International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-04, Issue-10, Jan 2019

Simulation Based Study and Analysis of Single and Multiple Black Hole Attacks in Mobile Ad Hoc Network Routing

Rahul D. Mehta, Assistant Professor, Electronics & Communication Engineering Department, Government Engineering College - Rajkot, Rajkot, Gujarat, India, rdmehta@hotmail.com

Shweta Adroja, Electronics & Communication Engineering Department, Government Engineering College - Rajkot, Rajkot, Gujarat, India, shweta.adroja8165@gmail.com

Abstract Mobile Ad Hoc Network (MANET) is an infrastructure less network having a group of nodes which act as routers as well as simple nodes to be active members of routing process. Hence, routing is one of most important parts while designing the protocols. These kind of open networks are most susceptible to various types of attacks which are very common in a MANET routing nowadays. This paper simulates and analyzes the effects of Single and Multiple Black Hole Attacks on performance of routing protocols which in turn affects the overall network performance. Packets delivery ratio, goodput, delay and throughput are considered as major performance measurement parameters. NS-2, with an additional support of NSG and APP tool, is used to simulate, analyze and to plot graphs to carry out simulation based comparative analysis.

Keywords — Mobile Ad hoc Network, Routing, AODV Protocol, Black Hole Attack, Infrastructure-less, Firewall

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) consists of nodes connected in Ad-hoc manner without any support of centralized infrastructure. MANET has grabbed attention and penetrated in the applications where a huge infrastructure is difficult to install as well as not cost efficacious. IEEE 802.11 Wi-Fi supports low quality Ad-hoc network services in the absence of access point. A MANET is a dynamic wireless network consists of mobile hosts which communicates with each other without help of any pre installed centralized infrastructure. All mobile nodes in a network can act as a host or as a router as and when needed. Every node in Ad Hoc network needs cooperation of all other participating nodes to efficiently route the network traffic [1]. Network topology gets modified with time due to the movements of the nodes or by adjustment in transmission and reception parameters.

Mobile Ad Hoc Network finds its application where infrastructure based communication is extravagant or inconvenient to utilize [2], [3]. Major areas of MANET applications include Defense, Disaster relief, Mining cite, Urgent business meetings, Personal Area Network (PAN), Community and Enterprise networks, Home as well as Emergency response networks, Vehicular networks etc.. The distinct features which make Mobile Ad Hoc Network more applicable include private access and accommodation regardless of geographic position, quick installation and setup, Router free operation and Mobility [18]. Whereas, limited resources, physical security, vulnerability to attacks, violation of network topology, non- compatibility of wired security protocols over wireless Ad Hoc network are the areas of concern in MANET.

Routing in MANET is one of the most important tasks to be performed to route the network traffic effectively in the absence of infrastructure based fixed network as well as to handle mobility related issues which are not taken care in case of fixed network [4], [19]. Policies, algorithms and protocols for MANET quite differ from the standard ones. As shown in Figure 1, MANET routing protocols are largely segregated into three major categories: Reactive, Proactive and Hybrid.

Proactive, known as table-driven, protocols actively determines the network layout. On every node, state and route information of the network are maintained by means of update packets exchanged between the nodes [5], [6]. This help in least delay in deciding routes, especially helpful in time-critical traffic. Few major Proactive MANET protocols are: Cluster-head Gateway Switch Routing Protocol (CGSR) Optimized Link State Routing (OLSR), and Destination Sequenced Distance Vector (DSDV) [7], [8]. On the contrary, instead of consuming resources unnecessarily in advance, route revelation process is initiated on the fly to discover a pathway i.e.

 DOI : 10.18231/2454-9150.2018.1302

establishing routes on demand. A variety of on-demand driven MANET reactive protocols include: Temporally Ordered Routing Algorithm (TORA), Dynamic Source Routing (DSR) and Ad hoc On-demand Distance Vector (AODV) [17], [21]. Proactive protocols are limited to tiny domain, while, reactive protocols are used to locate the nodes outside tiny domains. Hybrid protocols incorporate the beauty of both types of protocols by finding the balance between two major contenders in MANET routing protocol category. Zone-based Hierarchical Link State (ZHLS) and Zone Routing Protocol (ZRP) protocols are the examples of Hybrid MANET routing protocols.

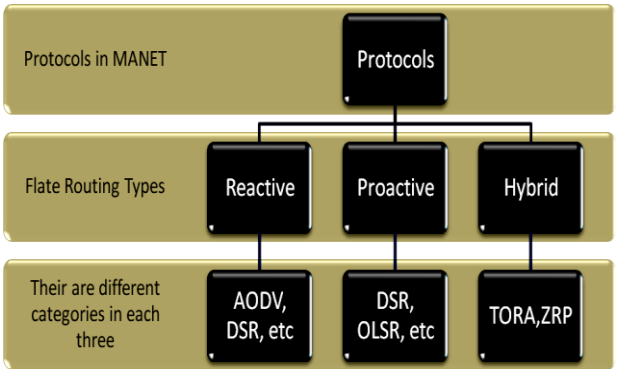

Figure 1: Classification of MANET Routing Protocols

II. TYPES OF ATTACKS IN MANET

There are number of attacks which occur under different network environment and scenarios that affect the network performance in various ways. The goal of the security services for MANET is to ensure a framework containing availability, confidentially, integrity, authentication and non-repudiation to offer the services to the mobile user. Few major and well known attacks observed frequently in MANET are discussed here.

A. Active and Passive Attacks

These categories of attack could be of Internal or External types of attacks in broad sense. In active attack, as shown in Figure 2, the attacking node is a part of active network and tries to alter as well as destroys the current transmission by altering data by means of capturing of data or by Denial of Service (DoS) attack. Whereas, in passive attack, as shown in Figure 3, attacking node not being directly a part of a network, it intercepts enough information of nodes regarding its current communication and positions of nodes in a network before an attack.

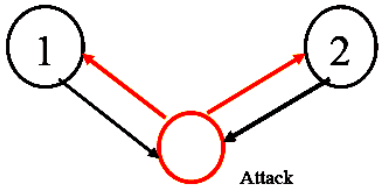

Figure 2: Active Attack

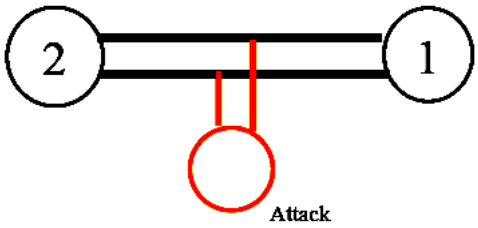

Figure 3: Passive Attack

B. External and Internal Attacks

As shown in Figure 4, an external attacking node tries to get access to current network. After succeeding, it starts interrupting ongoing transmission which drastically affects the complete network performance. External attacks can be prohibited by blocking unauthorized access to the network through proper installation and configuration of the Firewalls. Whereas, as shown in Figure 5, in an Internal attack, an attacker node is somehow already being a part of a network and contributes to its usual network activities [11]. But, later on, the attacking node starts showing its malevolent behavior. Hence, it is very intricate to locate a malicious one out of all active nodes which shows that Internal attack has got more impact on functionality of a network compared to an External attack.

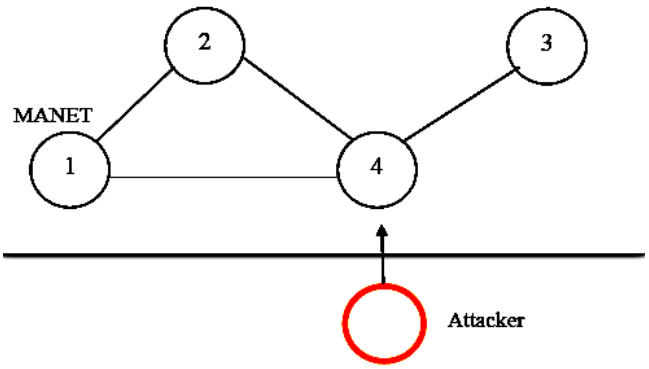

Figure 4: External Attack

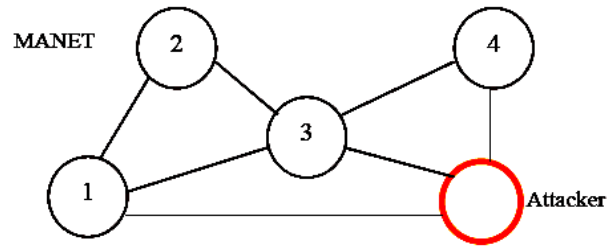

Figure 5: Internal Attack

C. Worm Hole Attack

It is a kind of attack which targets MANET routing functionality. In this attack, a false impression is created by colluding nodes such that two distant regions of a MANET are directly connected via nodes which appear to be nearby although in reality those are far-away from one another [1], [25], [26]. This attack proves to be lethal on MANET routing where two attackers, connected by a very high

 DOI : 10.18231/2454-9150.2018.1302

speed off-channel link, are deliberately located at dissimilar points of a network.

D. Black Hole Attack

In a black hole attack, a malevolent node transmits false routing knowledge, announcing as if it has got optimized route and attracts remaining nodes to route data traffic through it [26]. The attacker node then misuses and castoffs the traffic which in turn destroys the network communication and causes network performance to reduce drastically.

E. Flooding Attack

The intention of the flooding attack [25], [26] is to wear out the network resources, like bandwidth. Also, it consumes resources like processing and battery power as well as disrupts the routing functionality that causes brutal deprivation in network performance.

F. Link Spoofing

In this kind of attack, a malevolent node announces forged links with non-neighbors to interrupt routing functionality and the attacking node than can manipulate information as well as alter routing traffic [25].

G. Link Withholding

In this attack, a wicked node neglects the necessity to publicize the link of particular nodes or a cluster of nodes [26]. This will end up in link loss for these nodes. The performance of OLSR protocol is critically harmed by this type of attack.

H. Replay

Alteration in Topology, i.e. physical arrangement, is quite obvious and repeated in MANET due to node movement. In a replay attack [25], [26], a node remembers control information of other nodes and resends them afterwards. This forces nodes to form their routing database with decayed route information. This attack is used to imitate a particular node or to bother the routing functionality of MANET routing.

I. Jellyfish Attack

Adding an end to end delay is the wicked intention of this kind of attack. In this type of attack, the attacker node seeks for access to the network [25]. As soon as it gets the space, it starts adding redundant delay to all information passing through it which in turn drastically alters the whole network performance.

J. Gray Hole Attack

The strategy of the attacker node remains partially same as the attacking node plans Black hole attack. The difference is that in this attack, packets are dropped with certain probability. The attacker node drop packets received from certain particular nodes whereas leaving all other packets intact [25], [26]. This changing suspicious and normal behavior makes it quite difficult to differentiate evil node.

III. BLACK HOLE ATTACK IN MANET

Black Hole attack is an Internal type of attack that takes place at Network layer and is very tricky to recognize [10]. A black hole node transmits forged routing information by claiming to have optimized route to destination and hence consumes majority of the packets. This strategy degrades the network performance by increasing workload due to unwanted transmission as well as reduces network lifetime by consuming more energy by dropping critical packets [16].

As shown in Figure 6, presume P as a source node, R as a Black Hole attacker node and U is the destination mode. P wants to communicate to U but it does not have the path to U in its routing entries. Hence, it broadcasts RREQ (Route Request) packets to its neighbors Q, S and V. On receiving the RREQ packet, nodes S, V look their cache to find the route. On the other side, node Q sends the RREP (Route Reply) packet to P before any other nodes with advanced sequence number as node R advertises itself has got the route to U. Node P on receiving RREP assumes that node Q has the path and hence sends the data packets to it. On reception of data packets, immediately black hole node R drops all of them, while source node P assumes that data packet will reach to the destination node U [9], [12], [13], [14], [15], [20]. The node R is identified as a malicious attacker node and the type of attack is well-known as Black Hole Attack. There could be single or multiple attackers in the network.

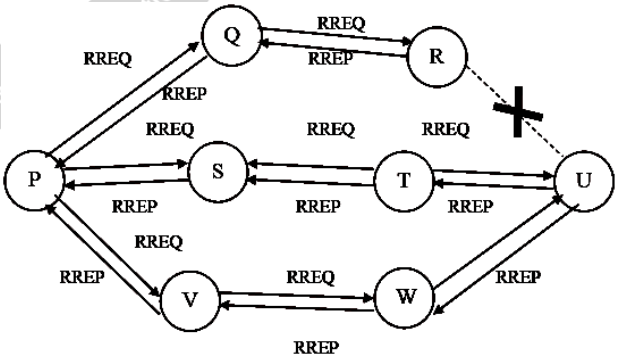

Figure 6: Black Hole Attack in MANET

IV. SIMULATION ENVIRONMENT

Network Simulator (*ns-2*), NS2 Scenarios Generator (NSG) and Automated Post Processing (APP) tool are used to simulate topology, generate tcl script and plot graphs from trace data respectively [22], [23]. Figure 7 & 8 show the topologies used to simulate and analyze the effect of Single Black Hole Attack on the performance of MANET

 DOI : 10.18231/2454-9150.2018.1302

routing protocols. Topology I & II consist of seven mobile nodes and all are having their own mobility and other parameter constraints. Some standard parameters which are set to create realistic scenario are tabulated in Table 1. Topology-I shows routing without an attacker node whereas Topology-II feels the presence of an attacker, node number 5 as an attacker node, during routing. Attacker node intentionally sends fake information claiming optimum route to destination and attracts most of the traffic to pass through it [24]. It consumes all incoming packets and drops them; hence routing as well as packet transfer ratio is altered to a great extent which finally results in complete destruction of the network.

Simulation topology III of Figure 9 simulates the effect of multiple nodes with multiple Black Hole Attacks in MANET routing. Simulation Scenario consists of 25 nodes where node number 11, 17 and 20 are acting as source nodes, node number 18 is a destination node and node number 1, 7 and 13 are malicious nodes which generate Black Hole Attacks. Simulation parameters for Topology III are listed in Table 2.

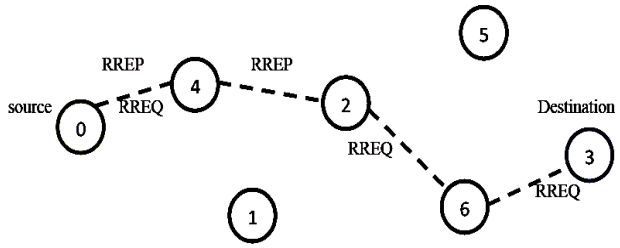

Figure 7: Simulation Topology – I

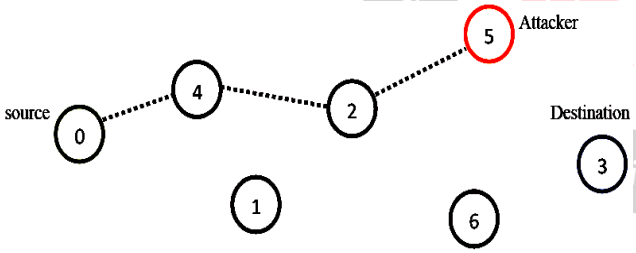

Figure 8: Simulation Topology – II

Table 1: Simulation Parameters (Topology I & II)

Simulator	NS2
Traffic	CBR
No. of nodes	7
Malicious node	1
Attack	Black hole
Protocol	AODV
Packet size	1500 for CBR
Topology	800 x 541
Stop time	100 sec
Data rate	Mbps

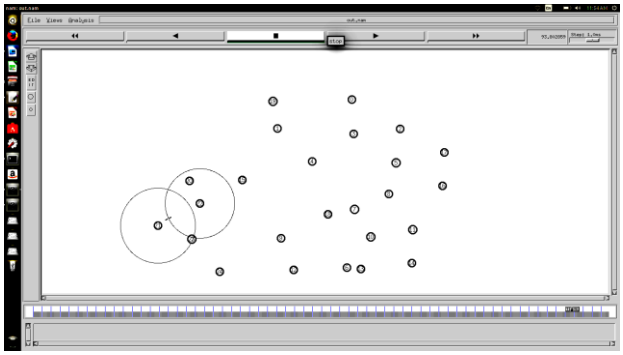

Figure 9: Simulation Topology – III

Table 2: Simulation Parameters (Topology III)

Simulator	NS2
Traffic	CBR
No. of nodes	25
Malicious attack	3
Attack	Black hole
Protocol	AODV
Packet size	1000 for CBR
Stop time	100 sec
Data Rate	0.1 Mbps

V. Simulation Results And Discussion

Simulation results for topology I and II are tabulated in Table 3 and 4 respectively. Simulations are carried out for 100 seconds to see the initial response as well as steady state response of the routing protocols and to observe the effect of Black Hole Attack and its consequences on the performance of the network. As shown in Table 3, in case of no Black Hole Attack, there are equal numbers of packets transmitted and received and hence packet transferred ratio is maintained at 1. Whereas, in case of Black Hole Attack, attacker attracts the transmitted packets by means of fake advertisement and drops all of them. This in turn, does not allow any packets to reach to the destination and gradually whole network routing gets disturbed and it experiences major communication gap between the nodes. Observations tabulated in Table 4 justify the problem discussed above by means of zero packets received and a zero packet transfer ratio. Figures 10, 11 and 12 graphically represent the performance of AODV protocol in terms of instantaneous throughput, goodput and delay respectively. The performance of AODV protocol, in absence of Black Hole Attack, increases linearly as route are getting developed between the nodes and routing becomes easy and quick. After initial response, performance achieves average throughput around 247Kbps, as shown in Table 5, in steady state condition. In case of multiple Black Hole Attacks, results show zero packets received at receiving node 18 with 11, 17 and 20 as transmitting nodes.

 DOI : 10.18231/2454-9150.2018.1302

Table 3: CBR output without black hole Attack -Topology I

Send line(s)	1238
Receive line(r)	1238
Forward line(f)	2478
Ratio of r/s	1

Table 4: CBR output with black hole Attack – Topology II

Send line(s)	1238
Receive line(r)	0
Forward line(f)	2478
Ratio of r/s	0

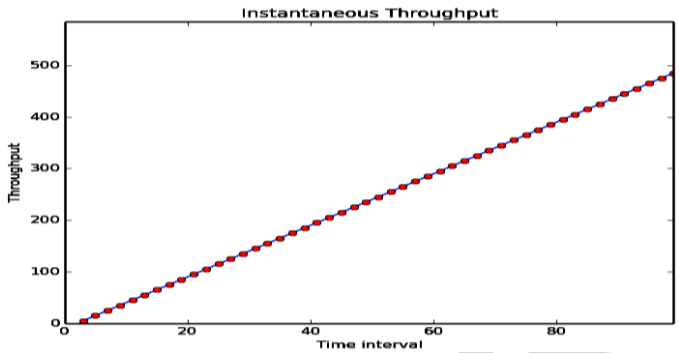

Figure 10: Instantaneous Throughput - Topology I & II

Table 5: Throughput Data - Topology I & II

Average throughput	
Start Time	1
Stop Time	99
Received Packets	4970
Avg. Throughput [kbps]	247.526

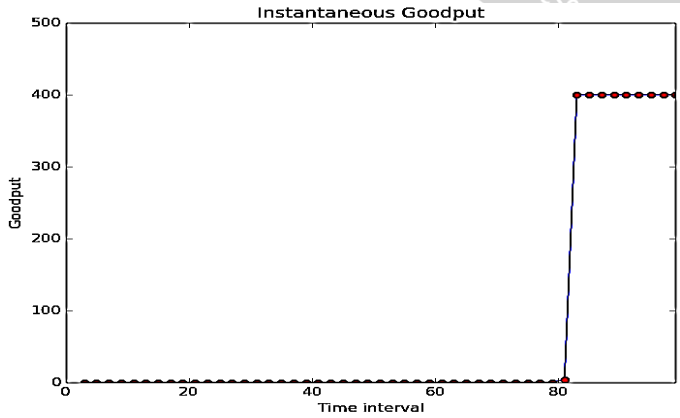

Figure 11: Instantaneous Goodput – Topology I & II

Figure 12: Instantaneous Delay – Topology I & II

VI. Conclusion

MANET has evolved as an application specific network with enhanced functionalities and features but at the cost of major concerns related to vulnerability to the common threats which frequently attack networks. The study in this paper shows that this kind of open and least secured network with mobility constraints are bound to get affected in routing process by various types of attacks which in turn drastically reduce the overall network performance. Simulation results and analysis reflect how single as well as multiple Black Hole Attacks can take place internally or externally as well as actively or passively. In-depth analysis also discovers how the strategy of attracting the routing traffic by temptation of having path to the destination through it, stops packets reaching to the receiver as well as destroys the complete communication between the source, destination and intermediate nodes. Hence, there is a prompt requirement of explicit detection and correction mechanisms for each kind of attacks to achieve an adequate routing performance in MANET.

References

[1] M. Elboukhari, M. Azizi, and A. Azizi, “Impact Analysis of Black Hole Attacks on Mobile Ad Hoc Networks Performance,” *Int. J. Grid Comput. Appl.*, vol. 6, no. 1/2, pp. 1–11, Jun. 2015.

[2] N. Tiwari and R. Yadav, “Detection of Black Hole Attack using Control Packets in AODV Protocol for MANET,” *Int. J. Comput. Appl.*, vol. 118, no. 24, pp. 23–29, May 2015.

[3] K. Munjal, S. Verma, and A. Bakshi, “IJMIE A Monthly Double-Blind Peer Reviewed Refereed Open Access International e-Journal-Included in the International Serial Directories Cooperative Black Hole Node Detection by Modifying AODV,” 2012.

 DOI : 10.18231/2454-9150.2018.1302

[4] S. Sarkar, T. Basavaraju, and C. Puttamadappa, *Ad hoc mobile wireless networks: principles, protocols, and applications*. 2016.

[5] A. Bakshi, A. Sharma, A. M.-I. J. of, and undefined 2013, "Significance of mobile AD-HOC networks (MANETS)," *pdfs.semanticscholar.org*.

[6] E. M. Royer and Chai-Keong Toh, "A review of current routing protocols for ad hoc mobile wireless networks," *IEEE Pers. Commun.*, vol. 6, no. 2, pp. 46–55, Apr. 1999.

[7] M. Bhat, D. Shwetha, … D. M.-… journal of computer, and undefined 2011, "SCENARIO BASED STUDY OF ON-DEMAND REACTIVE ROUTING PROTOCOL FOR IEEE-802. 11 AND 802. 15. 4 STANDARDS," *Technopark Publ.*

[8] K. G.-A. M. in computer science, undefined pp-1-36, and undefined 2006, "Routing protocols in mobile ad-hoc networks," *academia.edu*.

[9] E. Royer, C. P.-U. of California, S. Barbara, and undefined 1999, "Multicast Operation of the Ad-hoc On-Demand Distance Vector Routing Algorithm," *people.cs.ucsb.edu*.

[10] G. Jayakumar, G. G.-I. J. of Computer, and undefined 2007, "Performance comparison of mobile ad-hoc network routing protocol," *researchgate.net*.

[11] N. Sharma, A. S.-A. C. & Communication, and undefined 2012, "The black-hole node attack in MANET," *ieeexplore.ieee.org*.

[12] M. K. Marina and S. R. Das, "Ad hoc on-demand multipath distance vector routing," *Wirel. Commun. Mob. Comput.*, vol. 6, no. 7, pp. 969–988, Nov. 2006.

[13] "Reactive protocols - AODV." [Online]. Available: http://www.olsr.org/docs/report_html/node16.html#adhoc_aodv#adhoc_aodv %E2%80%93accessed on may-2009. [Accessed: 15-Jan-2019].

[14] A. Rahman, Z. Z.-E. J. of S. Research, and undefined 2009, "Performance comparison of AODV, DSDV and I-DSDV routing protocols in mobile ad hoc networks," *Citeseer*.

[15] C. Perkins, P. B.-A. S. computer communication, and undefined 1994, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," *dl.acm.org*.

[16] H. Nguyen, U. N.-A. H. Networks, and undefined 2008, "A study of different types of attacks on multicast in mobile ad hoc networks," *Elsevier*.

[17] M. Abolhasan, T. Wysocki, E. D.-A. hoc networks, and undefined 2004, "A review of routing protocols for mobile ad hoc networks," *Elsevier*.

[18] I. Chlamtac, M. Conti, J. L.-A. hoc networks, and undefined 2003, "Mobile ad hoc networking: imperatives and challenges," *Elsevier*.

[19] S. Sesay, Z. Yang, J. H.-I. T. Journal, and undefined 2004, "A survey on mobile ad hoc wireless network," *docsdrive.com*.

[20] L. Abusalah, A. Khokhar, M. G.-I. C. Surveys, and undefined 2008, "A survey of secure mobile ad hoc routing protocols.," *academia.edu*.

[21] S. Mohapatra, P. K.-P. Engineering, and undefined 2012, "Performance analysis of AODV, DSR, OLSR and DSDV routing protocols using NS2 Simulator," *Elsevier*.

[22] T. Issariyakul and E. Hossain, "Introduction to Network Simulator 2 (NS2)," in *Introduction to Network Simulator NS2*, Boston, MA: Springer US, 2012, pp. 21–40.

[23] "NSG2 - Peng-Jung Wu." [Online]. Available: https://sites.google.com/site/pengjungwu/nsg. [Accessed: 15-Jan-2019].

[24] "Mohit P. Tahiliani." [Online]. Available: http://mohittahiliani.blogspot.com/. [Accessed: 15-Jan-2019].

[25] S. Kaushal and R. Aggarwal, "A study of different types of attacks in MANET and performance analysis of AODV protocol against wormhole attack," 2015.

[26] J. Verma, P. Shukla, R. P.- traffic, and undefined 2016, "Survey of various Trust based QoS aware Routing Protocol in MANET," *researchgate.net*.

 DOI : 10.18231/2454-9150.2018.1302