efficiency. However, they were generally designed for a non-adversarial network setting that assumes a trusted environment hence there is no security mechanism has been considered. But there are more realistic setting such as a battle field or a police rescue operation in which an attacker may attempt to disrupt the communication; a secure ad hoc routing protocol is highly desirable. This section of this paper, presents the literature about the earlier work in the detection and prevention of the gray hole attack which are describing below:

Kumar & Dushan [4] proposed solution considered this deployment approach for detection and built a solution to using IDS-agent approach to detect highest sequence number node. When it detects the suspicious node, it adds it into blacklist of source node to avoid further transmission. *Rana & Mittal [5]* presented a Watchdog mechanism proposed in is a monitoring method used for wireless sensor networks, and is the basis of many misbehavior detection algorithms and trust or reputation systems. *Soliyal and Bhadauria [6]* Analyzed nature of packet dropping and bandwidth attack based on AODV routing protocol on MANET, and proposed node bypassing technique to detect gray hole attacks.

Dumne and Manjaramkar [7] Proposed a method to resolve this problem by using malicious node detection scheme based upon DSR mechanism -cooperative bait detection scheme (CBDS) which uses hybrid defense architectures. CBDS technique helps to find out malicious node by using a reverse tracing technique. *Chaudhari [12]* proposed iTrust, misbehavior detection scheme that uses a probability, for secure DTN routing towards efficient trust establishment. The basic idea of iTrust is introducing a regularly available Trusted Authority (TA) to judge the node's behavior based on the routing evidences collected and probabilistically checking. *Dhaka et al. [13]* proposed a scheme in which we are sending a control sequence to the neighbor nodes and we are expecting the nodes response. Based on the node response we can identify the malicious node. In the existing AODV Routing protocol we have been introducing two packets which are Response sequence (Rseq) packet and Code Sequence Packet (Cseq). These packets are transmitted in the AODV-MAC layer when a node wants to access the channel.

3. PROPOSED METHODLOGY

In the proposed scheme use probabilistic based rebroadcasting scheme and differ timing of re-broadcasts to keep away from redundant packets and overdoing packets transmission. In probabilistic based scheme each node forwards communication with probability *P* on receiving side at first time. When *P=1*, then it is indicating something happening wrong into the entire network. So as soon as node receiving RREQ (route request) packet, it retransmits with probability *Prt* and with probability (1-*Prt*) it disallows the packet acceptance. Retransmit RREQ packet occurs only once, which is identifies through sequence number. So by means of evasion, source node *Prt* is set to 1, to initialize RREQ.

Additionally in proposed approach set IDS node that observe the neighbors node furthermore if IDS gets any discarded inactivity in close proximity range so continue observe the meticulous node and if aggressor node receive packets excluding not forward, consequently that node set as attacker and it gets to be blocked, an additional mania is if several node continues throwing the routing packet to the particular node, then it will also treated as attacker node, then it will be also blocked in to entire network. Later than the successfully blocking it changes the entire route moreover starts sending data to the destination node. While the transmission of packets they also observe the performance of PDR, if it gets decreases at any time moment then it should be go to the observation period until not identified the reason of that.

3.1 Proposed Algorithm

For the simulation of our proposed methodology on Network Simulator-2 consider variables as Total number of mobile nodes, sender node, receiver node, gray hole node, simulation time, radio range etc.

```
Set mobile node = node    //Total Mobile Nodes
Set Sender node = S
Set Receiver Node = R
Set Routing Protocol =AODV
Start simulation time = $t_0$
Set radio range = rr;    //initialize radio range
```

To initialize RREQ in AODV set variable probability Prt, Sender node S, Receiver node R, Radio Range rr.

AODV-RREQ_B(Prt, S, R, rr)
Check there is need for retransmit packet or not if Ret(i)= 0, it means node doesn't accept the retransmit Request.

For the simulation here we choose 550 meter radio range of communication.

If those nodes exits out of this range, cannot be communicated with them and Destination is unreachable.

To transmit the packets from source to destination generate packets sequence numbers. Each packet has a particular sequence number and transmitted randomly

```
{
        If IRet(i) = 0 Then
        {
Node is not authorized for   retransmitting request for while
                Set IRet (i) = 0;

                If rr>550
                Destination is unreachable
        }

        Pkt_rndno= rnd()
```

```
            {
Generate random sequence number
            }
}
```

For the route discovery process each node maintain its routing table in which exist the information about total number of hop count ,next hope sequence number, source and destination IP addresses and their sequence number.

Initially for finding route source node broadcast the RREQ message to nearest node to establish connection from source to destination and forwarded hop by hop until it reaches at destination node. If the current node is destination node send acknowledgement to source node to permit the route setup then data can be send through this route.

If destination is unreachable change the packet sequence number.

```
TravesreRoute ()
                        {
rtable->insert(rtable->rt_nexthop); // nexthop to RREQ source
rtable1->insert(rtable1->rt_nexthop); // nexthop to RREQ destination
if (dest = true)
{
Send ack to source node with rtable1;
Data_packet_send(s_no, nexthop, type)
            }
Else
{
Destination node is unreachable;

Pkt_rndno= rnd() //change packet sequence no

                                    }
                        }
```

If the retransmission Probability is greater than or equal to the*1-Prt* retransmit the route request again and set IRet(i) = 1. Then again send route request RREQ from source, update its routing table, update the node retransmission index.

If the retransmission Probability is less than the *1-Prt* packet sequence number, no need to retransmit the route request and drop the current packet.

```
            If (1-Prt <=Prt)
            Then Retransmit request again
           And
         Set IRet (i) = 1;
            {
rtable->insert(rtable->rt_nexthop); // nexthop to RREQ source
rtable1->insert(rtable1->rt_nexthop); // nexthop to RREQ destination

//Update routing table also
Update the node retransmission index IRet (i) by 1
             }
Else
Drop the current pkt
            End if
End if

}
```

Check the any suspicious activity occurs in the route; detect any gray hole present in the route.

For this continuously check the packet delivery ratio (PDR) of path, total broadcast messages and total received messages.

Calculate time between message sent time and message received time, count total send messages.

If PDR < 60 then this is not our acceptable limit and black that node.

If PDR > 60 and increasing continuously means there is a valid path for communication and nodes accepts the packets.

If PDR decreasing from this limit again route discovery process will starts for valid path.

```
If PDR < 60

                        {
Node is blacklisted node
RREQ_Blocked()
                        }
If (PDR >60.00) Then //and increasing continuously
            {
Valid path
And accepts packets
        }
            Else
{
Start Discovery of new path
}
                }
```

5. EXPERIMENTAL RESULTS

The simulation of the proposed methodology is done using the well known network simulator NS-2.34. It is an open-source object-oriented discrete-event simulator for network research. The simulator is written in C++, with an OTcl (Object Tool Command Language) interpreter used as the command interface. The C++ part constitutes the core of the simulator, where detailed protocol implementation and the simulation engine are located.

5.1 Scenario Setup

The implementation of an algorithm is done in well known network simulator NS-2.34 [13]. The simulation environment is setup to simulate the algorithm in which we take an area of 900x900 to transmit the packet TCP/FTP, UDP/CBR protocol AODV is used and the channel wireless operation mode 802.11, mobility model random waypoint with least frequency 50 Hz is used for the simulation time period of 200 sec. In this work, mainly focuses for providing better security by consuming less energy. The comparison of above is done using different parameter such packet delivery ratio, throughput, routing load, delay etc. The simulation parameters are shown in table 1.

Table 1: Simulation Setup

Parameter	**Value**
Area	900x900
Nodes	30
Packet	TCP/FTP,UDP/CBR
Channel wireless	802.11
Mobility model	Random Waypoint
Simulation Time	200
Protocol	AODV
Least Frequency	50 Hz

5.2 Performance Metrics

The performance of the ad hoc network can be measured by using different parameter such as Throughput, Packet delivery ratio, routing load.

1. Packet delivery ratio

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources.

2. Throughput:

Throughput is the aggregate number of data packets that are delivered at the destination node with in a time‘t’. It is also average rate of successful message delivery over a communication channel.

3. Routing Load:

It is the number of routing packets transmitted per data packet sent to the destination node. Also each forwarded packet is counted as one transmission.

We have simulated the network using AODV routing protocol. It shows the performance in terms of packet delivery ratio in which the method gives better result than the existing method. The analysis is done by varying the simulation time of the nodes and PDR.

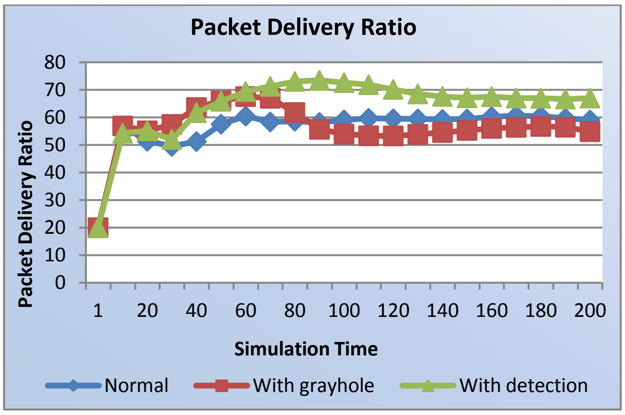

Fig.3: Comparison of simulation time Vs PDR% with existing and proposed methodology

Next performance metric is throughput used for analyzing the proposed work performance and to enhance the throughput of the network. It is found that our method gives better throughput result by varying the simulation time.

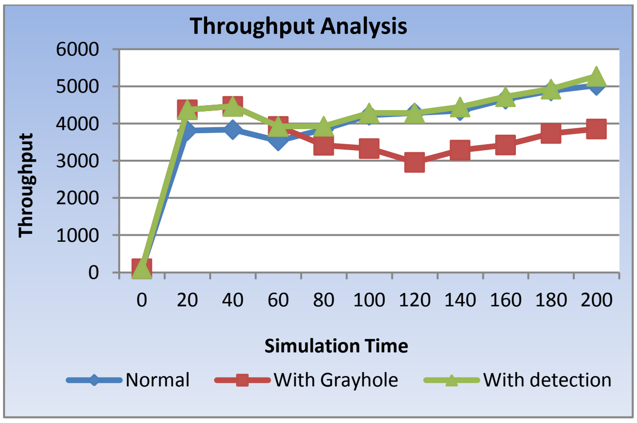

Fig.4: Comparison of simulation time Vs Throughput with existing and proposed methodology

The normalized routing load of the existing and proposed methodology differs as we increase the simulation time. The routing load of any network must be high and find that the existing method has more routing load than the proposed methodology which as shown in fig. 5.

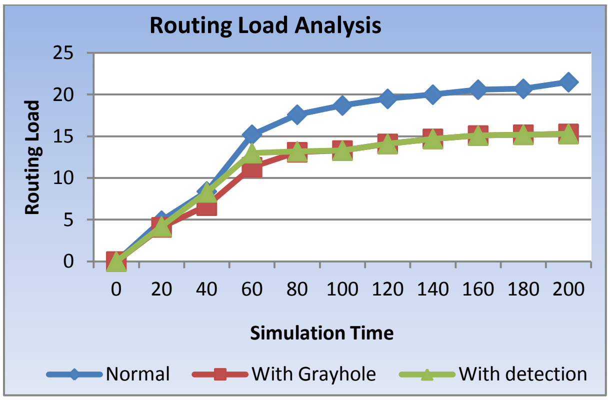

Fig.5: Comparison of simulation time Vs Routing Load with existing and proposed methodology

6. CONCLUSION

Security issues are major challenging task in wireless ad hoc network. It has been overlooked while designing routing protocols for ad-hoc networks. AODV is susceptible to many attacks including Gray hole and Black hole attacks. The main goal of proposed work to show the performance of AODV under normal surroundings, under gray hole attack and performance after elimination of gray hole attack in term of Packet Delivery Ratio, throughput and Routing load. In this work investigated some of the existing solutions for these attacks and proposed a probabilistic based approach and Intrusion Detection System to counter these attacks that efficiently finds short and secure route to the destination. The experimental analysis shows that our approach would greatly increase PDR and throughput with negligible difference in routing load. Concept has shown improved results after elimination of the gray-hole attack in the simulation. Elimination of malicious nodes takes place on Network layer by broadcasting the information of malicious nodes. Overall, elimination of gray hole attack has been done so that ad-hoc communication can be normalized as normal communication. For saving a lot of resources it will be very helpful for mobile ad-hoc communication as we have used uncasting process instead of broadcasting which saves resources as malevolent nodes are only detected through partial multicasting process The algorithm is equally applicable to other reactive protocols.

7. FUTURE SCOPE OF WORK

In this work can enhance other performance metrics like end to end delay, false positive rate and energy efficiency etc..This methodology can also be proposed for other reactive and proactive protocol. In future will enhance every layer misbehavior detection and transmission rate of metrics and can be compare with the all Protocols. Also update IDS module and 100% recovery procedure done. It can also apply the other techniques like changing source and destination addresses, packet capturing and false route forwarding, etc.

8. REFERENCES

[1] V. Dharman, G. Venkatachalam " Detection of Gray Hole Attack in AODV for MANETs by using Secure Message Digest", South Asian Journal of Engineering and Technology Vol.2, No.17 321–329 (2016).

[2] Aarti, S. S. Tyagi "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering May - 2013.

[3] Jyoti Jain, Mehajabeen Fatima, Dr. Roopam Gupta, Dr..K.Bandhopadhyay "OVERVIEW AND CHALLENGES OF ROUTING PROTOCOL AND MAC LAYER IN MOBILE AD-HOC NETWORK" Journal of Theoretical and Applied Information Technology 2005 - 2009 JATIT.

[4] Sudheer Kumar, Nitika Vats Dushan "A Modified Approach for Recognition and Eradication of Extenuation of Gray-Hole Attack in MANET using AODV Routing Protocol", Symposium on Colossal Data Analysis and Networking (CDAN), in proceeding of IEEE 2016.

[5] Ankita Rana, Er. Ankita Mittal "A Mechanism For Detection and Prevention of Multiple Gray Hole Attack In Wireless Sensor Networks", IJARIIE Vol-2 Issue-1, ISSN (O)-2395-4396 2016.

[6] Neema Soliyal, H. S. Bhadauria "Preventing Packet Dropping Attack on AODV Based Routing in Mobile Ad-Hoc MANET", Intl. Conference on Advances in Computing, Communications and Informatics (ICACCI), Sept. 21-24, Jaipur, India. Pradeep R. Dumne, Arati Manjaramkar "Cooperative Bait Detection Scheme to prevent proceeding of IEEE 2016.

[7] S. Corson and J. Macker, RFC 2501, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," Jan. 1999.

[8] C. Suhashini, S. Sivakumar "A Secure Approach with Physical Layer Encryption in MANET", International Journal of Innovative Research in Science, Engineering and Technology, ISSN ONLINE(2319-8753) PRINT(2347-6710).

[9] R. Divya Paramesvaran, Dr. D. Maheswari "Study of Various Security Attacks in Network Layer and the Mitigation Techniques for MANET", International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 2, February 2016. ISSN (Online) 2278-1021.

[10] A.Saini, R. Sharma, "A Study of various Security Attacks & their countermeasures in MANET" IJARCSSE, vol.1, Issue.1, Dec 2011.

[11] Dhamande C.S and Deshmukh H.R "A Competent to diminish the brunt of gay hole attack in MANET" Vol.2, Issue 2 Mar 2012.

[12] Yogita Avinash Chaudhari "A Probabilistic Black hole & gray hole attack Detection Scheme towards Efficient Trust Establishment in Delay-tolerant Networks-Review", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 2, February 2017.

[13] Arvind Dhaka, Amita Nandal and Raghuveer S. Dhaka "Gray and Black Hole Attack Identification using Control Packets in MANETs", Eleventh International Multi-Conference on Information Processing, Procedia Computer Science 2015.

[14] V. Solomon Abel, "Survey of Attacks on Mobile Ad-Hoc Network" IJCSE, Vol.3, No.2, Feb 2011.

[15] Vishnu K, and Amos J .Paul," Detection & Removal of cooperative Black/Gray hole attack in Mobile ADHOC Networks." International Journal of Computer Applications 2010, Volume 1-No.22, pp.38-42.

[16] Sukla and Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Proceedings of the World Congress on Engineering and Computer Science WCECS, October 22-24,San Francisco, USA 2008.

[17] Oscar F. Gonzalez, God win Ansa, Michael Howarth and George Pavlou. "Detection and Accusation of Packet Forwarding Misbehaviour in Mobile Ad-Hoc networks", Journal of Internet Engineering, 2:1, 2008.

[18] Jiwen CAI, Jialin CHEN, Zhiyang WANG, Ning LIU, "An Adaptive Approach to Detecti Black and Gray Hole Attacks in Ad Hoc Network", IEEE International Conference on Advanced Networking and Applications,2010.

[19] Chundong She 1, Ping Yi 2, Junfeng Wang3, Hongshen Yang4 "Intrusion Detection for Black Hole and Gray Hole in MANETs"KSII Transactions on Internet and Information Systems Vol. 7, no. 7, jul. 2013

[20] V.Dharman, G. Venkatachalam "Detection of Gray Hole Attack in AODV for MANETs by using Secure Message Digest", South Asian Journal of Engineering and Technology Vol.2, No.17 321–329, ISSN No: 2454-9614 2016.

[21] Hizbullah Khattak, Nizamuddin "A Hybrid Approach for Preventing Black and Gray Hole Attacks in MANET", In proceeding of IEEE-2013.

[22] Hiremani. Vani A, Jadhao. Manisha Madhukar, "Eliminating Co-operative Blackhole and Grayhole Attacks Using Modified EDRI Table in MANET", IEEE, 2013.

[23] Merkle, R. C. (1988). "A Digital Signature Based on a Conventional Encryption Function"."Advances in Cryptology CRYPTO '87 ". Lecture Notes in Computer Science 293. p. 369. doi: 10.1007/3-540-48184-2_32. ISBN 978-3-540-18796-7, 1988.

[24] Doori. Ali, Mohammad Karimizadeh Takabi. Tahereh, "Black hole attack analysis and network discovery in MANET ", Regional Conference on Electrical and Computer Engineering methods of calculation software, Islamic Azad University Safashahr, February (in persian) 2014.