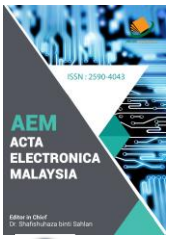
ZIBELINE INTERNATIONAL PUBLISHING

ISSN: 2590-4043 (Online)
CODEN: AEMCDV

Acta Electronica Malaysia (AEM)

***DOI** : http://doi.org/10.26480/aem.01.2019.01.05*



CrossMark

REVIEW ARTICLE

PERFORMANCE ANALYSIS OF AODV IN PRESENCE OF MALICIOUS NODE

Rohit Rana, Rajendra Kumar

Computer Science and Engineering Department, Vidya College of Engineering, Meerut
***Corresponding Author Email:** rohitrana@vidya.edu.in , rajendra.kumar@vidya.edu.in*

ARTICLE DETAILS

Article History:

Received 15 November 2018
Accepted 20 December 2018
Available Online 7 January 2019

ABSTRACT

Un-wired Computers (Mobile Computers) such as Laptops, Net-books, Notebooks and Personal Digital Assistants (PDAs) are the fastest growing segments of Computing Industry; this changing aspect of computing has led to the invention of Mobile Ad-Hoc Networks (MANET). Mobile Ad Hoc networking is a new era of infrastructure less communication networks for mobile devices (hosts, nodes etc.), where mobile nodes that are in radio range for each other can directly communicate with each other when in range and can even use intermediate nodes as routers when are moving away or are getting out of range from the connected nodes, this property along with the ability of switching from one network topology to another help in improving node mobility. Due to this mobility factor and undefined infrastructure security is a major concern in mobile Ad Hoc networks. In this paper we are providing a detailed analysis of the performance of ad-hoc routing protocol AODV in Mobile Ad Hoc networks with and without the presence of malicious node. We have used Qualnet version 5.0 (simulator) to measure the effect of attack on mobile ad-hoc networks that gives a clear picture for the throughput, variations in CBR, packet delivery delay, average jitter and end-to-end delay in mobile ad-hoc networks when attack effects the mobile ad-hoc network.

KEYWORDS

CBR, WSN, MANET, AODV, ZIG- BEE

1. INTRODUCTION

Unwired computers (Mobile Computers) like PDA's, Laptops, Smart phones are the fastest growing industry of today's computing segment as the world is becoming global, we need to cope up with the increasing pace of world and in this scenario these unwired computers play a vital role and proves to be very helpful when combined with Ad-Hoc networks. As we know that MANET is a networking system that do not require any planned networking infrastructure or in other words we need not to worry about placing the router, switches or any other devices for network formation, combining the concept of Ad-Hoc Networking with sensor contained mobile Nodes we can get into another phase of comfort-full networking while being mobile and resource-full at the same time. But as we know that every prone comes with some corn, the same is true for mobile ad-hoc sensor networks, no doubts they are adding a lot to our comfort and are reducing the cost and time required to establish and maintain networks but are on the other hand are proving to be very challenging for the integrity and confidentiality of our precious data and transactions we are making using these networking systems [1]. As discussed earlier in mobile Ad Hoc networks there is no fixed architectural infrastructure (or defined structured network) is required for the formation of networks. The mobile nodes that are in radio range for each other can directly communicate with each other when in range and can even use intermediate nodes as routers when are moving away or are getting out of range from the connected nodes, this property along with the ability of switching from one network topology to another help in improving node mobility. Due to this mobility factor and undefined infrastructure, security is a major concern in mobile Ad Hoc networks. Beyond the basic concerns related to Availability, Confidentiality, Authentication, Non-Reproduction etc. The existence of different Active and Passive Network Attacks presents a sever threat to the security of Mobile Ad Hoc Networking systems, Attacks like Wormhole, Black hole, Sybil are hard to be detected and prevented in this scenario (where we are not having any defined layout of the networking system we are dealing with). In the present paper we are providing a detailed analysis of the performance of ad-hoc routing protocol AODV in Mobile Ad Hoc networks with and without the presence of malicious node. We have used Qualnet version 5.0 (simulator) to measure the effect of Black-hole attack on mobile ad-hoc sensor networks and the plotted results gives a clear picture for the throughput, variations in CBR, packet delivery delay, average jitter and end-to-end delay in mobile ad-hoc networks when the presence of malicious nodes effecting the performance of AODV and mobile ad-hoc sensor networks.

2. CONCEPTUAL ARCHITECTURE OF MANET

After a deep analysis of mobile ad-hoc sensor networks we conclude that there are some major constraints that we need to look after while dealing with mobile ad-hoc sensor networks; all the devices we are going to have involved in a pure mobile ad-hoc sensor network will be using a battery to support mobility and will require some short of wire-less (radio) transmitters and receivers to transmit and receive signals [2].
A wireless sensor network (WSN) is a system of spatially distributed autonomous sensors to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The main characteristics of a WSN include:

- Ability to cope with node failures
- Mobility of nodes
- Communication failures
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use

- Power consumption constraints for nodes using batteries or energy harvesting

Sensor nodes can be imagined as small computers, extremely basic in terms of their interfaces and their components. They usually consist of a *processing unit* with limited computational power and limited memory, *sensors* or MEMS (including specific conditioning circuitry), a *communication device* (usually radio transceivers or alternatively optical), and a power source usually in the form of a battery.

Standards are used far less in WSNs than in other computing systems which makes most systems incapable of direct communication between different systems. However predominant standards commonly used in WSN communications include:

- ZigBee
- 802.15.4
- 6LoWPAN

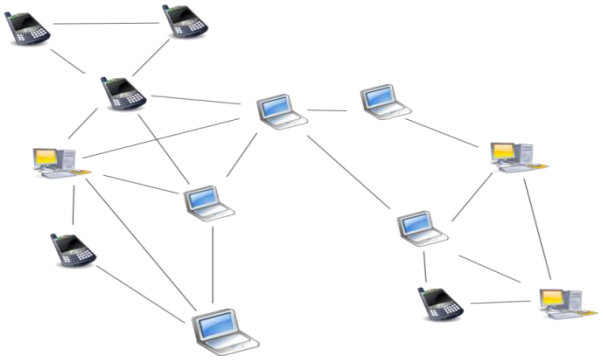


Figure 1: Mobile Ad-hoc Network

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

Ad hoc On-Demand Distance Vector (AODV) routing protocol is intended for use by mobile nodes in an ad hoc network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and determines routes to destinations within the ad hoc network. It uses destination sequence numbers to ensure loop freedom at all times (even in the face of anomalous delivery of routing control messages), avoiding problems (such as "counting to infinity") associated with classical distance vector protocols.

The AODV Routing Protocol uses an on-demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. It employs destination sequence numbers to identify the most recent path. In AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission [3]. Mobile nodes in an ad-hoc network use AODV protocol for dynamic linking, instant route discovery and maintaining low network utilization. In other words, AODV helps mobile nodes in discovering instant routes for participation in communications and helps mobile nodes to respond quickly to changes in network topology [4]. AODV make use of three type of messages transferred through UDP and normal IP header processing in operations; Route Request (RREQs), Route Replies (RREPs) and Route Errors (RERRs), limited IP broadcast address 255.255.255.255 is used for the broadcast of these messages. AODV uses the following fields for operations in ad-hoc networks:

- Destination Address.
- Destination sequence number.
- Valid destination sequence number flag.
- Other state and routing flags.
- Hop count.
- Next hop.
- List of participants.
- Life time of route.

In active state the operational procedures of AODV can be defined from the state when nodes generate route request (RREQ), route replay (RREP) and route error (RERR) messages to communicate with a destination node and this can be understood by the figure below:

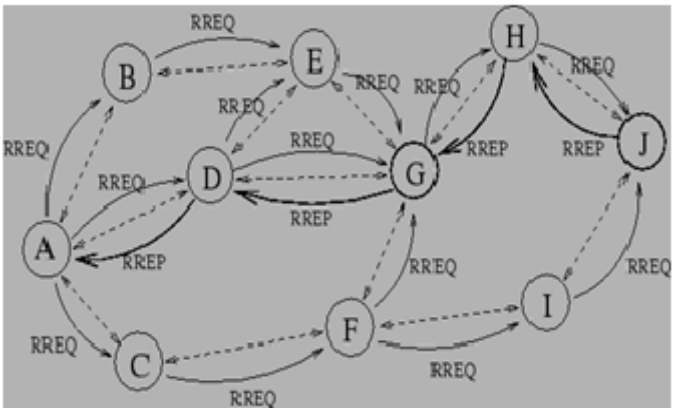


Figure 2: Operational Procedure of AODV

The main advantage of this protocol is having routes established on demand and the connection setup delay is low. Disadvantage of this protocol is that intermediate nodes can lead to inconsistent route information and this is where we are focusing in our present research work [5].

3.1 Issues related to Security in Ad-hoc Networks

From the discussion so far, we can conclude that all ad-hoc networks are infrastructure-less networks that do not have a centralized administrator and infect these networks involves minimum amount of planning at the time of deployment they are so constructed that can be used as soon as possible [6]. This basic architecture of ad-hoc network is perhaps the main reason that they are more prone to be attacked from inside the network as compared to other networks. These attacks can be classified based on their behavior (Passive or Active Attacks), the existence of the attacks (Internal or External Attack), and the number of the nodes involved in the attack (Single or Multiple Attack). The various attacks defined above effects the network in different ways, some are intended to steel passive information, and some are actively involved in masquerading the performance of the network [7]. So, it is very important to understand the basic theory behind these attacks and for the same we need to understand each of them separately.

3.1.1 Sybil Attack

Sybil attack named after a woman's case study of multiple personality disorder in Sybil attack a node in the network claims multiple identities and can lead to several security threads. Networks generally relay on the identities where each node (Computer) represents an identity, when an insecure node is trapped by some intruder (attacker) and claims multiple identities. These multiple identities can then be used by the attacker to effect communication, steal information or to produce unwanted circumstances in the network. Ad-hoc networks can easily get affected by sibyl attack.

3.1.2 Wormhole attacks

Wormhole attacks generally involve the engagement of multiple nodes but can either be performed by single node. In wormhole attack the attacker usually disturbs the packet flow by disrupting routing for the transmissions. In general; two or more nodes are connected via a wormhole link making a tunnel, the packets transmitted in the network are captured at one end and replayed at the other end of the tunnel, as AODV unable to track routes longer than one or two hopes it becomes easy for the attacker to make the tunneled packet arrive with better metric than a normal multi-hope route, they can make use of a single long-range wireless link or through a direct wired link to colluding attacker It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. Due to the nature of wireless transmission,

the attacker can create a wormhole even for packets not addressed to it, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole [8].

Wormhole attacks can be categorized as:

- **In - Band Wormhole Attacks**

In-band wormhole attacks are the most dangerous and easy to implement type of wormhole attacks as they do not require special hardware support and can make use of the existing infrastructure, they are considered to be more dangerous and harmful. They can be self- contained or extended type, the self-contained wormhole promotes a false link connecting the attacking nodes while the extended in-band wormhole promotes its fake link between two nodes that are never involved in the attacks. The extended in-band produces a wormhole attack that goes further than the attacker nodes, thus can be more drastic and dangerous.

- **Out-of-band Wormhole**

This kind of wormhole attack may require additional hardware to create direct communication link to the network; the two end points for the tunnel this link so established by the attacker is an external link to the network using wired or wireless mediums, one end is used to receive packets and other end is used to retransmit (replay) them back to the network via wormhole, thus the packets traveling through this wormhole link or tunnel are always under threat [9].

3.2 Black-hole Attack

Black-hole Attack or some time referred as Packet drop attack is concerned to denial-of-service attack in which a router that is supposed to relay packets instead discarding them. There may be a number of causes that can compromise the router and can put the system under threats of black-hole attack. Once into its frame Black-hole attack can proceed as. A malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. In flooding based protocol, if the malicious reply reaches the requesting node before the reply from the actual node, a forged route has been created. This malicious node then can choose whether to drop the packets to perform a denial-of-service attack or to use its place on the route as the first step in a man-in-the-middle attack.

4. OVERVIEW OF CURRENT LITERATURE

After going through many research articles and analyzing the work of several researchers in the field of mobile ad-hoc networks we focused on the working of AODV protocol and its behavior under certain undesirable circumstances. AODV is subjected to several threats of attacks from outside as well as inside of the network. The attacks from within the network are more eyes catching when it comes to performance analysis as they can prove to be more dangerous and are very difficult to be tracked.

5. SIMULATION PARAMETERS

As Qualnet 5.0 is based on GUI, parameters can easily be set using different options available on the menu bar of the interface. In the current experimental setup, we have used the following values to configure network for simulation, from the results we can easily conclude that the performance of AODV is a prime concern while the system is set under attack.

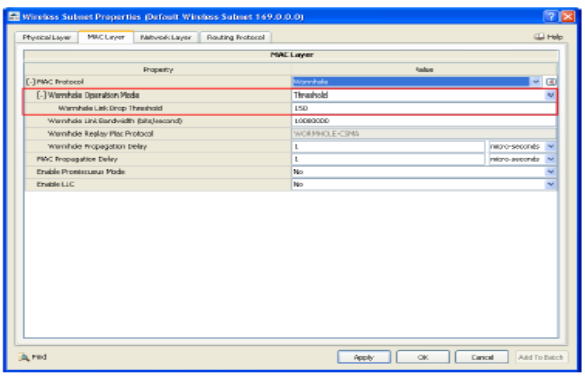


Figure 3: Setting up Simulation Parameters

- Simulation area 1500*1500 meters
- Simulation Duration = 180 sec
- Connection = FTP
- Radio/Physical layer parameters= 802.11 b
- Routing Protocol used is AODV
- Pause Time are 10, 20, 30, 40 and 50 sec.
- Number of nodes were 50
- Maximum segment size was 512 bytes
- Maximum data transfer rate was 2mbps
- Radio range was 300 meters
- Traffic type set was CBR
- Mobility was taken as Random way point

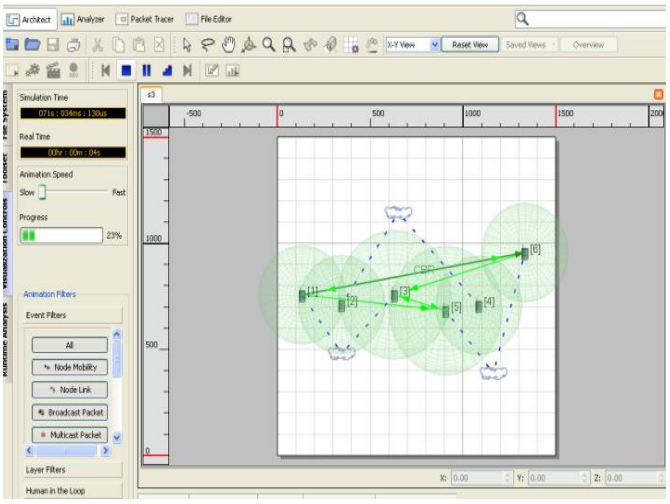


Figure 4: After configuring Attack

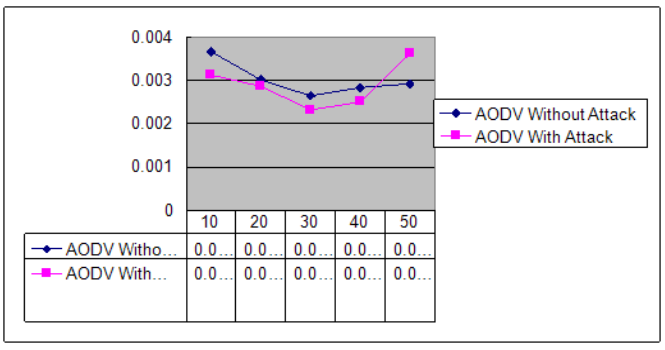
5.1 Pause Time Vs Average jitter(s)

From the graph below, we can easily conclude that the average jitter values are showing variations while the system is put under attack, it is clear from the graph that the value of average jitter are dropping in a linear way till the pause time 40 but after that a sudden rise in average jitter can be seen this is the point when the node under attack started to forward packets to flood the network. In other words, performance of AODV is getting affected by the presence of malicious node as uncertain variations in the value of average jitter can be seen. Table 1, through graph 1 displays results for it.

Table 1: Pause Time Vs Average jitter

Time Slots (ms) →	10	20	30	40	50
AODV Without Attack	0.003661	0.00301	0.002641	0.00283	0.002919
AODV With Attack	0.00312	0.002861	0.002316	0.002501	0.003611

Graph 1: Pause Time Vs Average jitter



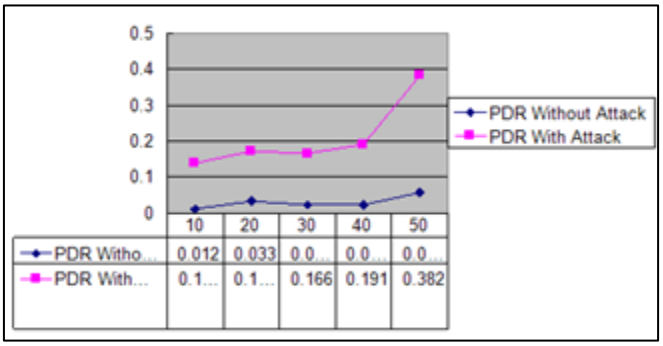
5.2 Pause Time Vs Packet Drop Ratio

From the graph under we can analyze that the packet drop ratio is increasing while the system is performing under attack, as it is clear from the curves that the number of packets dropped during the attack are more than the number of packets dropped under normal conditions. Table 2, through graph 2 displays results for it.

Table 2: Pause Time Vs Packet Drop Ratio

Time Slots (ms) →	10	20	30	40	50
PDR Without Attack	0.012	0.033	0.0231	0.0233	0.0572
PDR With Attack	0.1387	0.1721	0.166	0.191	0.382

Graph 2: Pause Time Vs Packet Drop Ratio



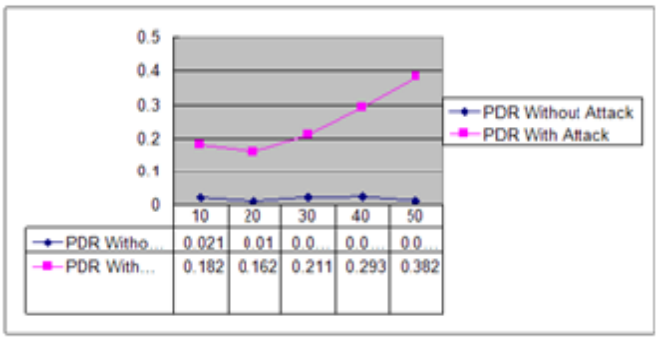
5.3 Packet Drop Ratio with Varying Node Speed

From the graphs below, we can see that when system is performing under attack the variation in node speed is affecting the packet drop ratio in a very visible fashion. While the system is performing in ideal conditions the variations in PDR values are almost constant with variations in node speed but as soon as the system is put under attack the variations are clearly visible. Table 3, through graph 3 displays results for it.

Table 3: Packet Drop Ratio with Varying Node Speed

Time Slots (ms) →	10	20	30	40	50
PDR Without Attack	0.021	0.01	0.0221	0.0231	0.0112
PDR With Attack	0.182	0.162	0.211	0.293	0.382

Graph 3: Packet Drop Ratio with Varying Node Speed



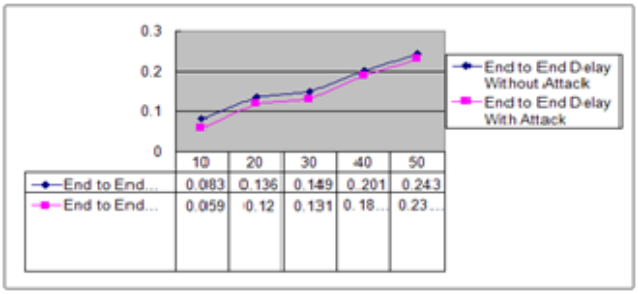
5.4 End to End Delay at AODV with respect to Node Speed

When it comes to end to end delay the results describes that the system is performing well under attack ie., the values of end to end delay are less than the values encountered while the system was under ideal conditions. This is because the malicious nodes are broadcasting fake routing information to the communicating nodes. Table 4, through graph 4 displays results for it.

Table 4: End to End Delay at AODV with respect to Node Speed

Time Slots (ms) →	10	20	30	40	50
End to End Delay Without Attack	0.083	0.136	0.149	0.201	0.243
End to End Delay with Attack	0.059	0.12	0.131	0.1892	0.2301

Graph 4: End to End Delay at AODV with respect to Node Speed



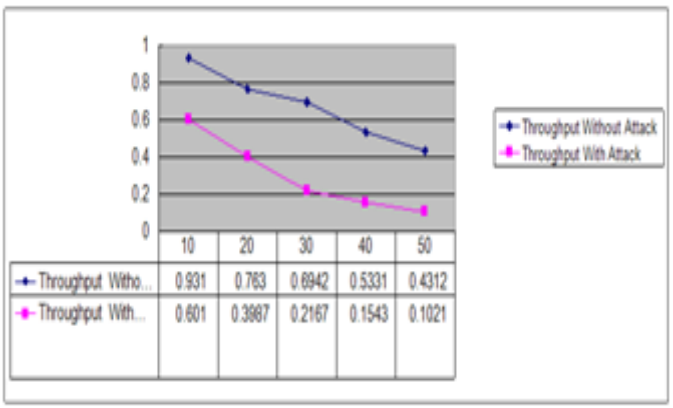
5.5 Throughput Vs Node Mobility

From the results we can conclude that the throughput is very much affected by the presence of malicious node in the network and the values so obtained are showing overall performance degradation, we can easily conclude that overall throughput is dropping in drastic fashion and AODV is performance is getting affected in a major way. Table 5, through graph 5 displays results for it.

Table 5: Throughput Vs Node Mobility

Time Slots (ms) →	10	20	30	40	50
Throughput Without Attack	0.931	0.763	0.6942	0.5331	0.4312
Throughput with Attack	0.601	0.3987	0.2167	0.1543	0.1021

Graph 5: Throughput Vs Node Mobility



6. CONCLUSION AND FUTURE SCOPE

After analyzing the simulation results, so, obtained we concluded that the performance of AODV is a major concern, when the system is performing under attack. The values of Throughput, Average jitter and Packet drop ratio are providing enough to analyze the AODV performance. Experimental results obtained from industrial version of Glomosim simulator called Qualnet (version 5.0), gives a clear picture, that the attacks on MANET that are striking from within the network are more dangerous and drastic then the attacks that are from outside the networks. MANET' are more prone to security threats then compared to wired networks and performance of AODV under attack require more attention from researchers, much work is needed to improve the secure flow of

routing information within the network. The information in routing tables needs to be maintained on a more secure note.

REFERENCES

[1] Akyildiz, F., Kasimoglu, I.H. 2004. Wireless Sensor and Actor Networks: Research Challenges, Ad Hoc Networks, 2(4), 351-367. https://tools.ietf.org/html/rfc3561.

[2] Al-Shurman, M. 2004. Black Hole Attack in Mobile Ad Hoc Networks, Proceedings of the 42nd Annual Southeast Regional Conference, 2004, Huntsville, Alabama, USA, April 2-3.

[3] 2003. IETF RFC 3561 Ad hoc On-Demand Distance Vector (AODV) Routing.

[4] Creswell, J.W. 2003. Research Design: Qualitative, Quantitative and Mixed Methods Approaches, Second Edition.

[5] Hu, Y., Perrig, A., Johnson, D.B. 2006. Wormhole Attacks in Wireless Networks, IEEE Journal on Selected Areas in Communications, 24(2), 370-380.

[6] Gorlatova, M.A., Mason, P.C., Wang, M., Lamont, L., Liscano, R. 2006. Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis, In Proceeding of Military Communications Conference, MILCOM, IEEE, 23-25 Oct. 2006, 1-7.

[7] van Glabbeek, R., Hofner, P., Portmann, M., Tan, W.L. 2016. Modelling and Verifying the AODV Routing Protocol, Distributed Computing, 29(4), 279-315.

[8] Kumar, M. 2010. Comparative analysis of CBRP, DSR, AODV routing protocol in MANET, (IJCSE) International Journal on Computer Science and Engineering, 2(9), 2853-2858.

[9] Rana, R., Shekhar, J. 2012. Consequences and Measures of Wormhole Attack in MANET, Conference: International Conference on Recent Trends in Engineering & Technology (ICRTIT).