A Brief Review of Routing protocols on Mobile Ad-hoc Network

Sonam Choubey[1], Krishna Kumar Joshi[2]
[1, 2] Department of Computer Science Engineering
[1, 2] MPCT, India

Abstract- *Mobile Ad-hoc Networks is a wireless network of mobile nodes communicating with each other in a multi-hop manner without the support of any fixed infrastructure such as base stations, wireless gateways or entry features. MANETs allow wireless networking in environments where there is no wired or mobile infrastructure. Due to dynamically changing topology, open atmosphere and absence of centralized infrastructure MANET's are at risk of many attacks. So in (MANETs), safety is among the principal issues.*

Keywords—MANET; AODV; DSR; RREQ; RREP, etc.

I. INTRODUCTION

A mobile ad hoc network (MANET) is an spontaneous network that might be set up with none consistent infra-structure or a topology. As a result of this every one of its nodes act as routers and partake in its revelation and remodel of routes i.e. Nodes within each and every other's radio variety keep in touch straight via wireless links, even as those that are not in every other's radio variety use other nodes as relays[1] . The term ad hoc implies that this network is based for an exact, more often than not extemporaneous service customized to detailed applications. MANETs permit wireless networking in environments the place there is not any wired or cellular infrastructure; or, if there's an infrastructure, it isn't sufficient or cost potent [2].

MANETs offer two or three favourable circumstances over customary networks together with lessened framework costs, simplicity of foundation and fault tolerance, as routing is carried out in my view by means of nodes using different intermediate network nodes to forward packets, this multi-hopping reduces the risk of bottlenecks, however the important thing MANET appeal is greater mobility when compared with wired solutions [3].

II. CHARACTERISTICS OF MANET

The topologies between the nodes are altering regularly.

The communication medium is broadcast and connection of exclusive nodes is wireless.

The Nodes are permitted to communicate with any another node. Because of the occurrence of attacker nodes, the reduction in the performance is happen [4].

III. SECURITY CHALLENGES & ISSUES OF MANETS

MANETs use wireless media for transmission, which introduces security flaws to the networks. Basically any one with the proper equipment and knowledge of the current network topology and the protocols may obtain access to the network. Both active and passive attacks like impersonation, eavesdrop-ping, message redirection, and traffic analysis, can be per-framed with the guide of a adversary.

In specific scenarios, MANET nodes may be scattered over a large area. Some nodes or network components may be un-monitored or hard to monitor, and exposed to the physical attacks.

On account that MANETs should not have any significant authority, this can be a important barrier to safety. The security mechanisms employed in wired networks, such as Public Key Management, Node Authentication, and Determination of Node Behaviour, are in fact very difficult to achieve without any central administration.

Ad hoc networks are highly dynamic in nature. Node joins and departures are not predictable. Moreover, network topology is perpetually changing in ad Hoc networks [5].

IV. MANETS ROUTING PROTOCOLS

Routing is vital in MANET; however it create problem and Challenges as compared to the routing in fixed infrastructure. The concern in routing is as a result of the swiftly changes in the topology of the nodes and the gadgets. Mainly there are three types of routing are present i.e. proactive routing, Reactive routing and Hybrid routing.

There is a fixed topology are used as a single protocol in *Proactive routing*. The proactive routing protocols are OLSR and DSDV.

In Reactive routing, there's a number of protocol are used between the 2 instruments and the variety of topology is exchange consistent with the condition. AODV and DSR are the reactive routing protocol [4].

In Hybrid routing, they mix points from each reactive and proactive routing protocols, usually trying to milk the diminished manage visitors overhead from proactive techniques even as lowering the route discovery delays of reactive systems by using keeping some type of routing desk [6]. The hybrid routing protocols are TORA and ZIP.

V. MANET VULNERABILITIES

Vulnerability is a weak point in safety process. A specified process is also susceptible to unauthorized information manipulation considering the procedure does not affirm a consumer's identification earlier than Permitting information access. MANET is extra susceptible than wired neighborhood. One of the vital vulnerabilities are as follows:-

a) Lack of centralized management:

MANET doesn't have a centralized screen server. The absence of management makes the detection of attacks elaborate for the reason that it's not east to monitor
The traffic in an incredibly dynamic and colossal scale ad-hoc community.

b) Resource availability:

Resource availability is a most important difficulty in MANET. Supplying cozy communiqué in such altering atmosphere as good as safeguard towards special threats and attacks, results in progress of more than a few security schemes and architectures. Collaborative ad-hoc environments additionally permit implementation of self-organized protection mechanism.

c) Scalability:

because of mobility of nodes, scale of ad-hoc network altering always. So scalability is a essential difficulty related to safety. Security mechanism must be able of handling a colossal community as good as small ones.

d) Cooperativeness:

Routing algorithm for MANETs typically assumes that nodes are cooperative and non-malicious. Consequently a malicious attacker can conveniently turn out to be a principal routing agent and disrupt network operation by means of disobeying the protocol specifications.

e) Dynamic topology:

Dynamic topology and changeable nodes Membership would disturb the trust relationship among nodes. The trust can also be disturbed if some nodes are detected as compromised. This dynamic behaviour could be higher covered with allotted and adaptive security mechanisms.

f) Limited power supply:

The nodes in MANET have got to do not forget constrained power give, which will reason a couple of issues. A node in cell ad-hoc network could behave in an egocentric manner when it's discovering that there's only limited energy supply.

g) Bandwidth constraint:

Variable low knowledge hyperlinks exists as compared to wireless network which are extra inclined to outside noise, interference and signal attenuation outcome.

h) Adversary inside the Network:

The mobile nodes throughout the MANET can freely become a member of and depart the network. The nodes within community may also behave maliciously. That is tough to notice that the behaviour of the node is malicious. As a consequence this attack is more detrimental than the external attack. These nodes are known as compromised nodes.

i) No predefined Boundary:

In MANET we cannot precisely outline a bodily boundary of the community. The nodes work in a nomadic environment the place they're allowed to become a member of and depart the wireless community. As soon as an adversary comes within the radio range of a node it'll be in a position to keep up a correspondence with that node. The attacks include Eavesdropping impersonation; tempering, replay and Denial of service (DoS) attack [5].

VI. ATTACKS

A. Black hole attack [6,7,8]:

A black hole node is a malicious node that sends a false reply with an it appears valid path to the destination node

It replies each single RREQ with false sequence number, so it acquires the route, after which eavesdrops or drops all knowledge packets that go by means of it.

Single Black Hole Attack: Only one node act as malicious or cooperated node which misbehaviour with the network in Single black hole attack. It is regularly alluded to as black hole attack with single malicious node.

Collaborative Black Hole Attack: More than one nodes acts as malicious node in the group and works in co-agent way in Collaborative black hole attack. Sometimes called black hole with a couple of malicious nodes.

B. Gray hole attack (selective black hole) [7,8]:

Appears like a black hole attack, however a malicious node randomly changes its state between common node and black hole node. For that reason, gray hole is tougher to be detected by security strategies.

Grey hole is a node that may change from behaving thoroughly to behaving like a black hole that is it is without a doubt an attacker and it'll act as a common node. With a view to identify quite simply the attacker considering it behaves as an ordinary node. Each node keeps a routing table that stores the next hop node working out which is a route packet to destination node [8]. If a supply node is in have got to route a packet to the destination node it uses a specific route and it will be checked in the routing desk whether it's to be had or not. On the off chance that a node starts a route discovery handle by method for broadcasting Route Request (RREQ) message to its neighbor, with the guide of accepting the route request message the intermediate nodes will replace their routing tables for reverse path to the supply [9]. A route reply message is shipped back to the source node when the RREQ query reaches both to the vacation spot node and to another node which has a present route to endpoint.

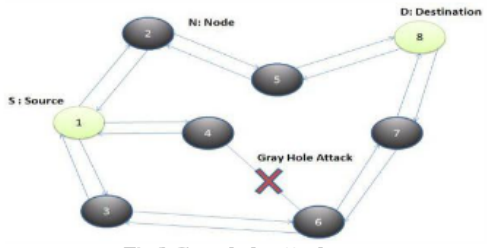

Fig.1 Gray hole attack

The grayhole attack has two phases:

Phase 1:

A malicious node exploits the AODV protocol to advertise itself as having a legitimate path to vacation spot node, with the intention of interrupting packets of spurious route.

Phase 2:

In this section, the nodes has been dropped the interrupted packets with a specified probability and the detection of grey hole attack is a difficult approach. By and large in the gray hole attacks the attacker acts maliciously for the time with the exception of the packets are dropped after which change to their standard propensities [10]. Both traditional node and attacker are identical. As a result of this behavior it is very rough to discover in the network to determine such variety of attack.. The inverse recognize for grey hole attack is node making misbehaving attack.

C. Cooperative black hole attack [11,12]:

Two nodes or more on this attack cooperate to obtain the path between the source and the vacation spot nodes. When one node good points the path selectively drops or forwards the info packets to considered one of its cooperating nodes. Cooperation between black hole nodes helps malicious nodes to flee from monitoring procedures.

Black hole attack disturbs the routing protocol by misleading other nodes concerning the routing understanding. A black hole node works inside the accompanying plan: once accepting RREQ and RREP messages, the attacker answers RREP messages in a split second and claims that it's the destination node. The supply node is more likely to obtain a pseudo-RREP from the attacker before the actual RREP returns. Beneath these conditions, the supply node sends knowledge packets to the black hole as a substitute of the destination node. When the supply node transmits knowledge packets via the black hole, the attacker discards them without sending again a RERR message. As for gray hole, its routine are just like a black hole. A gray hole does now not drop all data packets however simply part of packets. The grey Magnitude is outlined because the percentage of the packets which can be maliciously dropped via an attacker. For representation, a gray hole is dim extent of 60% will drop a data packet with a chance of 60% and an established black hole has a gray size of 100%. The black and grey hole attack [13] will deliver great harm to the efficiency of advert Hoc network. The malicious drop cost is outlined by way of the ratio of dropped packet number and obtained packet number. Exceptionally, the malicious drop expense of a black hole is 100%.

VII. EXISTING TECHNIQUES

A. Intrusion Detection Systems

Intrusion Detection methods (IDS) [15] are one of the vital basic techniques in use to avoid any attacks against protection threats. Intrusion detection can be arranged as group based IDS and host based IDS. Network founded IDS (NIDS) may also be set up on information awareness points of a network such as switches and routers. It screens site visitors at chosen points on a community (like the switches, routers, and so on) or the interconnected set of networks. The NIDS filters the traffic packet by way of packet, in order to attempt to decide the intrusion patterns. The NIDS additionally scrutinizes network-degree, transport-stage or software-degree protocol motion not like a host-founded IDS; a NIDS inspects packet traffic that's heading toward probably inclined laptop methods on a network.

B. Route Confirmation Approach (RCA)

In [16], the authors introduce the route confirmation request (CREQ) and route affirmation reply (CREP) procedure to restrict the black hole attack within the community. In this strategy, the intermediate node not only sends RREP messages to the source node but additionally sends CREQ messages to its next-hop node toward the vacation spot node. This is to investigate about the route to the destination node. After receiving a CREQ message, the following-hop node searches its cache for a route to the destination. If it has the route, it sends the CREP to the source. On receiving the CREP message, the source node confirms the validity of the route via evaluating the route in RREP message and the one in CREP. If each are the equal, the supply node confirms that the route is correct. One trouble of this technique is that it can't preclude the black hole attack in which two consecutive nodes work in agreement with every other, that's, when the next-hop node is an attacker working in conjunction with the malicious node sending CREPs that aid the flawed path.

C. Multiple Route Replies (MRR)

In [17], the authors have discussed the AODV protocol that suffers from the Black hole attack in MANETs and has proposed a sensible answer for the black hole attacks, which may also be applied on the AODV protocol. This mechanism expects a supply node to wait except an RREP packet arrives from greater than two nodes. Upon receiving multiple RREPs, the supply node assessments whether or not there is a shared hop or no longer. If there's, the source node confirms that the route is secure and can be utilized. The essential main issue of this solution is that it introduces time delay, for the reason that it has to wait except multiple RREPs arrive.

D. Statistical Anomaly Detection (SAD)

In [18], the authors examine the consequences of black hole attack in MANETs and shows that a malicious node have got to expand the vacation spot sequence number properly to steer the supply node that the route furnished is amply adequate. Headquartered on this investigation, the authors propose a statistical situated anomaly detection technique to observe the black hole attack within the network, founded on the difference between the vacation spot sequence numbers of the a couple of bought RREPs. The competencies of this approach is that it will probably notice the black hole at low fee without launching further routing site visitors, and it does not require any change of the present protocol. Nevertheless, false positives, the place the malicious node raises a false alarm indicating that a given situation has been fulfilled when it genuinely has now not been, are the most important quandary of this procedure due to the nature of anomaly detection.

E. Further Request Approach (FRA)

In [19], according to the authors‟ answer, when any intermediate node replies for an RREQ message, knowledge concerning the next hop to the vacation spot will have to be included within the RREP packet. The source node then sends a different request (FREQ) message to the next hop of the node that replied to the RREQ message and asks about the node that answered as well as the path to the destination. By means of using this approach the credibility of the responding node can also be identified, provided that the following hop is trusted. However, this solution are not able to avert cooperative black hole attacks on MANETs. For illustration, if the following hop additionally obliges with the replied node, the reply for the FREQ will likely be readily answered “sure” for both the questions. Then the source will think the next hop and transmit data through the replied node which is a black hole node.

F. Prior - Receive Reply Method

The paper [14] proposes an algorithm that identifies the malicious node which is responsible for the black hole attack. On this system we will verify whether there's any gigantic change between the sequence quantity of the source nodes and intermediate nodes who has despatched back RREP messages or not. Naturally, the first route reply within the routing desk shall be from the malicious node with high destination sequence quantity. The first destination sequence

quantity will also be when put next with the source sequence quantity. If there exists so much difference between source and vacation spot sequence number, then the vacation spot node is a malicious node, allowing the elimination of that entry from the routing table instantly. This is achieved as 5 distinctive procedures which comprise the initialization method, storing process, identification and removing of the malicious node, node determination process and in the end the default procedure.

Technique	**Objective**	**Scalability**	**Efficiency**
IDS	Monitors data callers at information awareness facets	Controlled to data awareness points	Mostly for probably inclined programs
RCA	Prevents false routing know-how from getting into the network	Will also be applied handiest to prevent one malicious node	Efficient in terms of one black hole node
FRA	To establish the credibility of the responding node	Scalable to any community where each node has trusted neighbors	not compatible for cooperative attacks
MRR	Detecting and removing black hole nodes in the MANET on the initial stage itself without any delay.	Scalable as it covers the security of greater than two nodes	Inefficient in terms of time prolong
SAD	finding of High accurateness	Adaptive even in a altering community environment	Effective except for false positives

VIII. LITERATURE SURVEY

In this survey MURTHY et al[21] MANETs form a temporary network of mobile nodes, which is infrastructure less. In this network, intermediate nodes cooperate and act as a router and send messages from one node to a different. It is quite useful in situations where we have lack of fixed network infrastructure, such as an emergency situations or rescue operation, medical assistance, disaster relief services, mine site operations, and military mobile network in battlefields. [21] MANETs are having issues of dynamically changing network topologies, no infrastructural support, and restricted bandwidth. For researcher it has been quite an interesting research area in designing a routing protocol discovering the best possible route in a dynamic environment of MANET's.[21]

VISHU et al. [22] Ad hoc on-demand distance vector(AODV) routing protocol uses an on demand approach for searching routes, that route is established only when it is required by source node for transmission of information bundles. It applies a destination sequence numbers to recognize the most recent late way. In an AODV, the source node broadcasts the RREQ message in the network when the route is not available for the destination. [22]]A node revive its way data just if the Destination Sequence Number of the present packet got, is more prominent than the last DesSeq Num put away at the node. At the point when any of middle of the intermediate nodes gets a Route Request, it either advances or gives a Route Reply, in the event that it has a substantial route to the destination.

Onkar et al. [23] proposed that Gray hole is one of the attacks initiate in ad hoc network. This acts as a slow toxic in the network. Hence, we can't assume how much data can be lost. In gray hole Attack [23], a malicious node wastes to lead certain bundles and just drops them. The assailant specifically drops the packets beginning from a solitary IP address or a scope of IP addresses and advances the rest of the packets. Grayhole nodes in MANETs are extremely viable. Each node saves a routing table, which keeps the following next hop data for a route a packet to destination node. At the point when source node needs to highway a packet to the destination node, it utilizes a specific course if such a course is accessible in its routing table.

Jhaveri et al. [24] proposed AODV protocol, when node receives a route reply packet (RREP), it checks the sequence number in routing table. In the event that the sequence number is more prominent than the one in the RREP, the RREP packet is acknowledged else it is disposed of. The route discovery prepare in this is done within the sight of a malicious node. [24] Source node broadcasts route request packet (RREQ) to the nodes within its neighborhood area or sort communication range. At the point when neighbor node get the RREQ and rebroadcasts RREQ to their neighbors until a node having a substantial course to the goal or goal itself gets RREQ bundles. This node sends RREP to the source node on the reverse path on which RREQ sent. The malicious node

sends RREP with higher yet manufactured sequence number to the source. Also, another RREP is sent by destination node, having really higher sequence number.

Deepali et al. [25] proposes the security methodology is invoked by a node when it establishes a suspicious node by looking at its DRI table. The node that starts the suspected node acknowledgment strategy is known as the Initiator Node (IN). The IN first picks a Cooperative Node (CN) in its district, in light of its DRI records and communicates a RREQ message to just its 1- hop neighbors asking for a route [25] In answer to this RREQ message the IN will get various RREP messages from its adjacent nodes. It will get a RREP message from the Suspected Node (SN) which, the last is truly a dim opening. As RREP is gotten from the SN, the IN sends a question bundle to the CN through the SN. After an ideal opportunity to live estimation of the question bundle is over, the IN checks the CN whether it has gotten the query packet or not. In the event that the answer to this question is certain, then the IN changes its DRI table. [25] However, in the event that the query packet is observed to be not came to the CN, the IN expands its level of doubt about the SN and begins the suspicious node recognition method.

P. Agarwal proposes a approach [26], the AODV protocol is a little modified and an new algorithm is known as Credit Based AODV (CBAODV). In which, firstly each and every node assigns a permanent value for its every adjacent node as the neighbor credit value. This credit esteem is increments by the protocol when it gets a route request packet (RREQ) and reductions when it gets the route reply (RREP) packet. At the point when a node discovers negative credit an incentive for one of its neighbors, then it recognized as the grayhole attacker [26] This additionally expels all current set up ways from its routing table which is experiencing that node. Every node allots a credit esteem that we are sending the route request for and subtracting the credit esteem when we got an answer from them. This algorithm is capable to detect cooperative grayhole nodes. [26]

S.jain proposes [27] there are some additional nodes-strong nodes, which help source and destination to discover black and grayhole attacks. These solid nodes are thought to be trustful and furthermore equipped for tuning its radio wire to huge ranges and short ranges. Each normal node is inside the range of one of these strong nodes. By using the strong nodes, source and destination starts to check if the data packets have reached the destination or not. [27] If any changes found in number of messages sent from source and received at destination, strong nodes ask the nodes in their areas about the monitoring results of one node's behaviour. If the checking results show misbehaviour according to the votes, then the network runs a protocol which can detect black or grayhole attack. At last announces malicious node to the network by broadcasting messages. [27]

Yanget al.[28] SCAN utilizes two thoughts to shield AODV in MANET: Local collaboration and Information cross-approval.

- In collaboration, nodes screen each other and furthermore keep up routing tables of each other. Every node utilizes a token that approves itself to the network. In the event that one hub is suspected to be malicious, other nodes invalidate its token and ready token denial to completely nodes in network and they embed that node in their token renouncement list. So, the malicious node does not have any access to the network.
- In Information cross-approval, every node checks routing packets originated from its neighbors. Every node knows each neighbor's routing tables, which can cross-check the caught transmissions of them

IX. CONCLUSION

A mobile ad hoc network (MANET) is a spontaneous network that can be founded without any fixed infra- structure or a topology. Because of this all its nodes behave as routers and participate in its discovery and renovation of routes i.e. Nodes within each and every other's radio variety keep in touch straight via wireless hyperlinks, even as those that are not in every deferent's radio variety use other nodes as relays. The term ad hoc implies that this network is headquartered for a specified, mainly extemporaneous carrier customized to particular applications. MANETs enable wireless networking in environments the place there is not any wired or cell infrastructure; or, if there is an infrastructure, it is not ample or cost effective.

REFERENCES

[1] MeghnaChhabra, Brij Gupta, AmmarAlmomani, "A Novel Solution to Handle DDOS Attack in MANET", http// www.scirp.org/journal/jis,Vol4,165-179, July 2013.

[2] S. Parthiban, A. Amuthan, N. Shanmugam, K. Suresh Joseph, "Neighbor attack and detection mechanism in Mobile ad hoc networks" International journal of Advanced Computing,Vol.3, No.2, March 2012.

[3] Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi, "A Review of Routing Protocols for Mobile Ad-Hoc Networks (MANET)",International

Journal of Information and Education Technology,Vol.3, No.1,February 2013.

[4] Satyam Shrivastava, Sonali Jain, "A Brief Introduction of Different type of Security Attacks found in Mobile Ad-hoc Network" International Journal of Computer Science & Engineering Technology(IJCSET), Vol. 4, No. 03, Mar 2013.

[5] Geetika, Naveen Kumari, "Detection and Prevention Algorithms of DDOS Attack in MANETs", ISSN: 2277 128X, Vol.3, No.8, August 2013@IJARCSSE.ltd.

[6] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", Journal of Wireless communications, IEEE,Vol. 14, No. 5, pp. 85-91, 2007.

[7] S. Kamboj, and M. Dua, "Comparison Study of Various DoS Node Detection Schemes in MANETs", International Journal on Computer Science and Emerging Trends (IJCSET), Vol. 2, No. 1, pp. 8-15, 2013.

[8] Vishnu K and Amos J Paul "Detection andremoval of Cooperative Black/Gray hole attack in MobileAdhoc Networks" IJCA Vol.1, No.22 Jan 2010.

[9] MeghaArya and Yogendra Kumar Jain "Gary hole attackand prevention in Mobile Adhoc Network" IJCA Vol.27,No.10. Aug 2011.

[10] OnkarV.Chandure, Prof V.T.Gaikwad " A Mechanismfor recognition & Eradication of Gray Hole attack usingAODV Routing Protocol in MANET" IJCSIT , Vol.2,No.6, Jul 2011.

[11] S. Jain, J. Singhai, and M. Chawla, "A Review Paper on Cooperative Blackhole And Grayhole Attacks in Mobile Ad hoc Networks", International Journal of Ad Hoc, Sensor & Ubiquitous Computing, Vol. 2, No. 3, 2011.

[12] L. Tamilselvan, and V. Sankaranarayanan, "Prevention of co-operative black hole attack in MANET", Journal of networks, Vol. 3, No. 5, pp. 13-20, 2008.

[13] D.B. Johnson; D.A. Maltz; J. Broch; "DSR: The dynamic source routing protocol for multiple wireless ad hoc networks". In: Perkins C, Ed, Ad Hoc Networking. Addison-Wesley, 2001. 139-172

[14] Dr. S. Tamilarasan, Securing AODV Routing Protocol from Black Hole Attack, International Journal of Computer Science and Tele communications, Volume 3, Issue 7, July 2012.

[15] Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection by YibeltalFantahumAlem& Zhao HhengXaun from Tainjin 300222, China 2010, IEEE.Fröhlich, B. and Plate, J. 2000. The cubic mouse: a new device for three-dimensional input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems

[16] BounpadithKannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato; "A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOC NETWORKS", IEEE Wireless Communications • October2007.PP: 85-90.Sannella, M. J. 1994 Constraint Satisfaction and Debugging for Interactive User Interfaces. Doctoral Thesis. UMI Order Number: UMI Order No. GAX95-09398., University of Washington.

[17] Modified AODV Protocol against Black hole Attacks in MANET by K. Lakshmi1, S.ManjuPriya, A.Jeevarathinam, K.Rama, K.Thilagam, Lecturer, Dept. of Computer Applications, Karpagam University, Coimbatore, International Journal of Engineering and Technology. Vol.2 (6), 2010.Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.

[18] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto; "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007, PP:338-346.

[19] Weerasinghe.H. "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", IEEE Student Member.

[20] HizbullahKhattak, Nizamuddin, "A Hybrid Approach for Preventing Black and Gray Hole Attacks in MANET", Digital Information Management (ICDIM) Eighth International Conference, pp. 55-57, IEEE September 2013.

[21] C. Siva Ram Murthy, B. S. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols, Person Education, ISBN 978-81-317-0688-6, 2004.

[22] K. Vishnu, A. J. Paul, "Detection and removal of cooperative black/gray hole attack in mobile

adhocnetworks", IJCA(0975-8887), Vol. 1 No. 22, pp. 38-42, 2010

[23] Onkar V. Chandure, V. T. Gaikwad, "Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol", International Journal of Computer Applications(0975-8887), Volume 41- No.5, pp. 27-32, March 2012.

[24] R. H. Jhaveri, S. J. Patel, D. C. Jinwala, "A novel approach for Grayhole and Blackhole attacks in Mobile Ad-hoc Networks", Second International Conference on Advanced Computing & Communication Technologies, IEEE, pp. 556-560, 2012.

[25] Deepali A. Lokare, A.M Kanthe, Dina Simunic, "Cooperative Gray Hole Attack Discovery and Elimination using Credit based Technique in MANET", International Journal of Computer Applications (09758887), Volume 88-No.15, pp. 13-22, February 2014.

[26] P. Agrawal, R. K. Ghosh and S. K. Das, "Cooperative black and gray hole attacks in mobile ad hoc networks", In Proceedings of the 2nd International Conference on Ubiquitous Information Management and Communication,pp.-310-314,January-2008.

[27] S. Jain, M. Jain, H. Kandwal, "Advanced algorithm for detection and prevention of cooperative Black and Gray hole attacks in mobile ad hoc networks", IJCA (09758887), Vol. 1-No. 7, pp. 37-42, 2010

[28] Yang, H., Shu, J., Meng, X., and Lu, S., "SCAN: Self-organized network-layer security in mobile ad hoc networks", IEEE journal, Vol. 24-No. 2, pp. 261-273, Feb-2006.