Anonymous Packet Format (APF) based Secure and Effective Routing Protocol in MANET

Prachi Sharma[1]and Miss S. V. Pandit[2]

[1]Department of Computer Science & Engineering,
ICOT, Bhopal, India

[2]Assistant Professor, Department of Computer Science & Engineering,
ICOT, Bhopal, India

ABSTRACT

Interest in the area of Mobile Ad-hoc Network (MANET) is growing since last few years because of its practical applications and requirement of communication in mobile devices. However, in comparison to wired network or infrastructure-based wireless network, MANET is particularly vulnerable to security attacks due to its fundamental characteristics, e.g., the open medium, dynamic network topology, autonomous terminal, lack of centralized monitoring and management. The black hole attack is one of such security risks. In this attack, a malicious node falsely advertise shortest path to the destination node with an intension to disrupt the communication. In this paper, we propose a solution to the black hole attack in one of the most prominent routing algorithm, ad-hoc on demand distance vector (AODV) routing, for the MANETs. The proposed method uses promiscuous mode to detect malicious node (black hole) and propagates the information of malicious node to all the other nodes in the network. The simulation results show the efficacy of the proposed method as throughput of the network does not deteriorate in presence of the back holes.

Keywords: component; formatting; style; styling; insert (key words)

1. 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 application 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. In Section III talks about AODV protocol. , where as section IV discusses about Security flaws with AODV protocol. Section V lands up with Related works. Section VI deals with proposed scheme for making MANET. Simulation and Results analysis is covered in Section VII. Finally conclusion and future directions are given in Section VIII.

2.BACKGROUND

Two approaches are used to provide solutions to the security issues in ad hoc networks: "Prevention" and "Detection and Reaction" Techniques. Prevention mechanism cannot 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 selfih 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 [4]. Virtual currency-based schemes use credit or micro payments to compensate for the service of a node. A node receives a virtual payment for forwarding the message of another node and this payment is deducted from the sender (or the destination node). Reputation systems are applied to wireless mobile ad hoc network to address threats arising from uncooperative nodes. They rely on neighbour monitoring to mitigate selfihness and stimulate cooperation in mobile ad hoc network. It is a system that takes feedback from users and provides a mechanism to accumulate and determine the quality of a given source based on this feedback. Monitoring, Reputation and Response are the basic fuction of reputation based schemes [5]. The Watchdog and Path rater scheme proposed by Marti et al 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. Aftrwards, 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. Aftrwards 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. In OCEAN, the rating of each node is initialized to Neutral (0), with every positive action resulting in an increment (+1) of the rating, and every negative action resulting in a decrement (-2) of the rating. Once the rating of a node falls below a certain faulty threshold (-40), the node is added to a faulty list. The faulty list represents a list of misbehaving nodes. OCEAN has fie components reside in each node to detect and mitigate misbehaviour. Recently a new algorithum has been proposed that handles network in an effient manner that would be relaiable too for the network.

3.AD-HOC ON DEMAND DISTANCE VECTOR PROTOCOL (AODV)

Ad hoc on demand vector (AODV) [10] has two operating modes, i.e., route discovery and route maintenance. This section discusses both operating modes[6] [7].

A. Route discovery mode

Figure 1 illustrates a route discovery process at which the source node A needs to obtain a routing-path towards the destination node D. As shown in the figure, a source node broadcasts a route request (RREQ) message to all neighbors since the node does not have a route-path to the destination node D. After receiving the RREQ message, a relay node B will check its routing table to determine if the node has a outepath to the destination node. Because the relay node does not have the route-path, the node then rebroadcasts the RREQ message. However, before rebroadcasting the route request message, the node will record the route-path to the last node visited by the RREQ message. All the process will be repeated until the route request message arrives to the destination node. When the RREQ message reaches the destination node, the destination node will unicast a route reply (RREP) message as the response to the RREQ message.

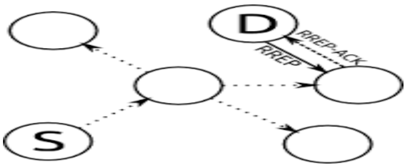


Fig. 1. AODV Route Discovery

Figure 1 shows the details of RREQ and RREP messages delivered by all nodes for discovering the route-path to the destination node. In the table, a1, b1, and c1 denotes route request messages; meanwhile 1d, and 1b symbolizes route reply messages. Each routing message has several fields to keep the routing data, for example, ‘IP Src’ for holding IP address of the source node, and ‘OrigSN’ for storing destination sequence number (DSN) of the originator node. In addition, the shaded rows in the table, i.e., HC, DSN, and Unknown DSN fields, store mutable data of the routing messages. These fields will be updated by the local node visited by the routing messages. As a result, the DSN data (‘*’) will change follow the DSN owned by the local node.

B. Route Maintenance

In routing, route maintenance will be used for adapting the network topology changes. For the purpose of route maintenance, all nodes in AODV must continuously listen to the communication channels for detecting link failure. Incoming of RREQ and RREP messages every n seconds to a node indicates that the route paths exist and no link fails between the node and the sender of messages. However, the unavailability of the messages for certain period indicates the link problems. If the node detects a link failure, it can send a hello message to check the failure. Furthermore, the ssucceeding of link failure detection insists that all nodes answer each of the incoming messages. When a node detects the link failure, the node can generate a route error (RERR) message. The following is the requirements to generate the essage:

a) if it detects a link break for the next hop of an active route in its routing table while transmitting data
b) if it gets a data message destined to a node for which it does not have an active route
c) if it receives an RERR from a neighbor for one or more active routes.

Figure 2 shows the process taken by nodes when a broken link detected. As shown in the figure, node 6 has detected a link failure while transmitting the data to node 9. Node 6 could not receive any response from node 9 after a certain period of time. Node 6 then generated an RERR message, and propagated the message back towards node 2. When node 4 receives the RERR from node 6, it compares and removes any entry in its routing table that has the RERR destination. The RERR itself is then sent either through broadcast or unicast message transmission.

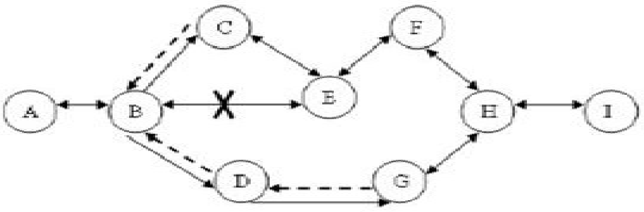


Fig. 2. Route Error Detection

C.Maintaining the Integrity of the Specifications

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

4.AODV PROTOCOL AND SECURITY FLAWS

Ad Hoc On-Demand Vector Routing (AODV) [10] is a reactive routing protocol. It uses destination sequence numbers to ensure the freshness of routes and guarantee loop freedom. To fid a path to a destination, a node broadcasts a route request (RREQ) packet to its neighbors using a new sequence number. Each node that receives the broadcast sets up a reverse route towards the originator of the RREQ unless it has a fresher one. When the intended destination or an intermediate node that has a fresh route to the destination receives the RREQ, it unicasts a reply by sending a route reply (RREP) packet along the reverse path established at intermediate nodes during the route discovery process. Then the source node starts sending data packets to the destination node through the neighboring node that fist responded with an RREP. When an intermediate node along the route moves, its upstream neighbor will notice route breakage due to the movement and propagate a route error (RERR) packet to each of its active upstream neighbors. Routing information is stored only in the source node, the destination node, and the intermediate nodes along the active route which deal with data transmission. This scenario decreases the memory overhead, minimizes the use of network resources, and runs well in high mobility situation.

The behavior of a malicious node is to disrupt the operation of the AODV routing protocol [8]. The malicious node can spoof source or destination IP address, modify RREQ or RREP packets and/or generate fake RREP or RERR packets. Some of the attacks such as blackhole and grayhole attack are discovered by the source node in connection-oriented protocols such as TCP because the lack of acknowledgments. The source node understands that there is a link error because the destination node does not send ACK packets. If the source 290 node sends out UDP data packets the problem is not detected because UDP is a connectionless protocol.

A.Flooding Attack on AODV

In a flooding attack [9], a malicious node takes advantage of the route discovery process of the AODV routing protocol. The malicious node aims to flood the network with a large number of RREQs to non-existent destinations in the network which takes a lot of the network resources. Since the destination does not exist in the network, a RREP packet cannot be generated by any node in the network and all the nodes keep on flooding the RREQ packet. When a large number of fake RREQ packets are broadcast into the network, new routes can no longer be added and the network is unable to transmit data packets. Thus, it leads to congestion in the network and overflow of route table in the intermediate nodes so that the nodes cannot receive new RREQ packet, resulting in a DoS attack. Moreover, unnecessary forwarding of these fake RREQ packets has serious effects in MANET as a result of limited computational and power resources of nodes.

However, the AODV protocol can mitigate against this attack by reducing the maximum number of RREQs that a node allowed to send per second.

B.Grayhole Attack on AODV

In a grayhole attack [10], a malicious node behaves normally as a truthful node during the route discovery process by replying with true RREP messages to the nodes that started RREQ messages. After the source node starts sending data through the malicious node, the malicious node starts dropping these data packets to launch a (DoS) denial of service attack. So, the malicious node forwards routing packets and drops data packets. This selective dropping makes grayhole attacks much more difficult to detect than blackhole attacks. Grayhole attack is also known as node misbehaving attack [1] as the malicious node misleads the network by agreeing to forward the packets in the network.

C.Blackhole Attack on AODV

In a blackhole attack [10] a malicious node absorbs the network traff and drops all packets. To carry out a blackhole attack, a malicious node waits for incoming RREQ packets from other nodes. When the malicious node receives an RREQ message, without checking its routing table, it inuniately sends a false RREP with a high sequence number and zero hop count to spoof its neighbours that it has the best route to the destination. Thus, the malicious node reply will be received by the source node before any reply from other nodes. When a source node receives multiple RREP, it chooses the RREP with the largest destination sequence number and the smallest hop count. Then the source node ignores other RREP packets and begins sending data packets over the malicious node. When the data packets routed by the source node reach the blackhole node, it drops the packets rather than forwarding them to the estination node.

The malicious node attacks all RREQ packets in this way and takes over all routes. Therefore all packets are sent to a point where they are not forwarding anywhere. If the malicious node generates false RREP messages that appear to come from another victim node, all messages will be forwarded to the victim node. By doing this, victim node will have to process all incoming messages and is ubjected to a sleep deprivation attack.

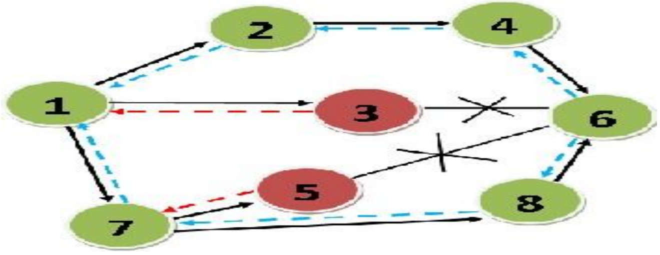


Figure 3. Routing discovery in AODV with black hole attack

5.Related Work

Piyush et.al [9] 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 [10] 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.

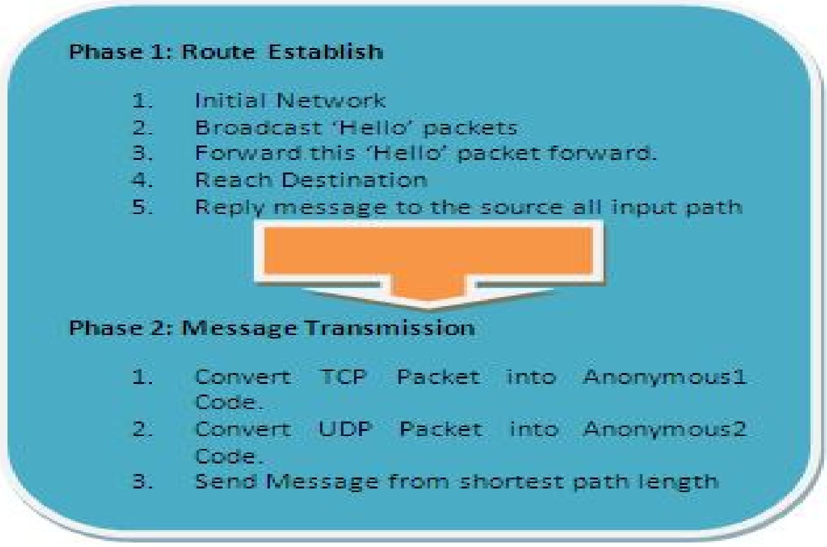
Ming-Yang et. al [6] proposed an intrusion detection system called Anti-Blackhole Mechanism (ABM) in which the suspicious value of a node is estimated according to the amount of abnormal difference between RREQs and RREPs transmitted from the node; all nodes perform ABM. With the requirement that intermediate 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 [10] 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.

6.PROPOSED WORK

To protect reactive protocols from Blackhole attacks, it is necessary that no node could identify the type of the packet during route discovery process. Our proposed approach does exactly the same.



Phase 1: Route Establish

1. Initial Network
2. Broadcast ‘Hello’ packets
3. Forward this ‘Hello’ packet forward.
4. Reach Destination
5. Reply message to the source all input path

Phase 2: Message Transmission

1. Convert TCP Packet into Anonymous1 Code.
2. Convert UDP Packet into Anonymous2 Code.
3. Send Message from shortest path length

Fig 4: Algorithm of Proposed Work

We propose a method which uses promiscuous mode of the node. This mode allows a node to intercept and read each network packet that arrives in its entirety, 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*.

6.SIMULATION AND RESULT ANALYSIS

The performance of proposed algorithms are implemented on network simulator (NS-2) and the results are compared with original AODV to check the performance. So by the result comparison we can say the now there are less blackhole effects in the network and now AODV performs better than the original AODV. To reduce the packet dropping attack in the network the security mechanism is implemented Anonymous Format Packet (APF) in the network and hence, reducing the packet dropping attack in the network. The simulation parameters used to implement the proposed algorithms have been tabulated in Table 1.

TABLE 1: SIMULATION PARAMETERS USED IN SIMULATION

Simulation Time	360 seconds
Protocol	AODV and AFP(Developed)
Area:	800 x800
Traffic	APF1/APF2
Channel	Wireless
Operation mode	802.11
Mobility	Random waypoint
Antenna	Omni directional
IFQ	100
Nodes	50
IFQLEN	1000

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

Packet Delivery Ratio (PDR): It is ratio of the total number of data packets received by the destination node to the total number of data packets sent. First of all we 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.

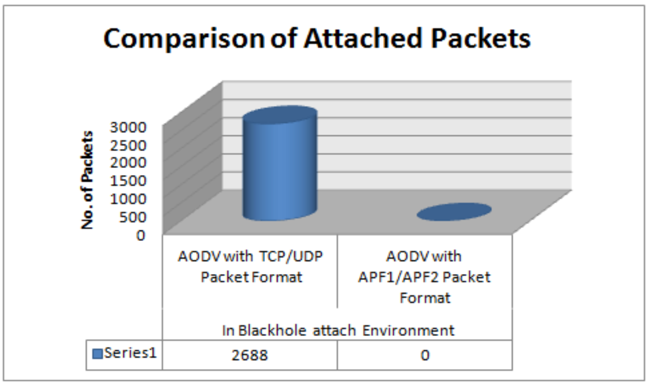


Fig 5: A Number of packet gets effected in base and proposed work

7.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. However, it poses a greater security risk in comparison to conventional wireless and wireless networks due to its inherent characteristics, e.g., the open medium, dynamic network topology, autonomous terminal, lack of centralized monitoring, lack of management point Mobile. In this paper, we discuss black hole problem which is a severe security risk in routing. We propose a simple, efficient and effective method with minimum routing overhead to combat the black hole problem. The proposed method uses new packet format 'Anonymous Packet Format'. The simulation results show effectiveness of the proposed method.

REFERENCES

[1] Ankur O. Bang and Prabhakar L. Ramteke,"MANET : History,Challenges And Applications," International Journal of Application or Innovation in Engineering & Management(IJAIEM), Volume 2, Issue 9,September 2013.

[2] Seema, Dr. Yudhvir Singh and Mr. Vikas Siwach,"Quality of Service in MANET,"International Journal of Innovations in Engineering and Technology (IJIET), Vol. 1 Issue 3 Oct 2012.

[3] Pooja Jaiswal and Dr. Rakesh Kumar ,"Prevention of Black Hole Attack in MANET," IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No5, October 2012.

[4] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard ,"Prevention of Cooperativ e Black Hole Attack in Wireless Ad Hoc Networks," citeseerx, 2003.

[5] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao,"A survey of black hole attacks in wireless mobile ad hoc networks," Tseng et al. Human-centric Computing and Information Sciences, 2011.

[6] Durgesh Wadbude and Vineet Richariya,"An Efficient Secure AODV Routing Protocol in MANET," International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012.

[7] Manveen Singh Chadha, Sandeep and Rambir Joon, " Simulation and Comparison of AODV, DSR and AOMDV Routing Protocols in MANETs," International Journal of Soft Computing and Engineering (IJSCE), Volume -2, Issue-3, July 2012.

[8] Ei Ei Khin and Thandar Phyu, "IMPACT OF BLACKHOLE ATTACK ON AODV ROUTING PROTOCOL, "nternational Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.2, May 2014.

[9] Parbhat Verma, Seema and Komal Manocha ,"Performance of AODV under Flooding Attack," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 8, August 2014.

[10] Divya Khajuria and Sudesh kumar,"Detecting multiple Blackhole and Grayhole attacks in MANETS by modifying AODV,"OSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 2, Ver. XII (Mar-Apr. 2014), PP 126-133.