Review of Defense Mechanism against Gray Hole and Black Hole Attack in MANETs

Deepali Raut [1], K .N. Hande [2]
PG Student, Dept of CSE, P .B .C. E, Nagpur, India [1]
Assistant Professor, Dept of CSE, P.B.C.E, Nagpur, India [2]

Abstract

The Mobile ad-hoc network (MANET) has got tremendous success and attention due to its self maintenance and self configuration properties or behavior. Mobile nodes communicate with each other using routing protocols. The dynamic topology of the network and absence of central base station makes MANETs vulnerable to various security attacks. These attacks are launched by participating malicious nodes against different network services. Black hole attack is one of the severe security threats in mobile ad-hoc networks which can be easily employed by exploiting vulnerability of on-demand routing protocols such as DSR. Many detection algorithms are available but most of them are suffers from a high false probability under high network overload. In this paper, a review on different existing techniques for detection black and Gray hole attacks with their defects are presented.

Index term- Mobile Ad Hoc Network, Black Hole Attack, Gray Hole Attack, DSR

1. Introduction

Mobile Ad hoc Networks (MANETS) are transient networks of mobile nodes, connected through wireless links, without any fixed infrastructure or central management. Due to the self-configuring nature of these networks, the topology is highly dynamic. Most important networking operations include routing and network management [1]. Routing protocols can be divided into proactive, reactive and hybrid protocols, depending on the routing topology. Proactive protocols are typically table driven. In these types of routing protocols, each node maintains a table of routes to all destination nodes in the network at all times. This requires periodic exchange of control messages between nodes. Examples of this type include DSDV, WRP. Reactive or source-initiated on-demand protocols, in contrary, do not periodically update the routing information. It is propagated to the nodes only when necessary. Example of this type includes DSR, AODV and ABR. Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes TORA, ZRP. Security is a major concern in all forms of communication networks, but ad hoc networks face the greatest challenge due to their inherent nature. As a result, there exist a slew of attacks that can be performed on an Ad hoc network. [2]. In Snooping the nodes misuse the inherent trust between nodes to obtain packet payload data and routing information. Flood storm attacks where malicious nodes flood the network with route requests and route replies, effectively paralyzing the network. In tampering attacks, the intermediate nodes modify the packet content or change source and destination address. Data packets are prevented from reaching node and also nodes are prevented from sending data packets in denial of service attacks [3]. In rushing attacks, malicious nodes advertise itself as having shortest route to destination node, thus all traffic is forwarded to it and the node does not forward any traffic at all in Black hole attack [4]. These black holes can be detected only by monitoring the traffic [5]. A wormhole attack [6] creates a tunnel called, wormhole tunnel, between two nodes. A wormhole tunnel diverts packets to some random node in the network rather than the intended destination. A Sybil attack [7] occurs when the malicious node acts like two or more nodes. Sybil nodes are created by false identities or impersonation of nodes in the network. Due to these kinds of attacks, MANET network becomes vulnerable for the poor performance threats. Many solutions are introduced for addressing this wireless networks attacks. The paper is organized as follows. Section 2 describes working of DSR. Section 3 describes Gray hole and Black hole attack. Section 4 is literature survey. Different techniques of black hole attack detection and prevention are discussed in section 5. Section 6 describes proposed work. Finally Section 7 concludes the paper.

2. Overview Of Dynamic Source Routing Protocol (DSR)

DSR is an on-demand protocol designed by D. B. Johnson, Maltz and Broch to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table update messages required in the proactive routing protocols. The distinguishing feature of Dynamic Source Routing (DSR) is the use of source routing. DSR is a reactive protocol i.e. it doesn't use periodic updates. It computes the routes when necessary and then maintains them. Source routing is a routing technique in which the sender of a packet determines the complete sequence of nodes through which the packet has to pass, the sender explicitly lists this route in the packet's header, identifying each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination host. There are two basic parts of DSR protocol: route discovery and route maintenance. Every node maintains a cache to store recently discovered paths. When a node wants to send a packet, it first checks the cache whether there is an entry for that. If yes then it uses that path to transmit the packet. Also it attaches its source address on the packet. If there is no entry in the cache or the entry is expired, the sender broadcasts a route request packet to all its neighbors asking for a path to the destination. Until the route is discovered, the sender host waits. When the route request packet arrives to any other nodes, they check whether they know the destination asked. If they have route information, they send back a route reply packet to the destination. Otherwise they broadcast the same route request packet as shown in figure 1(a). Destination node generates Route Response and adds it to the header of Route Request packet then returns back to the source node as shown in figure 1(b). Once the route is discovered, the sender will send its required packets using the discovered route as well as insert an entry in the cache for future use. Also the node keeps the age information of the entry to recognize whether the cache is fresh or not. When any intermediate node receives a data packet, it first sees whether the packet is sent to itself or not. If it is the destination, it receives that else it forwards the packet using the path attached on the packet.

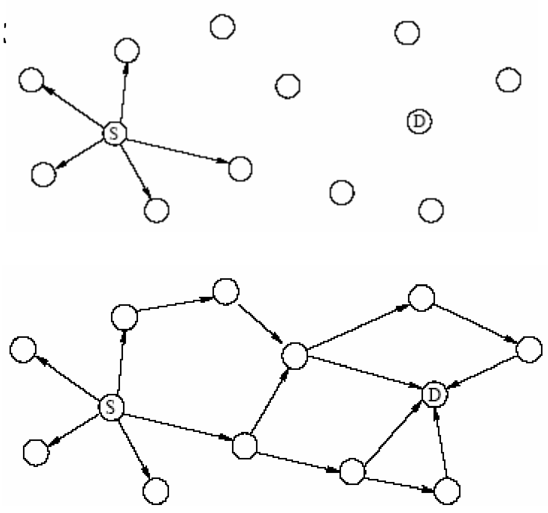

Figure 1(a) Propagation of Request (RREQ) packet

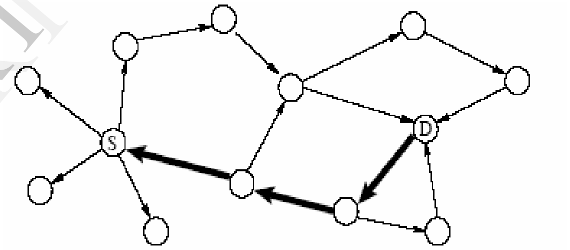

Figure 1(b) Creation of route in DSR

3. A Black Hole and Gray Hole Attack

A. Black Hole Attack

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it.

There are two ways this attack can happen

Using false address: In this method the malicious node will masquerade or use false address which may belong to another node. This cause all the data packets to reach at attacker's node instead of the true owner of the source address. All nodes in the network point their routes to this malicious node. The attacker can then drop the data packets.

Sending false route reply messages: The attacker exploits the DSR protocol [1]. Whenever a source node sends a route request message (RREQ) it waits for some time to get the reply. If the malicious node receives this RREQ message, it sends a false route reply message to the source node with modified higher sequence number. If the reply from attacker reaches to the source node before legitimate route reply message then attack occurs. This leads to an assumption by the source node that this node has a fresh and accurate route to destination. The source node denies any other reply messages and starts sending the data packets through the malicious node. The malicious node can now drop the packets and doesn't allow forwarding [8]. As shown in Figure 2, the Black hole node (BH) drops all the packets received by it without forwarding it to its next hop node Node2 (N2).

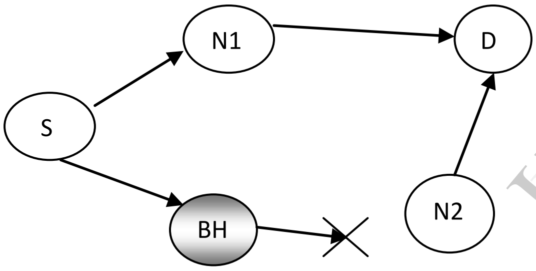

Figure 2. Black hole Attack

S – Source N1-Node1
N2 - Node2 BH – Black hole
D – Destination

B. Gray Hole Attack

The Gray hole attack is a variation of black hole attack. In this attack the attacker drops packets selectively. The attacker can use any policy of dropping the packets. It can drop all UDP packets while forwarding the TCP packets. The attacker can also use statistical method such as dropping only 50% of the packets. This can cause heavy destabilization of the network.

4. Literature Survey

For security in MANETs, many routing protocols have been designed in order to provide protection against the possible attacks.

Sun et al [8] presented a general approach for detecting the black hole attack. They planned a neighborhood based method to detect the interloper and a routing recovery protocol to set up a correct course to the true destination. They first introduced the neighbor set of a node, which is all of the nodes that are within the radio transmission range of a node. Two types of control packets are introduced to share neighbor set between different nodes. If two neighbor sets received at the same time are different enough, it can be accomplished that they are generated by two different nodes. One disadvantage of this scheme is that there must be a public key infrastructure or the detection is still susceptible.

Patcha *et al* [9] proposed a collaborative method for black hole attack prevention. A watchdog method is introduced to include a collaborative architecture to deal with collusion amongst nodes. In this algorithm, nodes in the network are classified into trusted, watchdog, and ordinary nodes. Every watchdog that is chosen should observe its normal node neighbors and decide whether they can be treated as trusted or malicious.

Shila et al [5] offered a solution to defend selective forwarding attack (gray hole attack) in Wireless Mesh Networks. The algorithm uses the detection threshold and packet counter to discover the attacks.

5. Black Hole and Gray Hole Detection Techniques

i) Neighborhood-based Technique
ii) Reputation based Technique
iii) Digital Certificate based Technique
iv) Hybrid Routing Technique
v) Coursed based Detection Technique

i) Neighborhood-based Technique:

In neighborhood based technique once the normal path discovery process is finished, the source node sends a special control packet to request the destination to send its current neighbor set. The neighbor set of a node is defined as all of the nodes that are within the node's radio transmission range. They claim this metric provides a good "identity" of a node, that is if the two neighbor sets received at the same time are different enough, it can be concluded that they are generated by two different nodes. They verified their claim through the following two experiments:
i) They measured the neighbor set difference of one node at different time instants *t* and *t*+1 seconds under

different moving speeds and network sizes. The result shows that there is not much change of a node's neighbor set during a route discovery process[8].

i) They examined the neighbor set difference of two different nodes at the same time, that is (({A's neighbor set} U {B's neighbor set}) – ({A's neighbor set} ∩ {B's neighbor set})). The result shows that the probability that node A's neighbor set is the same as that of node B is very small.

Detection: After source node receives the neighbor set information, it analyses them by measuring the neighbor set difference. If the difference is larger than the predefined threshold values, the source node knows that current network has black hole attacks and responds to it accordingly.

Response: They proposed a routing recovery protocol, with the following two-step approach:

i)when a black hole attack is identified, the source node uses a cryptography-based method to authenticate the destination, and

ii) once verified, the source node sends a control packet to destination node to form a correct path by modifying the routing entries of the intermediate nodes between them.

ii) Reputation based Technique :

CONFIDANT [11](Cooperative of Nodes, Fairness In Dynamic Ad-hoc Networks) is an extended version of Watchdog and Path rater. It is also implemented on unicast routing protocol such as DSR. Each node monitors the behavior of its next-hop neighbors. If a suspicious event is detected, the information is given to the reputation system. If the event is significant for the node, it is checked whether it has occurred more often than a predefined threshold, which is high enough to distinguish deliberate malicious behavior from simple coincidences such as collisions. If the occurrence threshold is exceeded, the reputation system updates the rating of the node that caused the event. If the rating turns out to be intolerable, the information is relayed to the path manager, which proceeds to delete all routes containing the intolerable node from the path cache. The node continues to monitor the neighborhood, and an ALARM message is sent by the trust manager component. This message contains the type of protocol violation, the number of occurrences observed, whether the message was self-originated by the sender, the address of the reporting node, the address of the observed node, and the destination address. When the monitor component of a node receives such an ALARM message, it passes it on to the trust manager, where the source of the message is evaluated and the report is forwarded to the reputation system. Reputation system shares this information with all nodes present in network.

CONFIDANT is suitable for small networks with low mobility; however it might be less efficient for large networks since each node needs to maintain a huge table for reputation purposes. Likewise, the high mobility of nodes increases significantly the communication overhead. Additionally, this protocol inherits all the problems of passive-feedback based schemes since it uses this mechanism for the monitoring function.

iii) Digital Certificate based Technique:

In Digital Certificate based Technique the nodes authenticate each other by issuing security certificate in digital form to all the other nodes in the network. It uses the route discovery scheme of DSR to issue security certificates. Every node participating in certificate chaining must be able to authenticate its neighbors, create and issue certificate for neighbors and maintain the set of certificates it has issued. The issue of certificates can be on the basis of security parameters of the node. Each node has a local repository consisting of certificates issued by the node to other nodes and certificates issued by others to the particular node. Therefore each certificate is stored twice. The extended route discovery process of DSR consists of the original route discovery process followed by an authentication phase[13]. To overcome black hole attack, source node does not initiate the data transfer process immediately after the routes are established. Instead it waits for the authenticated reply from the destination. The destination node sends authenticated messages appended with certificates taken from the corresponding node's repository. Since the security levels of participating nodes are updated based on their faithful participation in the network, any malicious nodes between the source and destination can be very well isolated from the network as these nodes would not be able to produce the certificates to be appended with the RREP message.

iv) Hybrid Routing Technique :

Hybrid routing approach is designed to prevent the collaborative black hole attacks. The proposed mechanism is composed of proactive and reactive method to form a hybrid routing protocol, and the major essence is the DSR on-demand routing. This solution is briefly introduced as below. In the beginning of routing stage, the source node sends bait RREQ packet before starting route discovery. The target address of bait RREQ is random and nonexistent. To avoid the bait RREQ inducing the traffic jam problem, BDSR use the same method with DSR. That is all bait RREQ packets only survive for a period time. The malicious nodes are easily expelled from the initial phase, because the bait RREQ is able to attract the forged RREP from black hole node. In authors' mechanism, the generator of RREP is recorded in the RREP's additional field. Therefore the source node can recognize the location of attacker from the reply location of RREP. Compare with the primitive DSR scheme and watch dog method, the simulation results show that BDSR provides an excellent packet delivery rate. The packet delivery ratio of BDSR is 90% which is more superior to DSR and WD approach. Moreover, the communication overhead is also lower than watch dog scheme but slightly higher than original DSR routing protocol.

v) Course based Detection Technique :

In course based detection method a source node does not watch every node in the neighbor, but only consider the next hop in current route path[25]. For example, in Figure 1, S is the source node; D is the destination node; and P is a gray hole.

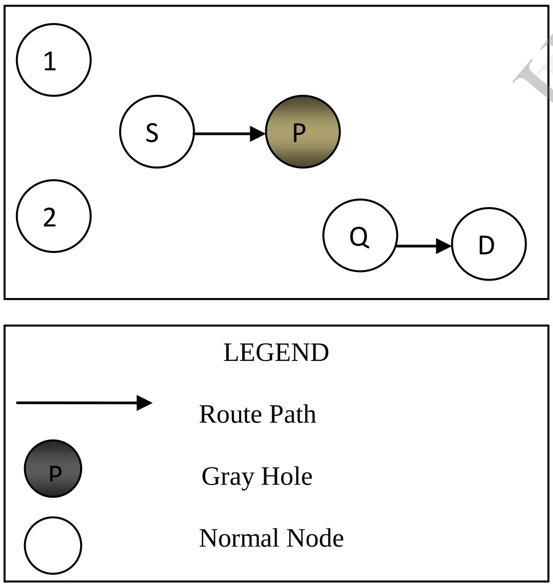

Figure 6. Course based detection technique

Node S is sending data packets to node D through the course S, P, Q, D. In this system, Node S only watches Node P, which is the next hop; but does not care Node 1 and Node 2.

To implement the algorithm, every node should keep a FwdPkt-Buffer, which is a packet digest buffer. The algorithm is divided into three steps:
1. When a packet is forwarded out, its digest is added into the FwdPktBuffer and the detecting node overhears.
2. Once the action that the next hop forwards the packet is over-heard, the digest will be released from the FwdPktBuffer.
3. In a fixed period of time, the detecting node should calculate the overhear rate of its next hop and compare it with a threshold.
If the forwarding rate is lower than the threshold, the detecting node will consider the next hop as a black or gray hole. Latter, the detecting node would avoid forwarding packets through this suspect node. One problem of this detection method is that it suffers from a high false positive probability under high network overload if a constant threshold is used.

6. Proposed Work

The proposed work is based on DSR protocol which is completely on-demand ad hoc network routing protocol collected of two parts: Route Discovery and Route Maintenance. Proposed work is divided into two parts i) Detection Algorithm ii) Analysis of False Positive Probability
The detection algorithm is based on a course based scheme as described in [25]. This detection method suffers from a high false positive probability under high network overload if a constant threshold is used. False positive probability is the ratio of number of honest nodes incorrectly detected as malicious and the total number of honest nodes. Theoretically, the proposed detection method should have a better performance on false positive probability than the fixed-threshold solution. It may confirm by comparing false positive probability between different solutions.

1) The cause of high false positive probability is hidden node problem in carrier-sensing multiple access with collision avoidance (CSMA/CA) protocol. A hidden node is a node which is beyond range of a packet sender (node S in Figure 6) but in the range of a packet receiver (Node P in Figure 6). In Figure 6, Node Q does not hear the data from Node S to Node P, and it is a hidden node. When Node Q transmits to node R, the transmission collides with that from Node P to node Q. Therefore, the hidden nodes guide to higher collision probability.
2) As for course based detection, black node problem will greatly increase the false positive probability. In

Figure 7, Node S is source node and Node R is destination node. Packet 1 is transmitted from Node Q to Node R. At the same time, Packet 2 is transmitted from Node S to Node P. Consequently, Packet 1 and Packet 2 will collide at Node P. Then Node S will retransmit Packet 2; but Packet 1 will not be sent again because Packet 1 has been received by Node R successfully.

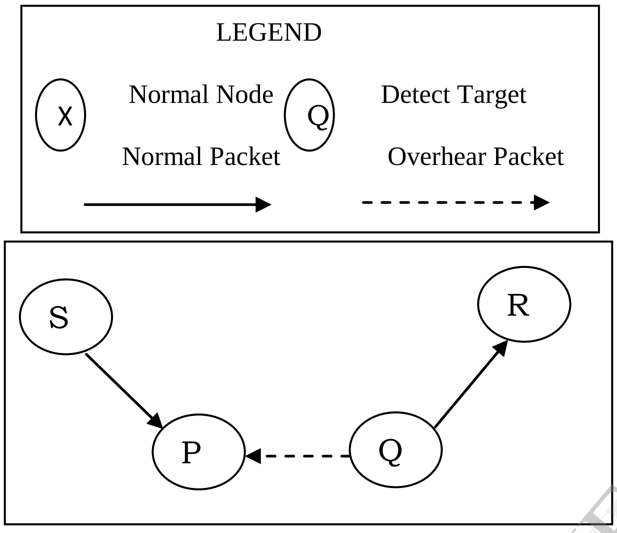

Figure 7: A collision problem with the course based detection scheme

3) As a result, Node P misses Packet 1 and treats it being dropped by Node Q deliberately. In summary, a high network overload leads to a high collision rate caused by hidden node problem, so that the probability that a detecting node fails to overhear its next hop increases consequently. Thus, the false positive probability rises in the end.

The aim of the proposed system is to lower the performance misuse by Gray hole and Black hole on detection using NS2 Simulator. Also high network overload leads to a high collision rate caused by hidden node problem, so that the probability that a detecting node fails to overhear its next hop increases consequently. Thus, the false positive probability rises in the end. The aim is that proposed detection method should have a better performance on false positive probability than the fixed-threshold solution.

7. Conclusion

In this paper a survey on different existing techniques for detection of black hole and Gray hole attacks in MANETs with their defects is presented. Although these may not be avoided in totality, there is a need for trade-offs to achieve a secure optimal performance. Based on the results in above techniques, it can be concluded that Black Hole attacks affect network negatively. Hence, there is need for perfect detection and elimination mechanisms. Future work is intended to design an efficient Black Hole attack detection and elimination algorithm with minimum delay, overhead and better performance on false positive probability as compare to existing solutions.

References

[1] Hongmei Deng, Wei Li, and Dharma P. Agarwal, “Routing Security in Wireless Ad Hoc Networks”, University of Cincinnati, *IEEE Communications magazine*, October 2002

[2] Johnson D. B., Maltz D. A. and Hu, Y. “The Dynamic Source Routing Protocol for Mobile Ad hoc Networks (DSR)”, *IETF MANET, Internet Draft*, 2003

[3] Douligeris, C. and A. Mitrokosta, “DDoS attacks and defense mechanisms: Classification and state of the-art” Computer Network., 2004,44: 643-666.

[4] Hu, Y.C., A. Perrig and D.B. Johnson,” Packet leashes: A defense against wormhole attacks in wireless networks” *Proceedings of the IEEE Societies 22nd Annual Joint Conference of the IEEE Computer and Communications*, Mar. 30-Apr. 3, IEEE Xplore Press, 2003a, pp: 1976-1986.

[5] Shila Devu Manikantan, Anjali Tricha, ”Defending Selective Forwarding Attacks in WMNs” *IEEE Transactions on Wireless Communications archive* ,Volume 9 Issue Pages 1661-1675, 5 May 2010.

[6] Hu, Y.C., A. Perrig, D.B. Johnson,”Ariadne: A secure on-demand routing protocol for ad hoc networks.” *Wireless Network*, 2005,11: 21-38.

[7] Douceur J.R., ”The sybil attack” Peer-to-Peer Syst. Lecture Notes Comput. Sci., 2002,2429: 251-260.

[8]Sun,Y. Guan; J. Chen, U.W. Pooch, “Detecting Black-hole Attack in Mobile Ad Hoc Networks”,*5th European Personal Mobile Communications Conference*, Pg.490-495, 2003.

[9] Patcha and Mishra “Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad HocNetworks” *IEEE Transactions on Wireless Communications,Pg.* 7803-7829, 2003

[10] S. Marti, T. Giuli, K. Lai, and M. Baker, “*Mitigating routing misbehavior in mobile ad hoc networks*,” The 6th ACM International Conference on Mobile Computing and Networking , August 2000.

[11] Sonja Buchegger and Jean-Yves Le Boudec, “Performance analysis of the CONFIDANT protocol” *Proceedings of the 3rd ACM international symposium on Mobile Adhoc networking &computing’* 2002. p.p:226–236.

[12] Wang W, Bhargava B, Linderman M ,"Defending against Collaborative Packet Drop Attacks on MANETs" *2nd International Workshop on Dependable Network Computing and Mobile Systems*, New York, USA, 27 September 2009

[13]K.Selvavinayaki, K.K.Shyam Shankar, Dr.E.Karthikeyan "Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANETs" *International Journal of Computer Applications (0975 – 8887)* Volume 7– No.11, October 2010

[14] Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L "Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs." *13th International Conference on Advanced Communication Technology*, Phoenix Park, Korea, 13-16 Feb. 2011

[15] Isaac Woungang, Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi and Mohammad S. Obaidat, "Detecting Black hole Attacks on DSR-based Mobile Ad Hoc Networks" 978-1-4673-1550-0/12/2012 IEEE

[16] Weerasinghe, H. and H. Fu,"Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation" *Future Generat. Commun. Netw.*, 2: 362- 367,2007.

[17] Mahmood Salehi, Hamed Samavati and Mehdi Dehghan, "Evaluation of DSR Protocol under a New Black hole Attack", 20th *Iranian Conference on Electrical Engineering*, 978-1-4673-1148-9 May 15-17,2012

[18] Isaac Woungang," Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks", 978-1-4673-1550-0, 2012 IEEE

[19] José Luis Tornos, Joan Josep Piles and José Luis Salazar "DSR: Authenticated DSR" *6th International Conference on Risks and Security of Internet and Systems* (CRiSIS) 978-1-4577-1891 5/11/2011 IEEE

[20] Ranjeet Suryawanshi, Sunil Tamhankar, "Performance Analysis And Minimization Of Black Hole Attack In MANET" ISSN: 2248-9622 *IJERA* Vol. 2, Issue4, July-August 2012, pp.1430-1437

[21] Ming-Yang Su, Kun-Lin Chiang and Wei-Cheng Liao , "Mitigation of Black Hole Nodes in Mobile Ad Hoc Networks", *IEEE International Symposium on Parallel and Distributed Processing with Application*, 2010.

[22] A. Nadeem, M. Howarth "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks" *IEEE Communications Surveys and Tutorials* Volume: PP , Issue: 99 , Page(s): 1 – 19, 2013.

[23] M. Patel, S. Sharma "Detection of malicious attack in MANET a behavioral approach" *3rd International Advance Computing Conference (IACC), IEEE* , Page(s): 388 – 393, 2013.

[24] Kozma W, Lazos L (2009) REAct: Resource Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits. Paper pre sented at the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16-18 March 2009

[25] Disha G. Kariya, Atul B. Kathole, Sapna R. Heda, "Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method" *International Journal of Emerging Technology and Advanced Engineering* ISSN 2250-2459, Volume 2, Issue 1, January 2012

[26] V. Ramesh, Dr. P. Subbaiah, N. Sandeep and C. P. Bhaktavastalam, "Secured Preemptive DSR(S-PDSR): An integration of SRP and SMT with Preemptive DSR for Secured Route Discovery", *International Journal of Ad hoc, Sensor & Ubiquitous Computing* Vol.1, No.3, September 2010.