International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 04, April-2015

Detection Prevention and Mitigation of Black Hole Attack for MANET

Mehak Kaushal [1]
M.tech E.C.E
Lovely professional university
Punjab-144411: India

Mr. Gunjan Gandhi [2]
Ass. professor (E.C.E dept.)
lovely professional university
Punjab-144411; India

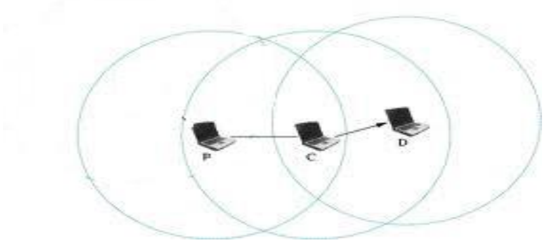
Abstract: **Wireless sensor networks are composed up of nodes which are deployed in an arbitrary positions and the communication between these nodes are done through the wireless channels. The data is send through these nodes. In WSN the security is the main issue which occurs through the inherent limitations of power usage and computational capacity. The network layer is responsible for routing packets, so we can say that this layer is the primary spot for the hackers and intruders. The basic attack on this layer is Black Hole attack which means denial of service and this attack disrupt the service of this particular layer. Transmission service is also affected by this type of dropping attacks. In this paper we will analyze the black hole effect which is the common attack during the routing process. In this attack, malicious nodes try to impersonate it as a destination node by sending wrong route reply packet to the source node. This is how the malicious nodes capture the data from the source node. Instead of forwarding there data the malicious node drop the packets. In this paper we will study various intrusion schemes and tries to mitigate the effect of black hole attack.**

Keywords: AODV, black hole attack, MANET's, HOOSc encryption scheme.

I.) INTRODUCTION

The main issue in wired and wireless networks is network security; it is the main requirement in the emerging field. The main attributes which should be satisfies in any network are authentication, confidentiality, access of integrity and non repudiation. Black hole attacks are prone in MANET's (Mobile Ad-hoc Network). MANET is a self configurable, self deployable and infrastructure less network in which nodes are continuously moving and creates dynamic topology. Mobile ad hoc network (MANET) is a collection of mobile hosts without the required intervention of any existing infrastructure or centralized access point such as a base station. The nodes of MANET do not require any infrastructure to communicate with one another. MANET's are used basically in the conditions where the wired and wireless infrastructure is inaccessible, overloaded, and destroyed. E.g. disaster relief applications and tactical battlefields.

MANETs [2] are not dependent on the fixed infrastructure where each node acts as an intermediate switch. The transmission of data or we can say that routing is done through different routing protocols. It is the recent active field and is getting spectacular attention because of self configuration and self maintenance, but security is the main issue which should be kept under consideration to protect the communication from the hostile environment. The present status of a node should be broadcasted to its neighbors before the source node wants to communicate with the target node. Because the current routing information is not known to the other nodes.



A.)MANET

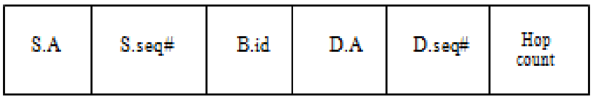
Basically there are three routing protocols named as:

Proactive routing protocol (table driven) *[3]:* it is also known as table driven protocol. In this type of routing protocol the nodes flashes their routing information to the neighbors periodically. Each node should have to manage its table by its own. The table should consist up of the number of hops, information of adjacent nodes and the reachable nodes. Each node should have to maintain the records of the neighbors as long as the network topology changes. The disadvantage of this protocol is that the overheads have been created in this protocol as the network size increases and the advantage is that the network status flashes immediately when any malicious node joins the network. Types of this routing protocol are destination sequenced distance vector (DSDV), optimized link state routing (OLSR), ZRP [4] and DBF [5].

Reactive routing protocol: This is also known as on demand routing protocol. The reactive routing only starts when the nodes are willing to send the data packets. The advantage is that the wastage of bandwidth can be reduced by using on demand routing protocols. The disadvantage is that this routing protocol suffers from certain packet loss. The main types of reactive protocol are AODV (ad hoc on demand distance vector) and dynamic source routing protocol (DSR).

Hybrid routing protocol: This protocol is the merged form of reactive and pro active routing protocol. It overcomes the limitations of both the protocol. These routing protocol forms a hierarchical or layered network. At the initial step of hybrid routing proactive routing is employed and gathers the unfamiliar information then to maintain the routing information reactive routing is being used. The type of hybrid routing is zone routing protocol (ZRP) and temporally ordered routing algorithm (TORA) [6]. TORA is highly distributed adaptive routing protocol. The operation is held under dynamic multi hop network. In TORA, to initiate the route the QUERY packet is send to all the neighbors. The QUERY is rebroadcasted through the network until it reaches the destination node. The recipient will broadcasts the UPDATE packet which contains the height list of the nodes with respect to the destination. When this UPDATE packet propagates in the network then each node which so ever is receiving this packet will set its height value higher than the value of neighbor from which the UPDATE packet received. When a node detects a network partition, it will generate a CLEAR packet that results in reset of routing over the ad hoc network.

AODV (ad hoc on demand vector routing) is reactive king of routing and generates the routes on the demands of routes. The key objective of the AODV is route discovery and route maintenance [7]. AODV is one of the most efficient routing protocols for the MANET as it is very dynamic in nature, self starting it also supports multi hop routing and it automatically detects the hidden routes and nevertheless it is loop free [9]. The discovery of route is initiated when the source node wants to find the route or when the lifetime of the existed route is expired. Each node is having its own sequence number which is increased by one when the topology changes [9]. The topology used in AODV [23] is multi hop. The three basic requests which are being followed by the AODV are RREQ (route request) RREP (route reply) RERR (route error). This process is started by broadcasting the RREQ packet to the neighboring nodes which rebroadcasted by the neighbor nodes until the sought route has been discovered. When RREQ is received by the nodes, some of the intermediate nodes which are having the fresh enough route or itself the destination nodes broadcast the RREP to the source node. Fresh enough route means the destination sequence number of sought node is greater than the destination sequence number of the source node itself. If the source node is getting multiple RREP's then the RREP packet with largest destination sequence number will be chosen and if the destination sequence number is same for two RREP's then the packet with the smallest hop count will be taken into account. RERR [9] is broadcasted when the node is having not any route to the destination. The node which does not have any connection to the destination node will put the address of the destination node in to the list and send the RERR to the other nodes. Then other nodes will check out for the route to the destination node by checking the route map and current list of RERR. If there is not any route present in the table then the RERR sent to the source node. In this way the source node gets the RERR packet.



S.A	S.seq#	B.id	D.A	D.seq#	Hop count

b.) *Packet format for AODV*

II.) BLACK HOLE

The problem of black hole attack is the serious problem that is faced by MANET's. In this attack a malicious node acts as the next node in the routing table and advertises that it is having the shortest path for the transmission of data, and then the interception of data takes place. If malicious node's reply reaches before the reply of the actual node then the forged route has been created and the denial of service, packet drop and other processes are been carried out by the malicious node. Black hole effects are of two types [11,20]:

1. ***Single Black Hole Attack***: in this type of attack an individual node acts as black hole node which hysterics into the route between source and destination. This node belongs to the data route. When any possibility of attack occur, this node make it active data route element.
2. ***Cooperative black hole attack***: as the name suggest, in this a group of nodes acts as malicious node or we can say that malicious node acts in group. Various nodes swallow the packets send by the source node. The initiative steps of this type of attack are likewise single black hole attack and afterwards a chain of attacks from different nodes has been created n therefore the networks gets corrupted easily and gradually.

Dropping attacks: we can classify the dropping attacks as *persistent and intermittent* dropping attack. An attacked connection is called the victim connection and the packets that are being dropped by the attacker are called the victim packets. There are different types of dropping pattern in each victim connection.
Periodic packet dropping (perPD)[12]: in this pattern, we would take into account the three main parameters named as (K, I, S) where K is total number of victim packets in the connection, I is the consecutive interval between two packets and S tells us about the position of the first victim packet. Take an example (K=4, I=7, S=4) it depicts that the 4th packet will be dropped, once every 7th packet and starting from the 4th packet seen by the attacker. The attacks created by the malicious nodes slow down the working of the TCP layer.

Retransmission packet dropping (RetPD): it is quite obvious that the intruder will drop the retransmission of specific packet. In this pattern K and S will be taken into consider ability. As S denotes the victim packet K is the number of times the dropping of retransmission packet. For instance a pattern is (3, 8) then the attacker will drop the 8th packet and retransmission will be done 3 times. When the retransmitted packet lost, then the TCP slows down and exponentially start to back out its value. This value is known as (retransmitted timeout value) RTO. We can say that after some consecutive retransmissions being dropped, the destination node has to wait for long time. This period is known as idle period. No packets send in this period.

***Random packet dropping (RanPD)**:* this is also known as natural dropping. These patterns have limited number of effect on TCP's performance. Because in this pattern intruder will randomly choose the value of K which has to be dropped.

III) DETECTION AND PREVENTION SCHMES OF BLACK HOLE ATTACK IN AODV:

A.)Detection, prevention, and reactive AODV (DPRAODV): [13] the concept of ALARM is used in this technique while in other techniques the dynamic threshold value has been used. The RREP sequence number is being checked whether it is higher than the entrance value or not. If the RREP sequence number is higher than the entered vale. Then the sender is considered as an attacker and the name of the node is updated in the black list and the ALARM is being broadcasted to its neighbors who are having the black list. As a result from the all phenomena the RREP from the malicious node is blocked. DPRAODV are highly used to detect the black hole and as well as it we used to prevent the black hole attack by updating the entrance value. The advantage of using this technique that is offers us a higher packet delivery ratio than the actual AODV. The disadvantage of this technique is that it is used to find the single black holes rather than the cooperative black holes

***B.)Neighborhood based and routing recovery scheme**:* [14] This technique is used to create the reliable path to the destination and it also discovers the black hole effect. In this method, we will encounter the black hole by two methods: detection and response. We will simulate it with ns2 and come to know that there is not even a problem of overheads. Neighborhood based method is used to detect the black hole and used to identify the nodes which are not confirmed and the routing recovery scheme is used to build the correct path. In this scheme modify route entry is being send by the source node to create the new path. In this particular scheme the time for detection is small and the throughput is comparatively high. This scheme does not work under the conditions where the cooperative black hole attack is forged.

***C.)REWARD** [15] **against malicious nodes**:* REWARD (receive, watch, redirect) basically a routing algorithm in which we use a distributed database for the detected black holes attacks. This database keeps the record for the areas and nodes which are supposed to be suspicious. Two types of messages are being used by this technique names as: MISS and SAMBA. When the destination receives any query then it send the RREP to the source node. Assume that the destination nodes do not receive the packets within a specified time then the destination node broadcast a MISS message (material for intersection of suspicious sets). The destination nodes will copy entire nodes which are involved in the query message to the MISS message. The most probable reason for not getting the packet is the black hole attack. Nodes that are listed under the MISS message are suspicious nodes all the nodes will collect the MISS message and they start to intersect the misbehaving participant nodes in the route. Another reason for not receiving the packet may be collision but the proper organization of nodes can tackle this problem. But the problem arises in dense network where the suspicious nodes may get avoided. This problem can be overcome by path matrices. The path with the highest metric should be selected. If after some destinations the destination nodes receives the same data packets. Each node is transferring the packets to both immediate neighbors. One node is forwarding and one node is back warding. If nay node performs a black hole attack and drops the packet it will surely be detected by the next node in the path. The watcher will wait for a time period and then transmit the packet by changing its path along with broadcasting the SAMBA (suspicious area mark a black hole attack) message. SAMBA message provide the location of the black holes attack.

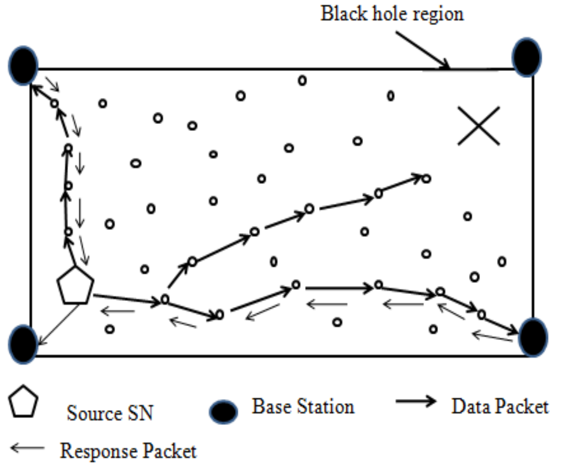
D.) Distributed cooperative mechanism (DCM** [16]**): this technique is used to mitigate the problem of collaborative black hole attacks. As the nodes are working with collaboration so this can detect the multiple black hole attack. The DCM is consists up of four sub modules named as local data collection, local detection, cooperative detection, global reaction. In the local data collection phase a table is designed and maintained by each n every node in the network. Overhearing packets are being determined by the nodes to evaluate whether there is malicious node is present or not. If one suspicious node is detected, then the check packets are being sent to the cooperative nodes. If the value of inspection is positive then the suspected node is remarked as the normal node otherwise the detection node starts the cooperative detection procedure and makes a notification to all the neighbors to participate in the decision. Network traffic is going to be increased in this method. Task for the global reaction phase is to execute a notification system and send warnings to all the nodes in the network. There are reaction modes in the global reaction phase; the first reaction phase notifies all the nodes in the network. Along with this overhead communication is being lost. Each node is concerned with its own black hole list and makes other transmission path through other node. The advantage of this technique is that it offers us a higher data delivery ratio.

E.) Intrusion detection system (IDS): It is the detecting mechanism which is used to detect the attacks against the wireless sensor networks. Intruders may be legitimate users or from outside the network. Intrusion detection system looks for attack signatures, which are specific patterns that usually indicate malicious or suspicious intent. The main designs that are for intrusion detection system are: the misuse detection design, hot based, network based and the anomaly detection design. Intrusion can be done through buffer overflows, unexpected combination, unhandled input and race conditions. Anomaly based IDS [17] is the usage of network with noise characteristics. Anything that would be distinct from the noise would be regarded as an intrusion activity. The disadvantage of this design model is that sometimes it may create the false alarms and hence the effectiveness would be compromised. The signature based IDS is programmed to interpret a certain series of packets. Most signature analysis is based on pattern matching algorithms. In this method, IDS looks for the sub string within a stream of data and carried out by packets. And it identifies those network packets as vehicles of attack.

F) REACT: This technique is used for finding out the collaborative black hole attack in the MANET's. It identifies individually the misbehaving nodes in the network that refuses to carry the data because that node is suspicious or malicious node. We can assume that there are two node disjoint path in any network. The identity of each node which is engaged in the path is known to the source. And then the pair wise key is used to protect the communication between the source and the intermediate node. Let's take an assumption that there are k intermediate nodes on the path between S to D. As in reactive method, when any packet drop occurs the destination node will reply back to the source node about the packet drop. Source node will select a node ni and verify that it correctly receives the packet from the previous hop. Source node will send an audit request through another path which is not same as the previous one. Audit request identifies a group of packet sequence number and ni will be asked to generate the behavioral proof by using the bloom filters Then the behavioral proof of the packets will be generated by using bloom filter. Bloom filter [18] is much smaller than the length of the whole packet. After generating the behavioral proof in signs the request and send it to S. the source node will generate its own behavioral proof based on the selected packets .then the comparison of both the behavioral proofs is done one behavior proof is from s and other is from ni .if the proofs are similar then S concludes that the misbehaving node is in between ni to D. And if it is not so then the misbehaving node will b in between S to ni This approach will not store the overheads and large communication. The process is continued till the two neighboring nodes are left in the suspicious set.

G.) DRI and cross checking: this technique is used to find out the collaborative or we can say that cooperative black hole attack in MANET's. In this technique the AODV is enhanced with an additional feature known as DRI table (data routing information).in these two additional requests are being added known as FREQ FREP [19]. Each node will maintain its own DRI table. 1 represents for true and 0 stands for false. The keywords of this technique are "from" and "through" means from which node data is coming n through which node the data is coming. The entry 1;1 in the table implies that the node 1 has successfully transmitted the data from or through node5. The entry 0;0 means that the data is not routed successfully from and through node 3. Let us create a scenario, where SN stands for source node IN stands for intermediate node NHN stands for next hop node.SN will broadcast RREQ and will get back RREP from the node and packets are being sent to that node. Intermediate node sends next hope node and DRI table to the source node. In the next step, the SN crosschecks its own DRI table with the DRI table that has been sent through the intermediate node to check the honesty of the intermediate node. SN will send request to the intermediate node's next hope node and asks for the routing information including the NHN, the NHN's DRI and its own DRI table. In the last step comparison is being done by the source node to find out the presence of the malicious node in the route. The disadvantage of this scheme is that the mobile nodes have to maintain extra database for the past routing information.

H.)Multiple base station technique for finding black hole attack: It is very advantageous to use multiple base stations in WSN [20]. The advantage by using the multiple base stations are decrease in energy consumption, scalability will be highly achieved and gradual computing accuracy with high accuracy. Instead of transmitting the data through the network we will send the agents through the network. the importance is more for the data delivery to the base station than to prevent the data capture by adversary .we are emphasizing on the packet delivery to the nodes which can be done by having various base stations to improve the likelihood of packets from the source node reaching at least one base station in the network. It will ensure us high packet delivery ratio. Multiple base stations to handle the flow of large amounts of, heterogeneous data from the network and several Optimization techniques have been designed for query Allocation and base station placement. So by using the multiple base stations we can maximize the delivery ration in the presence of the black holes. Source node can route the data packets to all the base stations in the network. Base stations are connected over by the wired network. We assume that the SNs in the network can be compromised by an external adversary and programmed to analyze the packets they receive and drop them instead of forwarding them to the BSs. We refer to a compromised SN as a black hole node. The adversary is capable of compromising more than one SN in the network, thus creating one or more black Hole regions. In addition, the compromised nodes are capable of colliding with other compromised nodes in their neighborhood or in other black hole regions to analyze the captured packets. We assume that the SNs in the black hole region do not perform their environment sensing tasks as they are compromised.



c.) Data delivery success improved with multiple base stations [21]

I.)BAAP (black hole avoidance protocol): we can detect the black hole attack in the network without using any external hardware. This protocol proposes ad hoc on demand multipath distance vector (AOMDV) .Correct path is established by the nodes by having proper legitimacy with the neighboring nodes. Intermediate node will create a route in which that node will not participate whose legitimacy ratio value is more than the threshold value. The packet loss in AODV is 90% while in BAAP [22] it is 15.6% to 21.3% in the presence of two three malicious nodes.

J.)Honey pot scheme of detection [23]**:** In honey pot detection scheme, topological knowledge is used to detect the spurious advertisement of routes. Trip of the network is done by some deployed roaming soft wares and luring of attackers is being done by sending route requests advertisement. This is how; enough valuable knowledge is collected by using intrusion logs. But the drawback of this algorithm is that it is not for MANET this is used by WMN as it is not proactive phenomena and the honey pot is not having the centralized authority.

IV) SOME OTHER TECHNIQUES TO DETECT AND MITIGATE THE EFFECTS OF THE BLACK HOLE ATTACK:

SAODV*:* it represents the solution to the black hole attack ad hoc on demand vector routing. In solution AODV the source node will not send the data packets instantly in fact the source node wait for the other route replies from the other neighboring nodes until the threshold time remains active. CRRT (collect route reply table) is used for collecting all the route replies. Then in CRRT, it is checked that there is any repeated next hop node is present or not. If the next hop node is there in the CRRT then it would be safe to transmit the data packets.

Real time monitoring*:* in this method we will check the neighbors of the RREP node creator and these are known as suspected nodes. Now it's the duty of the neighbor node to visualize the packets send by the suspected node. Neighbor node is counting two counters named as F count and R count. Addition of 1 takes place in the f count counter, when the neighbor node sends the packet to the suspected node. Now overhearing takes place by neighbor node when the suspected node will forward the packet and the r count is increased by the value 1. If the source node is receiving RREP from the node, it sends the data packets over the path to know that the node is malicious or not. Neighbor node is sending the packets to the suspected node till the f count reaches to the threshold. And when the r count becomes zero, RREP creator is identify as the malicious node and is blocked in the network.

Detect and overcome black hole effect*:* we can detect and overcome the black hole effect by modifying the original AODV. The node who originates the RREP must be honest. If the node is first to receive the RREP it may send directly it to the source node based on the opinion of the neighbors of RREP originator nodes. The neighboring nodes are requested to send an opinion about the RREP originator nodes. After receiving the reply, the source node comes to know that this is an honest node because RREP originator nodes have delivered many packets to the destination. If RREP originator nodes are having many received packets but do not move it further and the RREP packets are more in number then this node may also considered as the misbehaving node.

Comparison of destination sequence number: This method is used to prevent black hole effect in the AODV: All the RREP's from all the intermediate nodes are collected by the source node. The entry received by the source at the very beginning is marked as first entry in route reply table. The destination sequence number which is supported by the first entry is compared with the source sequence number. Now, if the sequence number is very less than the destination sequence number of the first entry then the node is to be considered as the malicious node. And this node is removed from the table. Now the path is selected from the remaining entries that are arranged in order by DSN. The node which is having the highest DSN is selected for route.

Secure route discovery to avoid black hole effect*:* in this method, different threshold values are assigned for different environmental conditions like small large and medium. The threshold value that is assigned to the environments is having some percentage of maximum sequence number. Two extra function units are being added to this first one is that the source node is using the threshold value to check the RREP from the neighboring nodes and second unit is that the destination node use the threshold value that is defined to check the RREQ message from the source node. If the destination sequence number of RREP exceeds its value from the threshold value then the node is considered to be malicious node

Calculation of peak value to detect black hole effect*:* during the route discovery process malicious nodes are being detected. In this process three parameters are being used that are 1.RREP sequence number 2. Routing table sequence number 3.number of replies received during the tome interval. Peak value is the maximum value of any RREP sequence number. If the peak value is less than the RREP value then that node is considered as the malicious node

V.) PROPOSED METHODOLOGY

We are proposing a solution to overcome the consequences of black hole effect by using the HOOSC scheme. In this proposed solution we are encrypting the data first and then send the data to the destination node. By using this technique intruder nodes cannot retrieve the information stored in packets. Multi hop routing technique is being used in the HOOSC scheme which means that the transmission of packet from source to destination is done through the intermediate nodes. HOOSC [24] scheme allows the sender in the identity based cryptography to send a message to the public key infrastructure. We are using 5 algorithms in this scheme. Those five algorithms are named as below:

a.) SET-UP
b.) IBC-KG
c.) PKI-KG
d.) Off-sign crypt
e.) On-sign crypt
f.) Unsigncrypt

VI.) CONCLUSION AND FUTURE WORK

In mobile ad hoc networks, the attacks always degrade the service of the entire network. Black hole attack is the attack which is performed with confidentiality in WSN. We have proposed efficient and simple approach to mitigate the effect of the black hole by using multiple base stations with encryption algorithm. In this paper we have proposed different type of prevention and detection techniques. For future work, we should encrypt the data in well efficient way that even if the drop age of the packet occurs, the data should be secure and authenticated enough and cannot be lost or damaged during the transmission. HOOSC scheme is used to done this task in an efficient way. This paper has focused on the numerous researches done in term of black hole attack for future work, to find an effective system which would present the black hole attack as well as give better performance by enhancing various parameters.

ACKNOWLEDGEMENT

I express my sincere gratitude to my guide Mr. Gunjan Gandhi assistant professor ECE department (lovely professional university) for his valuable guidance and to other faculty members for their continuous support and encouragement.

REFERENCES

[1] Xiaobing Zhang, S. Felix Wu, Zhi Fu, Tsung-Li Wu," Malicious Packet Dropping: How It Might Impact the TCP Performance and How We Can Detect It".

[2] Payal N. Raj and Prashant B. Swadas." DPRAODV: a dynamic learning system against back hole attack in AODV based" In: " international journal of computer science Vol. 2, 2009".

[3] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao "A survey of black hole attack in wireless mobile ad hoc networks" In: "2011 , human centric computing and information sciences; a Springer open journal".

[4] Z. J. Hass and M. R. Pearlman, "Zone Routing Protocol (ZRP)", Internet draft available at www.ietf.org.

[5] D. Bertsekas and R. Gallager, "Data Networks" Prentice Hall Publ., New Jersey, 2002.

[6] V. Park and S. Corson, Temporally Ordered Routing Algorithm (TORA) Version 1, Functional specification IETF Internet draft, http://www.ietf.org/internet-drafts/draft-ietf-manet-tora-spec-01.txt,1998.

[7] P.Samundiswary and P.Dananjayan. "performance analysis of trust based AODV for wireless sensor networks" In: "international journal of computer applications Volume 4– No.12, August 2010".

[8] Mangesh Ghonge, Prof. S. U. Nimbhorkar " Simulation of AODV under black hole attack in MANET" In: "international journal of advanced research in computer science and software engineering" ISSN: 2277 128X.

[9] Sakshi jain."Review of prevention and detection methods of black hole in AODV based mobile ad hoc networks" In: " international journal of information and computation technology Volume 4, Number 4 (2014), pp. 381-388".

[10] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto. "detecting black hole attack on AODV based mobile ad hoc network by dynamic learning method" In: "international journal of network security Vol.5, No.3, PP.338–346, Nov. 2007 ".

[11] Nidhi Chhajed and Mayank Sharma. "Detection and prevention schemes for black hole attack in WSN" In: "international journal of advanced research in computer science and software engineering Volume 4, Issue 11, November 2014".

[12] Xiaobing Zhang, S. Felix Wu, Zhi Fu, Tsung-Li Wu," Malicious Packet Dropping: How It Might Impact the TCP Performance and How We Can Detect It".

[13] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao "A survey of black hole attack in wireless mobile ad hoc networks" In "2011 , human centric computing and information sciences; a Springer open journal".

[14] Amin Mohebi and Prof.Dr.simon scott." A survey on mitigation methos to black hole attack on AODV routing protocol" In: "Vol.3, No.9, 2013 ISSN 2225-0603 (Online), www.iiste.org network and complex system".

[15] Zdravko Karakehayov(University of Southern Denmark Mads Clausen Institute)" Using REWARD to detect the black hole attack in WSN" .

[16] Chanchal Aghi and Chander Diwaker." Black hole attack in AODV routing protocol" In: "international journal of advanced research in computer science and software engineering Volume 3, Issue 4, April 2013 ISSN: 2277 128X ".

[17] Mozmin Ahmed and Md. Anwar Hussain . "performance of an IDS in an ad hoc network under black hole and grey hole attacks".

[18] Weichao Wang, Bharat Bhargava and Mark Linderman. " defending against collaborative packet drop attacks on MANETs" .

[19] Chander Diwaker, Chanchal Aghi and Kulvinder Singh." Detection and prevention of black hole attack in MANETs" In: "international journal of emerging technologies in computational and applied sciences ISSN (Online): 2279-0055 "

[20] Ms.B.R.Baviskar, Mr.V.N.Patil. " black hole attacks in wireless sensor network by using multiple base station using of efficient data and encryption algorithms" In: "international journal of advent research in computer and electronics". Multiple bs

[21] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard. " prevention of cooperative black hole attack in wireless ad hoc networks".

[22] Jaspreet kaur and bhupinder kaur .” BHDP using fuzzy logic algorithm for WSN under black hole attack” In : “international journal of advanced research in computer science and management studies,Volume 2, Issue 9, September 2014,”.

[23] Amanpreet Kaur, Manjot Kaur Sidhu.” Diminution of MANET attacks by HOOSC scheme” In: “International journal of science and research”.

[23] Anjaly Joy and Sijo Cherian.” Black hole attacks and its mitigation techniques in AODV and OLSR “In: “ international journal of computer science and engineering technology”.

[24] Bhoomika patel and khusboo trivedi.” A review-prevention and detection of black hole attack in AODV besed on MANET” In: “international journal of computer science and information technology”ISSN:0975-9646

[25] Ms. Twincle G. Vyas and Mr. Dhaval J. Rana.” Survey on black hole detection and prevention in MANETs” In:”international journal of advanced research in computer science and software engineering”.

.