Open access Journal International Journal of Emerging Trends in Science and Technology

DOI: http://dx.doi.org/10.18535/ijetst/v3i01.08

An Approach for Security Measures of Black Hole Attack in MANET

Authors
Prachi Goyal*[1], Chitvan Gupta[2]
[1]Department of Computer Science and Engineering, NIET,Greater Noida, UPTU, UP –India
Email: *Prachi.14.1989@gmail.com*
[2]Department of Computer Science and Engineering, Asst. Prof. NIET, Greater Noida, UPTU, UP –India
Email: *chitvangupta@gmail.com*

Abstract

Mobile Ad Hoc Network (MANET) is a major next generation wireless technology which is mostly used in future. MANET is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and predefine organization of available links. In a MANET mobile node will be increases and moveable, so that attacker will be attack by a malicious node which brings great challenges to the security of Mobile Ad Hoc network. The Black hole attack is one of such security issue in MANET. Our focus is specifically is on ensuring the security against the Black hole attack with the help of the popular routing protocol which is mostly used in MANET. Mobile Ad hoc Networks (MANET) are the extension of the wireless networks. They plays important role in real life applications such as military applications, home applications etc. these networks are exposed by a lot of security attacks such as alteration, Denial of service attack, Fabrication attack etc. Black hole attack is one of the dangerous active attacks on the MANET. In this research paper an efficient approach for the detection and removal of the Black hole attack in the Mobile Ad Hoc Networks (MANET) is described. The algorithm is implemented on AODV (Ad hoc on demand Distance Vector) Routing protocol. The algorithm can detects both the single Black hole attack and the Cooperative Black hole attack. The beauty of the algorithm described in this paper is that it not only detects the black hole nodes in case when the node is not idle but it can also detect the Black hole nodes in case when a node is idle as well.

Keywords: *Mobile ad hoc network (MANET); Black hole; routing security; NS2 simulation.*

Introduction

Mobile ad-hoc networks (MANET) are formed by a group of mobile nodes, and every node in MANET can both act as host or router, and this wireless host communicate with each other without the existing of fixed infrastructure and without a central control. MANET can have more flexible because node can move any direction inside the network and it can be turn up and turn down in a very short time. In MANET there is no any base station, these mobile nodes are interconnected via wireless link which agree to cooperate and forward packet each other's. These mobile node in mobile Ad-Hoc network dynamically creates routes among themselves and form their own wireless network on the fly. Figure 1 shows a simple Ad-Hoc network model with three nodes.

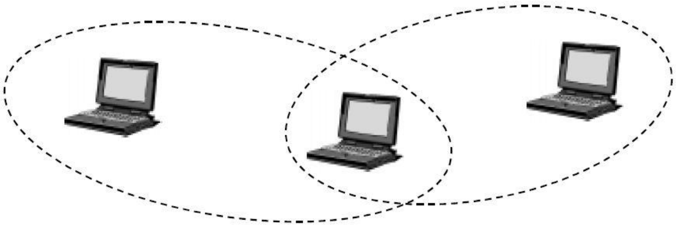

Fig 1. Example of Simple Ad-Hoc network with three participating nodes [15]

The outmost nodes are not inside transmitter range of each other. But the middle node can be used to onward packets between the both outermost nodes. The middle node work as a route and the three nodes have form an Ad-Hoc network.

An Ad-Hoc network have no need of any centralized administration. It ensure that the network won't failure since one of the mobile node moves from transmitter range. Nodes can be able to arrive or leave the network. Since the inadequate transmitter range of nodes, several hops can be needed to reach to the other nodes. In such a way every node acts as a both host and router. A node can be noticed as an abstract entity enclosing a router and a set of associated mobile hosts (figure 2). A router is an object, like other things runs among a routing protocol. A mobile host is simply an IP-addressable host in the old logic.

Ad-Hoc network are also accomplished to handling topology changes and faults in nodes. This can be fixed through network reconfiguration. If a node leaves the network and causes link damages, then affected nodes can request new routes and the problem will be resolve, it will faintly increase the delay, but the network will still be effective. MANET take the advantage of the nature of the wireless communication medium. In a wired network the physical cabling is done a priori curbing the connection topology of the nodes. Such type of restrictions are not occur in the wireless sphere and provide two nodes that are within transmitter range of each other, and rapid link between them may form.

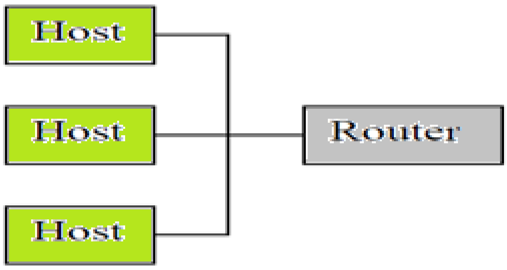

Fig. 2. Block diagram of mobile node acting both as hosts and a router [16].

Literature Review

Soufine Djahel, Farid Nait-Abdesselam and Ashfaq Khokhar proposed solution [3] to deals with the cooperative black hole attack an acknowledgement based on the alleviate the damage of topology evidence due to the releasing of topology control (TC) message by aggressors. In accumulation to the unique control message of OLSR are Hello and TC messages. They introduce another two type of control packets, they are named as 3hop_ACK and HELLO rep. The HELLO rep message is used by a node to advertise its 2 hop neighbors to a requesting multi point relay (MPR) node and 3hop_ACK message is used to acknowledge its reaction of a TC message by a node from the neighbors 3 hops away, and For the request, they utilizes one of the vacant bit in the HELLO message to specify the sender's MPR nodes would produce HELLO rep packet or not.

Ms. GayatriWahane and Ms. SavitaLonare has proposed scheme [5] for detecting and defending against co-operation black hole attack that identified and presented by an algorithm to the modification of AODV routing protocol with two types. First is maintenance of routing information table (RIT) and reliability checking of a node. In RIT every node maintains three bit information. In these three bit the first two bit is discuss earlier but the last one bit is represented by "through any trustful node". This last bit is set if any trustful node has routed data packet through the node. But in reliability checking of node is based on a intermediate node that generate the RREP has to provide the information about Next hopping node (NHN) and RIT entry for the NHN. Source node will check its own RIT to see whether IN is unreliable and source node send Additional request (ARq) message to next hop node.

Ankur Mishra, Ranjeet Jaiswal and Sanjay Sharma [11] propose the solution to find the trusted node source demand their respective DRI table with check bit and find one trusted node (CN) to destination With the help of check bit .Now source node send prob. packet 2 through remaining suspected node to that trusted node after TTL value OF FIRST PROB PACKET is over source node SN make enquiry to trust node

(CN) whether he receive prob. packet 2. If packet not receive then source node send another PROB PACKET 2 to CN. if any one of two PROB PACKET is received we consider that node as another trusted node and source node mark an entry under check bit as '1'for that node but if the packet is not received source treat them as 'black hole node' and maintains the identity of such node as MALI_ node, so in future it can discard any control messages coming from that node.to the intermediate node that replays the RREQ message to check whether the route from the intermediate node to the destination node exists or not. If it exists we can trust the intermediate node and send out the data packet .if not then source node just discard the reply message from the intermediate node and send out alarm message to the network and isolate the node from the network.

Suparnab is was, tanumoy nag and sarmishtaneogy proposed [9] a solution to prevention of black hole to average value for following parameters- rank, velocity, and battery power for selected a higher trust value among all the available routes. These trust values of all routes are compared and the route having highest average trust is selected for packet transmission. If the packet transmission through is selected for transmission destination node send an acknowledgement to source node which in turn increment the rank and decrements battery power of each of the node in that route.

Tamilselvan L and Sankaranarayanan [14], has projected a Time-based Detection system based on the original AODV routing protocol. This system is setting timer in the Timer Expired Table and for collecting the further request from other nodes after getting the first request. It will amass the packet's sequence number and the received time in a Collect Route Reply Table (CRRT), counting the timeout value based on the incoming time of the initial route request, judging the route belong to appropriate or not based on the above threshold value.

Problem statement:

(A) Black hole attack

Routing protocol has bare variety of attack. Black hole attack [1] [6] is denial of services (DOS) attack in MANET. Black hole attack is a type of active attack in which the malicious node takes the benefits of the liabilities of routing protocol. In this attack a malicious node falsely broadcasts the shortest path to the destination node during the route detection and maintenance phase to sending a fake RREP packet to the source node. When the source node receive his RREP packet its start sending a data packet to the malicious node and this malicious node engage all these data packet and drops them fully or sometimes partially. When another RREP packet is reaches from another route to the source node then they discard that RREP packet. So that source and destination node will not be able to communicate with each other. Black hole attack has two types:-

1. Single Black hole
2. Cooperative Black hole attack

1. Single Black hole attack: - It is very simple form of black hole attack because in this attack only one malicious node is used to perform attack. That malicious node advertise itself as a node of shortest path to the destination and when the packet reached at it this node simply discard the all packet which is sending from the source node to the destination.

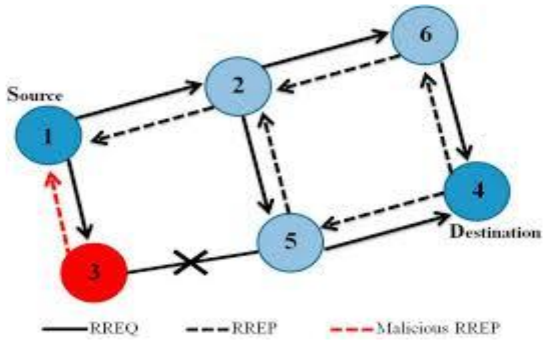

Figure 3. Single Black hole attack

2. Cooperative Black hole attack:- In black hole attack there are more than one malicious nodes are involve and these malicious nods have also send a false RREP packet to the source node that has started a route detection in order to show itself as a destination node or an intermediate node to the actual destination node. This malicious absorb, drop and then lost the entire packet which is sending from the source node. In sometime these malicious has cooperate with each other with the same aim of dropping packets these are known as cooperative black hole node [13] and these type of attack is known as cooperative black hole attack.

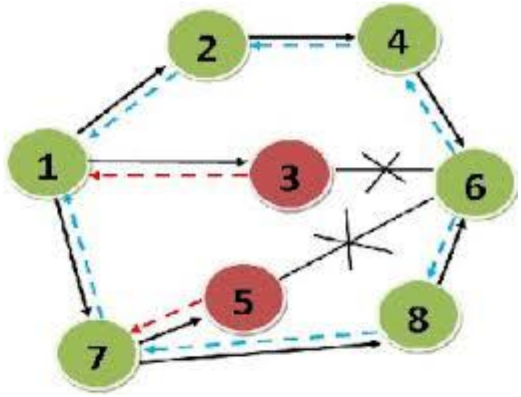

Figure 4. Cooperative Black Hole Attack

In the fig 4 source node wishes to transmit a data packet to the destination, it first broadcast the RREQ packet to the neighboring nodes. The (Black hole node) malicious nodes being part of the network, also receive the RREQ packet. The RREP packet from the malicious node 3 & 5 reaches to the source node, it start sending data to this malicious node and another RREP packet which is reached later from different route they discard it. This malicious node drop or absorb all data packets which is sending from the source to destination .This situation is follow only when single malicious node has occur in the network. But when multiple black hole nodes are acting in coordination with each other first black hole refer to its partner as next hop, the source node send further request (frq) through a different route. Node 1 asks if he is having route to 3 and route to destination node. Because 3 is cooperating with 5 its further reply is 'yes 'for both questions. Source node 1 start sending packet assuming route (1,3,6) is secure but the packet are drop by node 3.

(B) MANET routing protocol

MANET routing protocols is used for finding a route for shortest path in the network. The random and rapid motions of MANET's require that the node always find new routes. These new routes is finding with the help of these routing protocol: Proactive, Reactive and Hybrid touting protocol [12]

Proactive routing protocols: - These are the table-driven routing protocols. In proactive routing protocol, each node maintains a routing table which contains records of adjacent nodes and reachable node and also contains the number of hops. If the size of network increases, the overhead also increases. It is of several types which are mention in below:

i. DSDV ii. OLSR
iii. WRF iv. CGSR

Reactive routing protocol: - Reactive routing protocol is called On-demand routing protocols. These protocols do not attempt to maintain correct routing information on all nodes at all times. Routing information is collected only when it is needed and route determination depends on sending route queries throughout the network. This routing protocol is categorized into following way which is mention below:

i. AODV ii. DSR
iii. ACOR iv ABR

Hybrid routing protocol: -In Hybrid routing protocol, there is tradeoff between proactive and reactive protocol. Proactive protocol have large overhead and less latency while reactive protocols have less overhead and more latency so a hybrid protocol is presented to overcome the shortcoming of both proactive and reactive routing protocol. Hybrid routing protocol is combination of both proactive and reactive protocol. It is dived into few part which is mention below:

i ZRP ii. TORA
iii. ARPAM iv. OORP

MANET technology is a dynamic topology such that node can easily join or leave the network at any time .when the mobile Ad-Hoc network are being used in mission critical operations, other issues of security also arise. So that provides a ultimate goal to protected communication between mobile node in a hostile environment with the support of these some routing protocol such as AODV, DSR, DSDV and ZRP.

Ad-Hoc on demand distance vector (AODV)

AODV (Ad-hoc on demand distance vector) [13] routing protocol is a reactive routing protocol and it is the most popular and widely used routing protocol which is intended for Ad-Hoc mobile network. It is an on demand algorithm means that the route is established only when it is desired by the sourced node for transmitting a packet. AODV is capable for both unicast and multicast routing. This process is accomplished with route discovery mechanism which source node S sees its routing table if a valid route entries is found toward the destination D then source node S send the data to a given destination node D , else it initiate a route discovery procedure which source node broadcasting a Route Request(RREQ) message to the neighbor. When a RREQ is receiving by any intermediate node they finally see its routing table to find a fresh route toward the requested destination in RREQ. If such a route is obtain a route reply (RREP) is unicast toward a source via intermediate node .If intermediate node doesn’t obtain a fresh route its update its routing table and send RREQ to these neighbor. This process is repeated until RREQ accomplish the destination node D and they all have successful route from source to destination.

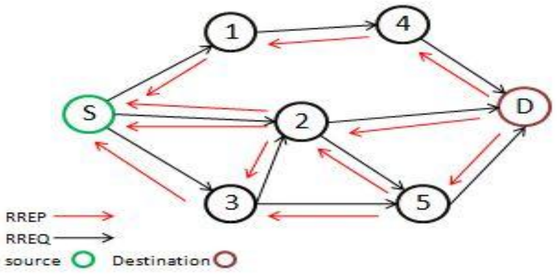

Figure 6. Route discovery process under AODV

Dynamic source routing (dsr)

Dynamic source routing (DSR) is a reactive routing protocol and is based on a method known as source routing. Where in reactive routing protocol are also called on demand protocol , so these protocol do not maintain routing information and do not need to maintain or update routing table. Basically DSR is designed for use of Multi-hop Ad-Hoc network of mobile node for small diameter which source initiates route discovery on demand basis. The sender determines the route from source to destination and it includes the address of intermediate node to route record in the packet. This process is done with the use of the cache technology to maintain the routing table. There are two phase in DSR: Route discovery and route maintenance. The node first check its route cache and then source node send the packet through the route to the destination node otherwise it initiate the route discovery process by broadcasting route request packet to the network to know the route dynamically.

Zone routing protocol (ZRP)

ZRP is a type of hybrid routing protocol [10]. This protocol distributes the whole network into several routing zones and postulates them into two separate protocols that work inside and between the routing zones. These two are: Intrazone (IARP) and interzone (IERP). The IARP operates inside the routing zone. It provide routes to all the nodes within the zone and also acquire the smallest space for them.

Proposed Methodology:

This proposed solution the requesting node without sending the DATA packets to the reply node at once; node has to wait till other replies with next hop details from the other neighboring nodes. After receiving the first request to our neighbors it sets timer in the ‘Timer Table’ to the node, for collecting the further requests from different nodes. It will store the ‘sequence number’, of RREP and the time at which the packet arrives. The time for which every node will wait is proportional to its distance from the source. It calculates the 'timeout' value based on arriving time of the first route request. It first checks in Route Reply Cache Table (RRCT) after the timeout value, whether there is any repeated next hop node or not. If any repeated next hop node is present in the reply paths it assumes the paths are correct or the chance of malicious paths is limited. Then it chooses any one of the paths with the repeated node to transmit the DATA packets. If no any repetition select random route from RRCT. Here again the chance of malicious route selected is reduced. We propose an additional route to the intermediate node that replies the RREQ message to check whether the route from the intermediate node to the destination node exists or not. When the source node receives the Further Reply (FRp) from the next hop, it extracts the check result from the reply packets. If the result is yes, we establish a route to the destination and begin to send out data packets. If the next hop has no route to the inquired intermediate node, but has a route to the destination node, we discard the reply packets from the inquired intermediate node, and use the new route through the next hop to the destination. At the same time, send out the alarm message to whole network to isolate the malicious node. If the next hop has no route to the requested intermediate node, and it also has no route to the destination node, the source node initiates another routing discovery process, and also sends out an alarm message to isolate the malicious node. Thus we avoid the black hole problem, and also prevent the network from further malicious behavior. But here we assume the black hole nodes do not work as a group and propose a solution to identify a single black hole. However, the proposed method cannot be applied to identifying a cooperative black hole attack involving multiple nodes. We may also develop a methodology to identify multiple black hole nodes cooperating as a group. The technique works with a little modified AODV protocol and makes use of the Data Routing Information (DRI) table in addition to the cached and current routing tables. A black hole has two properties. First, the node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the node consumes the intercepted packets. The proposed solution is illustrated in the below figure 7.

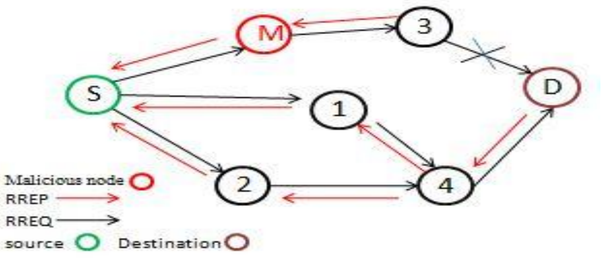

Fig. 7. Black hole attack solution.

Working principle

In the above figure 7, source node S wants to transmit to destination D. So it first broadcast the route request to all our neighboring nodes. Here node 1, node M and node 2 receive this broadcast request. This malicious node M has no intention to transmit the DATA packets to the destination node D but it wants to intercept/collect the DATA from the source node S. So it immediately replies to the request as (M – 3). Instead of transmitting the DATA packets immediately through M, S has to wait for the reply from the other nodes. After some time it will receive the reply from node 1 as (1 – 4), and node 2 as (2 – 4). According to this proposed solution it first checks the path that contains repeated next hop node to the destination. If there is no repeated node select random path and transmits the data through that path. The routing table from S to D is given in Table 2.In the above figure 7, source node S wants to transmit to destination D. So it first broadcast the route request to all our neighboring nodes. Here node 1, node M and node 2 receive this broadcast request. This malicious node M has no intention to transmit the DATA packets to the destination node D but it wants to intercept/collect the DATA from the source node S. So it immediately replies to the request as (M – 3). Instead of transmitting the DATA packets immediately through M, S has to wait for the reply from the other nodes. After some time it will receive the reply from node 1 as (1 – 4), and node 2 as (2 – 4). According to this proposed solution it first checks the path that contains repeated next hop node to the destination. If there is no repeated node select random path and transmits the data through that path. The routing table from S to D is given in Table 1.

Table 1. Routing Detail.

Source	Intermediate	Destination
S	M - 3	D
S	1 - 4 2-4	D

Proposed Algorithm

In this research paper a secure efficient algorithm for the detection of the Black hole attack is described. This algorithm firstly identifies the black hole node in the given Mobile Ad hoc Network and then removes the entries for that node from the routing table. The solution that we propose here, basically, only modifies the working of the source node without altering intermediate and destination nodes. In this method two main things are added namely Data Routing Information table and cross checking.

Steps:

```
1: Source node S broadcasts the request i.e. RREQ
2: Source node S receives an acknowledgement i.e. RREP
3: if RREP is from destination or a consistent node Then route data packets (source route)
4: Else
{
Send further RREQ and identity of intermediate Node to next Hop node
Receive further RREQ, next Hop node of current next hop node, now entry the data Routing Information for next hope nodes.  Place a data routing information entry for present intermediate node.
5: if (next hop node is a consistent node)
{
Check intermediate node for black hole using data routing information entry if (intermediate node is not a black hole)
route data packets (source route)
Else
{
Intermediate node is a malicious node
All the nodes along the reverse path from intermediate node to the node that generated
RREP are black holes (i.e. a malicious node)
}
}
                    Else
Current intermediate node = next hop node
}
6: Repeat step 4 & 5 until intermediate node is not a reliable node
```

Simulation Evaluation

Network simulator 2 (NS2) is an open–source event-driven simulator designed specifically for research in computer communication networks. Since its interception in 1989, NS2 has continuously gained tremendous interest from industry, academia, and government. Having been under constant investigation and enhancement for years, NS2 now contains modules for numerous network components such as routing, transport layer protocol, application, etc. to investigate network performance, researchers can simply use an easy-to-use scripting language to configure a network, and observe results generated by NS2. Undoubtedly, NS2 has become the most widely used open source network simulator, and one of the most widely used network simulators. We have implemented Black hole attack in an ns-2 simulator. For our simulations, we use CBR (Constant Bit Rate) application, TPC/IP (full duplex communication), IEEE 802.11b MAC and physical channel based on statistical propagation model. The simulated network consists of 30 randomly allocated wireless nodes in a 500 by 500 square meter flat space. The node transmission range is 250-meter power range. Random waypoint model is used for scenarios with node mobility. The selected pause time is 30s seconds. A traffic generator was developed to simulate constant bit rate (CBR) sources. The size of data payload is 512 bytes. In our scenario we take 30 nodes in which nodes 1-22 and 25-30 are simple nodes, and node 23 and 24 are malicious node or Black hole node. The simulation is done using ns-2, to analyze the performance of the network by varying the nodes mobility. The metrics used to evaluate the performance are given below.

Packet Delivery Ratio: The ratio between the number of packets originated by the "application layer" CBR sources and the number of packets received by the CBR sink at the final destination.

Throughput: Throughput is the average rate of successful message delivery over a communication channel.

Node Mobility: Node mobility indicates the mobility speed of nodes.

In this solution we implement the black hole attack based on the secure AODV routing protocol (SAODV) with timer table and RRCT using this tool. The scenario is show in the below table 2.

Table 2. Parameters used during MANET Simulation

Parameter	Value
Nodes	20
Simulation Time	5M
Mobility	Random way point model speed – 30 m/s pause time – Node mobility varied between 10 S to 90 S
Load	300 items, Data Pay Load 512 byte, Inter departure Time
Coverage Area	800m*800m

Conclusion

In MANET, security is major challenges for detection and prevention the malicious node for attacker. So here we can see that attacker will be attack through a some malicious node and this attack has comes under a black hole attack and this malicious node send a fake RREP packet with higher sequence number and Absorb all the data packet. So we can detect and prevent this black hole in some various techniques such as route discovery process, cross checking and DRI and some other way. This can be possible with the help of AODV routing protocol. Detection and prevention arises some defect which is packet delivery is low and consume a more time. So we solve these issues with the help of timer based and RRCT to SAODV to delivery packet with correct route. In this paper we have gone through the routing security issues of MANETs, described the black hole attack that can be mounted against a MANET and proposed a feasible solution for it in the AODV protocol. The proposed solution can be applied to: (a). Identify single and multiple black hole nodes cooperating with each other in a MANET; and (b) Discover secure paths from source to destination by avoiding multiple black hole nodes acting in cooperation. Also we showed that the effect of packet delivery ratio and Throughput has been detected with respect to the variable node mobility. There is reduction in Packet Delivery Ratio and Throughput. In Black hole attack all network traffics are redirected to a specific node or from the malicious node causing serious damage to networks and nodes as shown in the result of the simulation. The detection of Black holes in ad hoc networks is still considered to be a challenging task.

Future work

Future work is focused on design an algorithm for minimum delay and reduce packet dropping ratio and increase more packet delivery ratio in case of mobility of nodes in mobile Ad-hoc network. And also try to enhance the efficiency of mobile Ad-hoc network.

References

1. Yibeltal Fantahun Alem and Zhao Cheng Xuan, "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection",",2nd International Conference

on Future Computer and Communication , volume 3, 2010.

2. Jaydip Sen , Sripad Koilakonda and Arijit Ukil, A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks, Second International Conference on Intelligent Systems, Modeling and Simulation, pp 338-343 , Jan 2011Campbell Scientifi c, Inc., April 2008.
3. Soufine Djahel, Farid Nait-Abdesselam and Ashfaq Khokhar H. Yang, "An Acknowledgment-Based Scheme to Defend Against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol",IEEE Communications Society, 978-1-4244-2075-9/08/ © ICC 2008.
4. Ms. Gayatri Wahane and Ms. Savita Lonare " Technique for Detction of Cooperative Black Hole Attack in MANET", 4th ICCCNT ,IEEE- 31661 July 4-6, 2013, Tiruchengode, India.
5. Namrata Marium Chacko, Shini sam and P.Getzi Jeba Leelipushpam "A survey on various privacy and security features adopted in MANETs routing Protocol", International Multi-Conference on Kottayam,IEEE, pp 508 – 513, 22-23 March 2013.
6. Kishor Jyoti Sarma, Rupam Sharma and Rajdeep Das "A Survey of Black Hole Attack Detection in Manet", 978-1-4799-2900-9/14/ ©2014 IEEE.
7. Harsh Pratap Singh and Rashmi Singh "A Mechanism for Disco very and Prevention of Cooperative Black hole attack in Mobile Ad hoc Network Using AODV Protocol", Electronics and Communication Systems (ICECS),International Conference on Coimbatore ,IEEE, 13-14 Feb. 2014.
8. Kriti Chadha and Dr. Sushma Jain "Impact Of Black Hole And Gray Hole Attack In AODV Protocol", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014, Jaipur, India.
9. Suparna Biswas, Tanumoy Nag and Sarmistha Neogy "Trust Based Energy Efficient Detection and Avoidance of Black Hole Attack to Ensure Secure Routing in MANET",Applications and innovations in mobile computing (AIMoC),IEEE, Feb. 27 2014-March 1 2014, Kolkata, India.
10. Mangesh kumar S. Shegokar and R. R. Tuteja "Survey on Classified Ad-hoc Routing Protocols in MANET", International Journal of Science and Research (IJSR), Volume 3 Issue 4, April 2014
11. Ankur mishra, Ranjeet Jaiswal and Sanjay Sharma "A Novel Approach for Detecting and Eliminating Cooperative Black Hole Attack using Advanced DRI Table in Ad hoc Network", 3rd IEEE International Advance Computing Conference (IACC) , 2013.
12. Khushboo Sawant, Dr. M.K Rawat, "Survey of DOS Flooding Attacks over MANET Environment", Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 5(Version 6), May 2014, pp.110-115.
13. Sunil J. Soni & Suketu D. Nayak "Enhancing Security Features & Performance of AODV Protocol under Attack for", International Conference on Intelligent Systems and Signal Processing (ISSP) 978-1-4799-0317-7/13/2013 IEEE
14. Latha Tamilselvan & Dr. V Sankaranarayanan "Prevention of Co-operative Black Hole Attack in MANET", Journal of Networks, Vol. 3, No. 5, May 2008 Academy Publisher.
15. Stallings William(2000), network security essentials : applications and standards; Pearson education

16. Stallings William (2003), cryptography and network security principles and practices; Pearson education 3rd edition.
17. Sarvesh tanwar, Prema k.v ,“ threats & security issues in ad hoc network: a survey report”, International journal of soft computing and engineering (ijsce) ISSN: 2231-2307, volume-2, issue-6, January 2013.
18. Suparna Biswas, Tanumoy Nag and Sarmistha Neogy “Trust Based Energy Efficient Detection and Avoidance of Black Hole Attack to Ensure Secure Routing in MANET”,Applications and innovations in mobile computing (AIMoC),IEEE, Feb. 27 2014-March 1 2014, Kolkata, India.
19. Akshai aggarwal, Savita Gandhi, Nirbhay chaubey, Keyurbhai a jani, “trust based secure on demand routing protocol (tsdrp) for MANETs” , 2014 fourth international conference on advanced computing & communication technologies.
20. Morli Pandya, Ashish Kr. Shrivastava “Improvising the Performance with Security of AODV Routing Protocol in MANETs” , Nirma University International Conference on Engineering (NUiCONE), 978-1-4799-0727-4/13/$31.00 ©2013 IEEE.
21. Zhao Min, Zhou Jiliu “Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks” , International Symposium on Information Engineering and Electronic Commerce, IEEE computer society, 978-0-7695-3686-6/09 $25.00 © 2009 IEEE DOI 10.1109/IEEC.2009.12.
22. Pramod Kumar Singh ,Govind Sharma “An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET”, 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012 IEEE.