Cooperative Intrusion Detection Technique Against Blackhole and DoS Attacks in MANET

Aasif Hasan
Dept. of Computer Science & Engineering,
Manav Rachna International University,
Faridabad, INDIA
aasifhasan@gmail.com

Suresh Kumar
Dept. of Computer Science & Engineering,
Manav Rachna International University,
Faridabad, INDIA
E-mail: suresh.fet@mriu.edu.in

M K Soni
Dept. of Computer Science & Engineering,
Manav Rachna International University,
Faridabad, INDIA
E-mail: dr_mksoni@hotmail.com

Abstract: The display of the inspiring applications from the Mobile Ad-hoc collect so much name and fame in the practical world as well as research and technologies and this is because of their self-maintaining and autonomous nature. The node can quickly able to change their places that make the network movable, which is differ from any other sort of networks. In MANETs generally, there is absence of centralized control unit. Therefore the mutual corporations within the working entities are responsible to detect the routes towards the destination. Mobile Ad hoc is extremely defenseless to attacks because of its dynamic nature of their infrastructure, Out of all these attacks, routing attacks haves grabbed much attention, As it is capable of destructive damage to MANET. But somehow according to our experience there is no protocol which is complete by their selves. Hence we concentrate on making the On Demand Adhoc Vector (AODV) better to preserve it form the blackhole attacks and DoS. We have to analysis this work process regarding many performance matrices. The given work simulates with the help of the NS2 simulator.

***Keywords*—*MANET; DoS; Blackhole; Attacks; Packet Delivery Ratio, Infected Nodes.*

I. INTRODUCTION

An ad-hoc network can change its form depending on the work on hand. A MANET is an infrastructure-less network consisting of set of mobile nodes or mobile devices wishing to communicate with each other via shared wireless medium; it does not have any centralized administration and therefore, line of defense is pretty unclear. Each node has limited communication range in the network and it node acts as a router to forward packets to another node. It is rapidly deployable and highly adaptive in nature. Nodes have high mobility and communication is done via radio broadcast medium. Therefore, MANETs are widely used in applications such as military communication by soldiers, automated battlefields, emergency management teams to rescue, search by police or fire fighters, replacement of fixed infrastructure in case of earthquake, floods, fire etc., quicker access to patient's data from hospital database about record, status, diagnosis during emergency situations, remote sensors for weather, voting systems, sports stadiums, mobile offices, vehicular computing, electronic payments from anywhere, education systems with set-up of virtual classrooms, conference meetings, peer to peer file sharing systems [1]. The characteristics of MANET along with mobility and radio broadcast medium leads to some major issues for MANETs such as IP addressing, radio interference, routing protocols power constraints, security, mobility management, service discovery, bandwidth constraints, Quality of Services (QoS), etc. [2]. Among all research issues, though, one of the essential research issues in MANETs is security; Denial-of-Service (DoS) attacks are a major class of threat today. Two of the most common DoS attacks are Grayhole and Blackhole attacks in MANET. In Blackhole attack, the malicious node generates and propagates fabricated routing information and advertises itself as having a valid shortest route to the destined node [3]. If the malicious node replies to the requesting node before the genuine node replies, a false route will be created. Therefore, packets do not reach to the specified destination node; instead, the malicious node intercepts the packets, drops them and thus, network traffic is absorbed [4]. Grayhole attack is an extension of Blackhole attack in which a malicious node's behavior is exceptionally unpredictable. A node may behave maliciously for a certain time, but later on it behaves just like other ordinary nodes. Both Blackhole and Grayhole attacks disturb route discovery process and degrade network's performance [5].

In this paper, a mechanism to detect and remove these two types of attacks is proposed. In this proposed mechanism, an intermediate node receiving abnormal routing information from its neighbor node considers that neighbor node as a malicious node. The intermediate node appends the information about the malicious node in the route reply packet and every node receiving that reply packet then upgrades its routing table to mark the node as malicious node. When routing request is sent, a list of malicious node is appended to the packet and every node receiving the packet upgrades its routing table to mark the listed nodes as malicious. Thus, a node receiving fabricated routing information finds the malicious node either by identifying false routing information or by verifying its routing table; the node then tells other nodes not to consider the routing information received from the malicious node.

The remainder of paper is organized as follows. Section II describes background work. In Section III, AODV routing protocol is discussed. Related work is discussed in section IV. Section V describe and discuss about the proposed with proposed algorithm. VI section talk and consider about the simulation and it's result analysis part.. Finally conclusion is given in Section VII.

II. BACKGROUND

Two approaches are used to provide solutions to the security issues in ad hoc networks: "Prevention" and "Detection and Reaction" Techniques. Prevention mechanism can not provide guarantee to complete cooperation among nodes in the network. On the other side, Detection approaches specify the solutions that try to identify clues of any unauthorized activity in the network and take appropriate action against such nodes. There are different approaches that have been proposed to detect and prevent selfish nodes in mobile ad hoc networks. These types of nodes save their own resources and refuse to cooperate to other nodes. So for stimulating cooperation different approaches are present. Virtual Currency Based Schemes and Reputation based schemes are that approaches [6].

The Watchdog and Path rater scheme proposed by Marti et al [6] consists of two main modules, detect and mitigate respectively. Because of the reason of overhearing this technique did not work to detect misbehavior and raise false alarms in the existence of limited transmission power & ambiguous collision.

Afterwards, Buchegger & Ie Boudec proposed CONFIDANT protocol. Its motive is to detect and isolate misbehaving nodes in ad hoc network, then making it unattractive to deny cooperation and participation. Each individual node contains four components: Monitor, Trust Manager, Reputation system and Path Manager. Later another scheme was proposed is CORE. It suggests a generic mechanism to stimulate node cooperation based on a collaborative monitoring technique. This can be integrated with any network and application layer function that can contain packet forwarding, route discovery network management, location management.

Afterwards OCEAN (Observation based Co-operation enforcement in Adhoc network) was proposed by S.Bansal et al. In comparison to CONFIDANT protocol, OCEAN uses only direct fist-hand observations of other nodes behavior. It does not use second hand reputation information.

III. AODV ROUTING PROTOCOL WITH BLACK HOLE AND DOS ATTACK

The AODV routing protocol [2] uses on-demand approach to find routes, that is, a route is established only when it is required by a source node to transmit the data packets. It employs destination sequence number to identify the most recent path. The largest destination sequence number indicates the freshest route to the destination node, which is accepted by the source node for the data transmission. The source node and the intermediate nodes store the next-hop information corresponding to each flow of data transmission. The source node floods a RREQ packet in the network when it desires to obtain a route to the destination node for data transmission. When an intermediate node receives a RREQ, it either forwards it or prepares a RREP if it has a valid route to the destination; RREP is a unicast message back along the saved path to the source node. All intermediate nodes having valid route to the destination, or the destination node itself, are allowed to send RREP to the source. This process continues until an RREP message from the destination node or an intermediate node that has a fresh route to the destination node is received by the source node. The source node may obtain multiple routes to a destination for a single RREQ. The AODV is a collaborative protocol [2] and allows nodes to distribute the information they contain about other nodes. RREQ messages may not necessarily reach the destination node during the route discovery process. If an intermediate node already knows a route toward the destination, it does not forward the RREQ any further and generates a RREP message. This enables quicker replies and limits the flooding of RREQs.

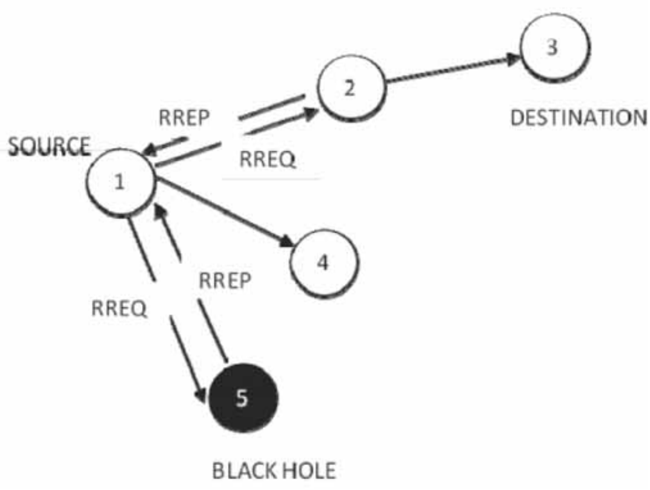


Fig. 1: Routing Discovery in AODV with Black Hole Attack

Route discovery process in AODV is vulnerable to the black hole attack [1][3][9]. The mechanism, that is, any intermediate node may respond to the RREQ message if it has a fresh enough route, devised to reduce routing delay, is used by the malicious node to compromise the system. In this attack, when a malicious node listens to a route request packet in the network, it responds with the claim of having the shortest and the freshest route to the destination node even if no such route exists. As a result, the malicious node easily misroute network traffic to it and then drop the packets transitory to it.

For example, in Fig. 1, the source node (node 1) broadcasts a route request packet RREQ to its neighbours to find a route to the destination node (node 3). It is assumed that routing table of an intermediate node (node 2) has a route to the destination node and node 5 is a malicious node in the network. When node 1 sends a RREQ packet to its neighbouring nodes (node 2, node 4, and node 5), the node 5 directly sends a fake RREP to node 1 without checking its routing table. So, the malicious RREP reaches fastest to the node 1 in comparison to the replies of other nodes in the network. Now, node 1 accepts the shortest route through the node 5 and sends application layer data to the node 3 via this node rejecting other RREP packets (in this case, a RREP packet from node 2). The source node assumes that the data would reach safely to the destination node but, in fact, the malicious node drops all data packets rather than forwarding them to the destination. The intension of implementing a black hole in the network may be as simple as disrupting the normal network operation to as severe as man in the middle attack or denial of service attack. This type of attack is first making sure that a specific node is not available for service. So the entire service of the network might be disturbed due to this attack [9].

IV. RELATED WORK

Piyush et.al [6] proposed a solution where source and destination nodes carry out end-to-end checking to determine whether the data packets have reached the destination or not. If the checking fails then the backbone network initiates a protocol for detecting malicious nodes. But, it works on assumption that any node in the network has more trusted nodes as neighbors than malicious nodes which may not be likely in many scenarios. If malicious nodes are more in numbers, this solution becomes vulnerable.

Chen et. al [7] presented a solution consisting of two related algorithms: key management algorithm based on gossip protocol and detection algorithm based on aggregate signatures. According to their solution, each node involved in a session must create a proof that it has received the message; when source node suspects some misbehavior, Checkup algorithm checks intermediate nodes and according to the facts returned by the Checkup algorithm, it traces the malicious node by Diagnosis algorithm. This solution may generate high traffic and computational cost of detection algorithm may be very high due to the basic limitations of gossip protocol and aggregate signatures.

A mechanism is proposed by Sukla et. al [8] in which before sending any block, source sends a prelude message to destination to make it aware about communication; neighbors monitor flow of traffic; after end of transmission, destination sends postlude message containing the number of packets received. If the data loss is out of acceptable range, the process of detecting and removing all malicious nodes is initiated by collecting response from monitoring nodes and the network. The mechanism has routing overhead increased due to additional routing packets.

For detecting packet forwarding misbehavior, Oscar et. al [9] proposed an algorithm that use the principle of flow conservation and accusation of nodes that are constantly misbehaving. Selecting correct threshold of misbehavior allows distinguishing well-behaved and misbehaved nodes. However, the average throughput cannot reach that of a network where there is no misbehaving node present because the algorithm requires definite time to gather the required data to identify and to accuse misbehaving nodes. Therefore, misbehaving nodes can drop packets before being accused and isolated from the network during the preliminary phase.

A trust-based approach is proposed by Arshad et. al [10] that uses passive acknowledgement as it is simplest; it uses promiscuous mode to observe the channel that allows a node to identify any transmitted packets irrelevant of the actual destination that they are intended for. Thus, a node can make sure that packets it has sent to the neighboring node for forwarding are indeed forwarded. Routing choices are made based on two parameters: trust and hop-count; therefore, the selected next hop gives the shortest trusted path. Though, monitoring overall traffic would have been a better choice instead of monitoring one node's request.

Ming-Yang et. al [11] proposed an intrusion detection system called Anti-Blackhole Mechanism (ABM) in which the suspicious value of a node is estimated according to the amount of abnormal difference between RREQs and RREPs transmitted from the node; all nodes perform ABM. With the requirement that intermediate nodes are prohibited to reply to RREQs, if an intermediate node is not the destination and never broadcasts RREQ for a specific route, but forward a RREP for the route, then its suspicious value will be increased in the nearby node's suspicious node table. When the suspicious value of a node goes beyond threshold, a Block message is broadcasted by the node to all other nodes in the network to isolate the suspicious node cooperatively. Though, the solution assumes that an authentication mechanism already exists in MANET.

An approach is discussed by Latha et. al [12] in which the requesting node waits for a specific time for replies from neighbors that include the next hop details. After the specific time, Collect Route Reply Table is verified to know whether there is any repeated next-hop-node or not. Existence of repeated next-hop-node in the reply paths indicates the truthful paths or limited chance of malicious paths. Though, the process of finding repeated next hop node increases overhead.

Payal et. al [13] suggested a protocol DPRAODV that finds a threshold value and compares that with difference of sequence number of reply packet and that of route table entry. If it is higher than the threshold value, the node sending reply is added to a list of blacklisted nodes. Also an ALARM packet containing blacklisted node is sent to its neighbors to inform that reply packets from the malicious node are to be discarded. The protocol has higher routing overhead due to addition of the ALARM packets.

An algorithm is proposed by Deng et. al [14] in which when a source node receives a route reply packet, it cross checks with the previous node on the route to the destination to verify that the node sending reply packet indeed has a route to the destination as well as to the intermediate node. If it does not have, the node that sent the reply packet is judged as malicious node. The mechanism, though, increases end-to-end delay and due to the addition of Further Request and Further Reply packets in the algorithm, routing overhead also gets increased.

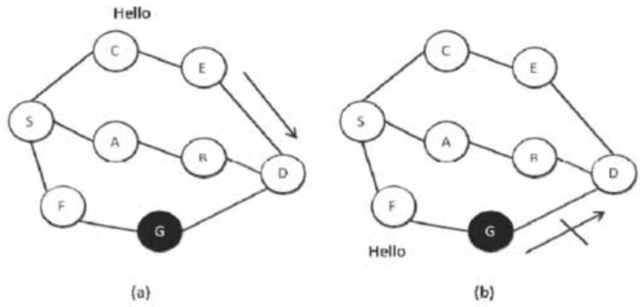


Fig. 2: Proposed Algorithm for Detection of Blackhole and DoS Attacks

V. PROPOSED WORK

To protect network from Blackhole and DoS attacks, it is necessary to discover malicious nodes during route discovery process when they pass fabricated routing information to attract the source node to send data through itself. Our proposed approach does exactly the same.

Researchers propose a method which uses promiscuous mode of the node. This mode allows a inspector node to intercept and read each node's Routing Table, in other words, promiscuous mode means that if a node *A* within the range of node *B*, it can overhear communication to and from B even if those communication do not directly involve *A*.

```
Start

Step 1: Root Discovery Process:
The source node S starts the route discovery phase by broadcasting the RREQ packet to the neighboring node.

Step 2: S Collecting Replies:
The Source node store all the replies arrived from the destination node or the intermediate nodes  in the terms of RREP.

Step 3: Identification of Blackhole & DoS Node:
Each node transferred into it’s Promiscuous mode.
Case 1: When a node is not Idle:
TopAdd=Source node retrieves the top entry from RR-Table.
Call the Procedure Blackhole_ DoS_Detection
Procedure (Blackhole_ DoS_Detection)
{
If (TopAdd == Address of Current_node)
Malicious node= Current_Node;}

Case 2: When a node is Idle (terminating node):

No need to take any Action

Step 4: Removal of Blackhole & Dos Attacked Node:

Do
Don’t Send Packet to the next node
Report to Inspector Nodes.
Remove the Entry of the entire malicious node (s) from the RR table detected through Blackhole_DoS_Detection Procedure in step 4
While (Packet Reaches to Destination)

Step 5: S selects the shortest path according to hop count.

Step 6: Continue Default Routing Process

Continue with the normal procedure of AODV Protocol.
Stop
```

Fig. 3: Flow of Hello packet towards destination (a) a good node forwards it (b) black node does not forward it.

The following is a detailed process. Consider a scenario as shown in Fig. 5; node *S* needs to communicate to node *D* and node *G* is a malicious node. Node *S* floods a RREQ packet in the network and waits for the RREP packet to obtain a fresh route to the destination node *D*. Now, there are two possibilities; the RREP packet may be received either from the destination node itself or from an intermediate node. In case 1, when the RREP packet is received from the destination node itself, a route is established. In case 2, when the RREP packet is received from an intermediate node, a node preceding to the node which sent RREP packet switches on its promiscuous mode and previous node check the Routing Table of the next node and after verifying the condition, it calls Blackhole_DoS_Detection function and removes the malicious node. All to gather researchers can say when there is no malicious node when there is no self looping in node’s Routing Table.

VI. SIMULATION AND RESULT ANALYSIS

The performance of proposed algorithms are implementaed on network simulator (NS-2) and the results are compared with original AODV to check the performance. So by the result comparison 370researchers can say the now there are less consumption in the network and now AODV with corporative IDS performs better than the original AODV. To reduce the packet dropping attack in the network the security mechanism is implemented to detect the malicious node in the network and hence, reducing the packet dropping attack in the network. It is evident from the results that the proposed algorithms are able to save energy of the nodes in the network as well as able to find the malicious nodes in the network. The simulation parameters used to implement the proposed algorithms have been tabulated in Table 1.

Table 1: Simulation Parameters Used in Simultation

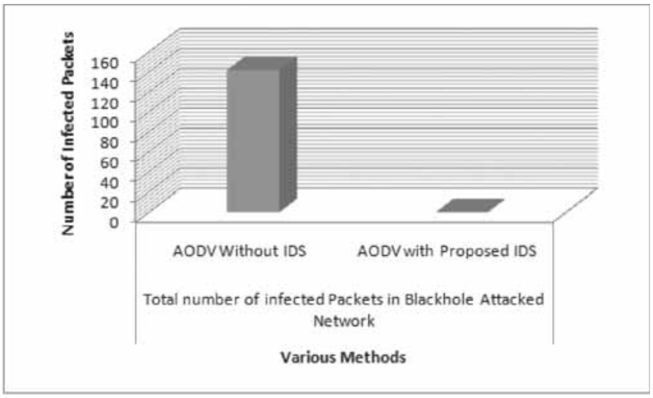
Simulation Time	360 seconds
Area:	1000 x1000
Traffic	TCP/FTP
Channel	Wireless
Operation mode	802.11
Mobility	Random waypoint
Antenna	Omni directional
IFQ	50
Nodes	50
IFQLEN	1000

The following parameters have been used for evaluation of the performance of proposed algorithms:

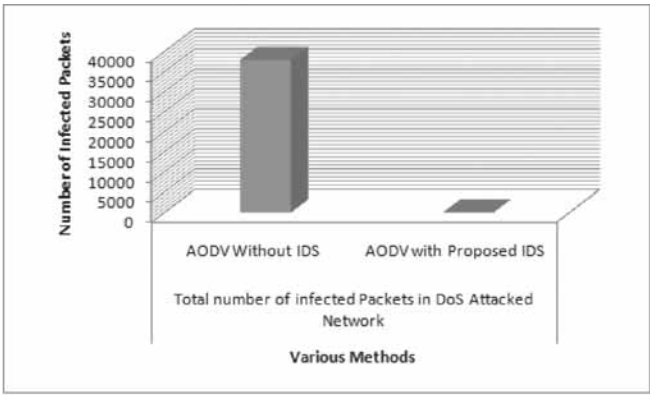
1) ***Packet Delivery Ratio (PDR):*** I*t is ratio of the total number of data packets received by the destination node to the total number of data packets sent.*

2) ***Number of infected Nodes:*** *The total number of infected nodes in the Adhoc network.*

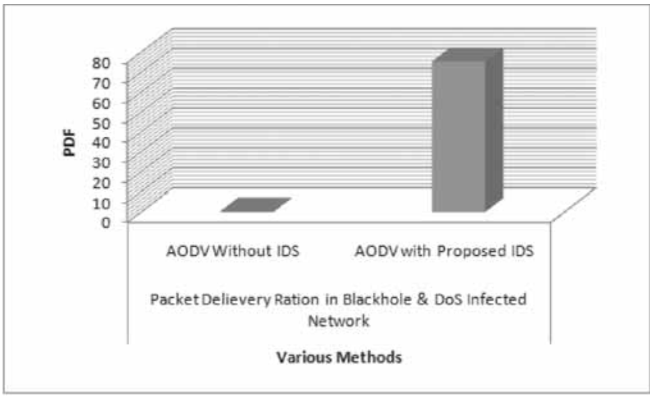
First of all researchers presents the results of security implementation part. The results are computed by tracing the output files generated by NS-2 simulator during simulation for all the proposed approaches. The performance of proposed algorithms are evaluated on the network with 50 nodes.



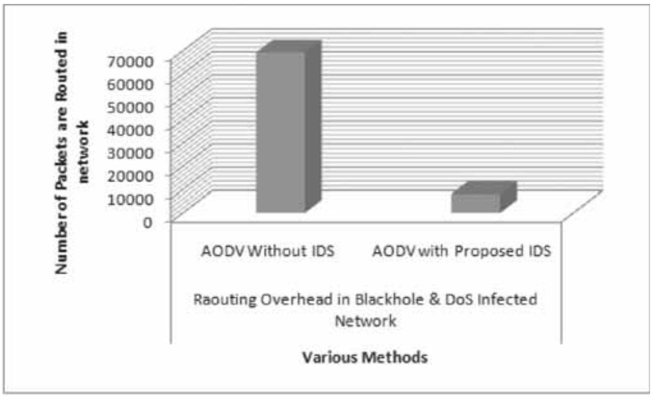
Graph 1: **It shows the number of infected packets in Blackhole Attacked Network without and with Proposed IDS.**



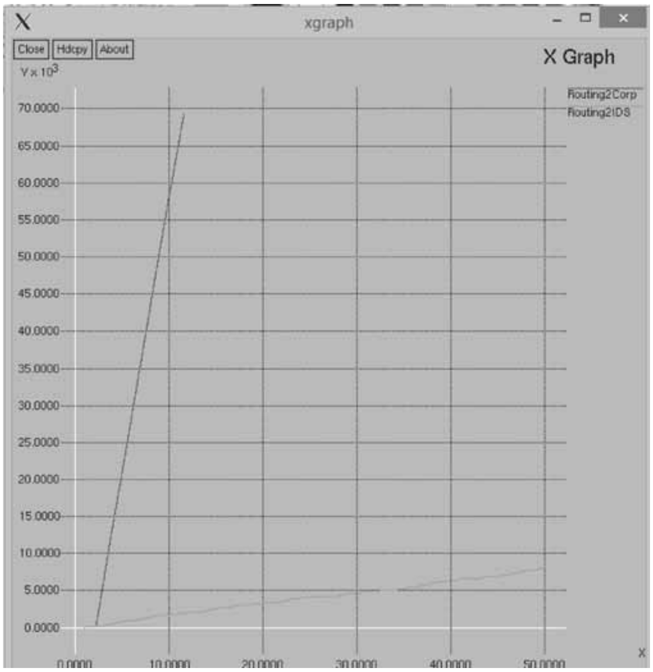
Graph 2: **It shows the number of infected packets in DoS Attacked Network without and with Proposed IDS.**



Graph 3: **It shows the Packet Delivery Ration in Blackhole and DoS Infected Network without and with Proposed IDS.**



Graph 4: **It shows the Number of Routed Packets in Blackhole and DoS Infected Network without and with Proposed IDS.**



Graph 5: **It shows the Routing Overhead in Blackhole and DoS Infected Network without and with Proposed IDS.**

Graphs 1, 2, 3, 4 and 5 explicitly shows that the performance of the proposed corporative Intrusion Detection System work over AODV routing protocol with Blackhole and DoS Infected Network without and with Proposed IDS.

VII. CONCLUSION

MANET is an emerging area as it has great potential in various diverse areas, e.g., military, disaster management, intelligent transportation system, monitoring, public safety. In this paper, researchers discuss blackhole and DoS attacks which is a severe security risk in routing. Researchers have proposed a simple, efficient and effective method with maximizing Packet Delivery Ration while maintaining minimum routing overhead to overcome the problem of the black hole and DoS attack problem with AODV routing protocol. The proposed method uses promiscuous mode of a node to overhear the neighbour's communication. It does not require any database, extra memory and more processing power. The simulation results show effectiveness of the proposed method over existing method on various parameters.

REFERENCES

[1] B. Wu, J. Chen, J. Wu, and M. Cardei, "A Survey on Attacks and Countermeasures in MANETs, *Springer*, 2006, ch. 12.

[2] Morli Pandya and Ashish Kr. Shrivastava , "Improvising the Performance with Security of AODV Routing Protocol in MANETs," IEEE 2013 Nirma University International Conference on Engineering (NUiCONE).

[3] N. Sharma and A. Sharma. The black-hole node attack in MANET. In Proceedings of the 2012 Second Interntional Corifence on Advanced Computing & Communication Technologies, ACCT ' 12, pages 546-550, Washington, DC, USA, 2012. IEEE Computer Society

[4] Y Guo and S. Perreau, "Detect DDoS floding attacks in mobile ad hoc networks," Int. 1 Secur Netw., 5(4):259-269, Dec. 2010.

[5] Dilli Ravilla and Dr Chandra Shekar Reddy Putta ," Performance of Secured Zone Routing Protocol due to the Effect of Malicious Nodes in MANETs," IEEE- 4th ICCCNT - 2013 July 4 - 6, 2013, Tiruchengode, India.

[6] Ajay Jangra, Shalini and Nitin Goel ," Prevention And Reaction Based Secure Routing In Manets," Journal of Global Research in Computer Science, Volume 2, No. 6, June 2011.

[7] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks," IEEE-2012 Second International Conference on Advanced Computing & Communication Technologies.

[8] Suresh Kumar, Gaurav Pruthi, Ashwani Yadav and Mukesh Singla, "Security protocols in MANETs," IEEE-2012 Second International Conference on Advanced Computing & Communication Technologies.

[9] Weichao Wang, Yi Lu, Bharat Bhargava, "On Security Study of Two Distance Vector Routing Protocols for Mobile Adhoc Networks", IEEE, 2003, 0-7695-1893- 1/03.

[10] L. Tamilselvan and D. V. Sankaranarayanan, "Prevention of blackhole attack in manet," 2007.

[11] Ming-Yang Su, "Prevention of Selective Black hole Attacks on Mobile Ad hoc Network through Intrusion Detection Systems", Computer Communications, 2010. Communications, 2007, pp. 21-26.

[12] Latha Tamilselvan, V. Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET", Journal of Networks, Vol 3, No 5, 13-20, May 2008.

[13] Payal N. Raj1 and Prashant B. Swadas2, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", IJCSI International Jtheynal of Computer Science Issues, Vol. 2, 2009.

[14] Akshai Aggarwal, Savita Gandhi, Nirbhay Chaubey and Keyurbhai A Jani,"Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs," IEEE-2014 Fourth International Conference on Advanced Computing & Communication Technologies. ❑