ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# SIMULATION BASED PERFORMANCE ANALYSIS OF MOBILE AD HOC NETWORK UNDER THE INFLUENCE OF ROUTE REQUEST FLOODING ATTACK

**Raman Preet[*1], Dr. Shaveta Rani [2], Dr. Paramjeet Singh [3]**
[*1]Research Scholar, I.K. Gujral Punjab Tehnical University, Kapurthala, Punjab, INDIA
[1,2]Professor, Gaini Zail Singh Campus College of Engineering & Technology (MRSPTU), Bathinda, Punjab, INDIA

**DOI**: 10.5281/zenodo.1066234

## ABSTRACT

In this paper, we investigate the impact of Route REQuest (RREQ) flooding attack on mobile ad hoc network (MANET). RREQ flooding is performed by nodes that intend to degrade the network performance and are generally called malicious nodes. Malicious nodes behave like legitimate nodes present in the network, only with a single difference that they perform route discoveries very frequently as compared to legitimate nodes. Using simulations, we show that the basic route discovery mechanism used by popular reactive protocols such as Ad Hoc On-demand Distance Vector (AODV) and Distance Source Routing (DSR) can be exploited by such malicious nodes to bring down the network performance drastically. The major objective of this `simulation based study is to figure out the reactive protocol that performs better under RREQ flooding attack so that, it could further be improved to detect and isolate malicious node(s) to ensure security in MANET. Extensive simulations are performed using network simulator NS-2 and performance of network is measured using parameters such as Packet Delivery Ratio (PDR), Average End-To-End Delay, Throughput and Jitter.

**KEYWORDS**: MANET, AODV, DSR, Simulation, RREQ, RREP, NS-2

## I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a temporary network constituted using heterogeneous mobile nodes that interconnect each other utilizing wireless links without any infrastructure or administrative support. Each node performs the functionalities of a host and a router, forwarding packets, extending their cooperation in carrying communication within network. Nodes constituting the network are randomly located in such a manner that the interconnections existing between nodes can change frequently making the network topology totally dynamic [1][2]. Nodes have the freedom to move into and out of a network. Nodes carry multi-hop communication with restricted battery capacities, limited bandwidth and minimal physical security. Due to these characteristics, MANETs popup as one of the best alternatives for interconnecting mobile devices rapidly for establishing communication in flood hit areas, battle fields, ad hoc conferencing and so on. Thus lack of infrastructure, open architecture and constrained environment, make MANET vulnerable to a variety of attacks [3].Route Request flooding attack [4] [5] is one of the serious attacks that has the ability to disrupt the network performance drastically, leading to denial of service [6]. In this paper we implement RREQ flooding attack in two popular reactive routing protocols – AODV and DSR to study and compare their performance.

## II. ROUTING IN MANETs

A major challenge in dynamically varying, bandwidth constrained, multi-hop, self-organizing wireless mobile ad hoc network is to find efficient routes for establishing uninterrupted communication between two communicating nodes. Each node in ad hoc network performs dual task of host as well as of a router. Therefore, routing protocols play a very important in these networks. Routing protocols in MANETs are divided into three categories (1) Table Driven or Proactive routing protocols (2) On-Demand or Reactive protocols (3) Hybrid Routing protocols. Studies reveal that, protocols falling under reactive category depict better performance as compared to proactive and hybrid category due to their reduced memory consumption and low control overhead. Moreover, route discovery and maintenance procedure in table driven and hybrid protocols push their

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

performances, comparatively down, due to the fact that they detect broken links in a slow manner and keep on exchanging and updating their routing information, when not desired also[13][14][15]. Therefore, in this paper we investigate and later compare the performance of AODV and DSR reactive routing protocols under RREQ flooding attack using simulations.

## III. GENERAL CHARACTERISTICS OF REACTIVE ROUTING PROTOCOLS

Reactive routing protocols discover the routes between the communicating nodes on "as needed" basis. For initiating communication, the source invokes a route discovery process by broadcasting route request (RREQ) control packets in the network. Assuming that the links are bidirectional in nature, a route reply (RREP) control packet is sent back to the source node using link reversal by the destination or an intermediate node having a fresh route to the required destination. The pool of reactive protocols, include protocols like Ad Hoc On-demand Distance Vector (AODV) [8], Distance Source Routing (DSR) [9], Dynamic Manet On-demand (DYMO) [10], Cluster based Routing Protocol (CBRP) [11], Signal Stability based Adaptive routing protocol (SSA) [12]etc. In this section two most important protocols AODV and DSR are discussed.

## IV. AODV

### Overview

Ad hoc On-Demand Distance Vector (AODV) [8][16] [17] is a reactive routing protocol for wireless ad hoc network. In this protocol a node initiates its search for a route to some destination node only when it wishes to transmit some data to the destination node. AODV is programmed for two operating modes namely: (1) Route Discovery mode and (2) Route Maintenance mode.

### Route Discovery in AODV

When a node is in need to transmit data and has no valid route in its routing table to the intended recipient/destination, it starts a route discovery process. For discovering routes, the source node broadcasts RREQ control packet to its neighbors. When the neighboring nodes receive the RREQ control packet, they broadcast the RREQ control packet further if they do not have a fresh enough route to the required destination in their routing tables as shown in figure 1 below.

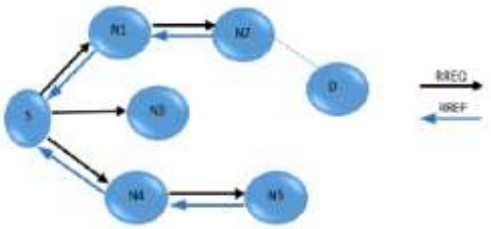


***Figure 1: Route Discovery in AODV using RREQ and RREP***

When the route request control packet reaches the intended destination or some intermediate node in possession of a valid route to the destination then, a Route REPly (RREP) control packet is framed and unicast to the source node. After receiving the RREP, the source node initiates transmitting data to the desired destination. During this phase if the source receives any other RREP packet stamped with a higher sequence number or the same sequence number with the less number of hops, it refreshes its routing table and uses the optimum route to the destination.

### Route maintenance in AODV

In AODV protocol, Hello packets are used to sustain routes. These packets are periodically sent by nodes in the network to provide connectivity information to their neighboring nodes. In this protocol a route remain active as long as a periodic flow of data takes places between source and destination. The link times out when the source stops sending data packets and eventually the route gets deleted from the routing tables of intermediate nodes. But if, a link breaks while the route is active state, the node lying upstream towards the link break transmits a Route ERRor (RERR) control message to the source stating that the destination has become unreachable. After

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

the receipt of RERR control message, the source node reinitiate route discovery process if needs to establish a route to the unreachable destination.

## V. DSR

### Overview

Another popular on-demand routing protocol is Dynamic Source Routing (DSR) [9] [18]. DSR is designed to handle wireless communication using multiple hops in wireless ad hoc networks. It utilizes source routing, that is the source is well aware of the complete route to the intended destination. An entire chain of intermediate nodes leading to the destination node are put in the header of each data packet. This protocol operates in two modes: (1) Route Discovery (2) Route Maintenance. Both these mechanisms operate fully "on demand".

### Route Discovery in DSR

Route discovery mechanism is initiated by any source node that intends to send some data a destination node and does not possess a route to it. For sending data the node first tries to fetch a route to the intended destination in its own route cache from the earlier recorded routes. If it succeeds in locating a route, the route information in embedded in the data before its transit. If fails to locate, it initiates route discovery process to locate a new route to intended destination by broadcasting a RREQ packet.

In figure2, if node S wants to send some data to destination node D and does not possess a route to it, then node S will initiate the route discovery mechanism by sending RREQ control packet.

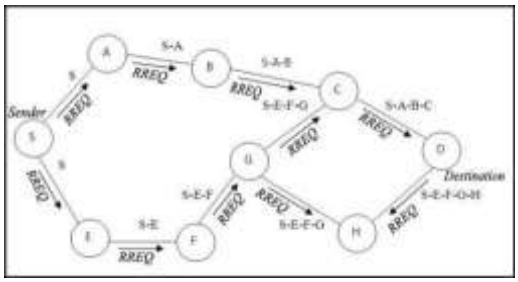


***Figure 2: Route discover using RREQ packet in DSR***

When this RREQ packet is received by some intermediate node, if it turns out to be the intended destination it returns a Route REPly (RREP) control message to the node S by providing a copy of the accumulated route details from the RREQ packet. On receiving this RREP, node S stores the route in its Route Cache for future use. If some other intermediate node receives a successive copy of the same RREQ, rejects it. The RREQ is also rejected if any intermediate node finds its own address existing in the RREQ. In other situation this node broadcasts the RREQ with same request id with its address appended to the route record in it.

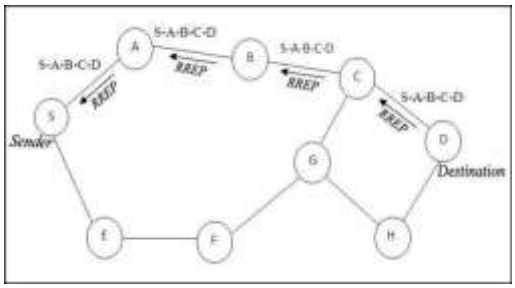


***Figure 3: Route reply using RREP packet in DSR***

For responding back to node S, node D searches its route cache, trying to locate a route back to node S. If node D finds one, it uses it for delivering RREP packet otherwise D executes route discovery process for source S.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

**Route Maintenance in DSR**

During the maintenance of routes, considering the scenario in figure 4, if node C is not able to link to its next hop neighbor D, C returns a RERR to node A, informing it about the broken link between C and D. Subsequently A deletes the broken route information from its cache. For retransmitting to node E, if node A finds alternative route to it, it uses that route for sending data immediately, otherwise it initiates a new route discovery process for communicating with node E.

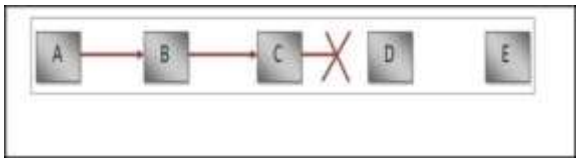


***Figure 4: Route maintenance in DSR***

## VI. EFFECTS OF RREQ FLOODING

The basic aim behind RREQ flooding is to degrade the network performance. In RREQ flooding, a malicious node floods the network with a large number of fake RREQs to non-existent a destination. Since the destination targeted is non-existent, a RREP control packet can't be propagated by any node in network. When such a situation occurs, the entire network gets congested with fake RREQs consuming significant proportions of the network capacity leading to the depletion of bandwidth available for data to be transmitted. In addition the routing tables tend to accumulate a lot of data pertaining to reverse routes to the source of fake packet generator. This often leads to overflow in routing tables and creates a situation where nodes start showing their inability to record new valid routes. RREQ flooding not only exhausts the network resources but consumes computational and battery power of nodes [23] [24] 25] [7] [27]. All these ill- effects cause serious disruption to the routing operations leading to severe degradation in network performance. These effects can be summarized as:

1. Formation of longer routes where shorter routes could have been possible under normal conditions.
2. Unnecessary consumption of memory in maintaining entries in routing table pertaining to bogus route requests.
3. Consumption of constrained processing power.
4. Depletion of the node's battery power.
5. Leading to reduced throughput of the network.
6. Denial of services to legitimate nodes in the network.

## VII. RELATED WORK

Alokparna Bandyopadhyay et al. [7] have described the effect of flooding attack in MANET using NS-3 simulator. Authors have chosen AODV for their experimentation and reported that due to heavy flooding in the network, there is an increase in parameters like average packet loss percentage, average routing overhead, average consumption of bandwidth etc.

Dong-Won K. et al. [26] evaluated the working performance AODV and DYMO protocols with respect to node mobility. Simulations performed show the accumulation of path in DYMO protocol reduces the routing overhead. At high mobility speed, throughput of DYMO can be better than the throughput of AODV.

HoudaMoudni et al. [24] analyzed the effect of black-hole, flooding and rushing attacks in wireless ad hoc networks. Authors present a comparison of performances that were shown by AODV under the three attacks with standard AODV in terms of metrics like PDR, average end to end delay and average throughput and observed a drop in all metrics under attacks.

M. Omari et al [29] performed simulations and later made comparison of DSR and DYMO protocols in MANETs. The two routing protocols are compared in terms of mean delay, throughput, number of collisions, number of dropped packets using OMNET simulator. They concluded that DYMO performs better than DSR in all metrics taken into consideration.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Ping Yi et al [19] studied the network performance in terms of flooding frequency, network bandwidth, number of attacker nodes and number of normal nodes. Authors analyzed that, in DSR protocol, with increasing frequency of attack, the packet delay initially increases and then declines to a stable value towards the end.

## VIII. RESULTS AND DISCCUSSION

### SIMULATIONS PERFORMED

NS-2 network simulator[28] [29]is used for simulating mobile ad hoc network and implementing route request flooding in it, firstly by considering AODV protocol and then DSR protocol. Simulations are performed by taking a network comprising 100 mobile nodes and varying number of RREQ flooding malicious nodes from 0 to 20. We use Random waypoint as the mobility model to achieve movement of nodes. Each node initiates movement at random speed from its initial location and traffic type is taken as CBR. Numerous parameters set for simulation are:

***Table 1: Parameters used in simulation***

| PARAMETER | VALUE |
|---|---|
| Channel Type | Wireless |
| Simulation Area | 1500 * 1500 |
| Routing Protocols | AODV, DSR |
| Number of mobile nodes | 100 |
| Number of malicious/flooding nodes | 0, 5, 10, 15, 20 |
| Packet size | 512 bytes/packet |
| Traffic type | CBR |
| Pause time | 30 s |
| MAC type | IEEE 802.11 |
| Mobility | Random way point |
| Packet Rate | 2 packets/second |
| Mobility speed | 4 m/sec |
| Number of packets from each source | 198 |
| Simulation Time | 100 ms |
| Transmission Range | 250 m |

### PERFORMANCE EVALUATION

#### *PACKET DELIVERY RATIO (PDR)*

PDR ratio represents a ratio of the count of packets received at the destination to that of count of packets sent by the source. For the purpose of comparing, a protocol showing a higher PDR is considered better. As shown in figure 5, PDR in AODV is better than that of DSR. The reason behind this result is that, the introduced RREQ flooding attack led to slow route discovery in case of DSR as it employs source routing. AODV performs better as RRER is communicated at every node, making it easy to update the routes. Therefore, PDR in AODV is less affected with the increase in the number of attacking nodes.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

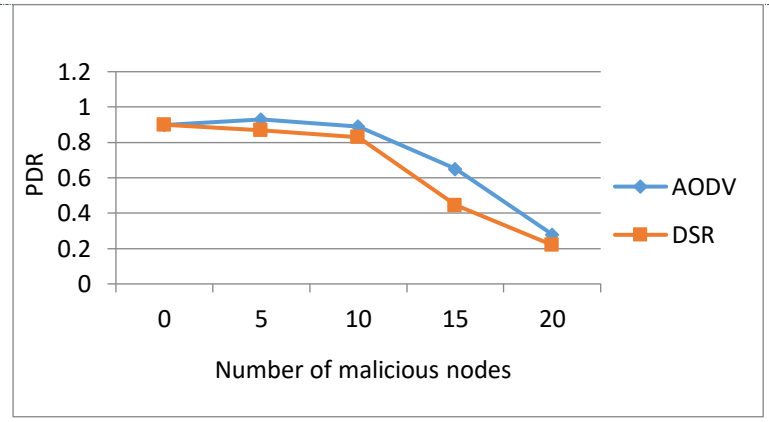


***Figure 5: Number of malicious nodes vs. PDR***

### *AVERAGE END-TO-END DELAY*

It is the total time consumed in seconds by a packet to reach its destination from the source. In contrast to PDR, average end-to-end delay should be minimum for better performing protocol. End-to-end delay in AODV and DSR with flooding introduced is shown in figure 6. The plotted curves depict that, with the increase in the number of flooding nodes, average end-to-end is more in DSR as compared to in AODV. The graph output indicates this because with the increasing number of attacking nodes, DSR is forced to update more routes, increasing its end-to-end delay whereas AODV shows better response in updating its routes.

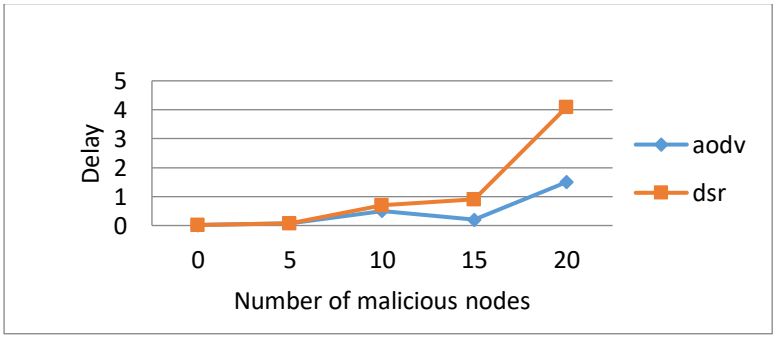


***Figure 6: Number of malicious nodes vs. Delay***

### *JITTER*

Jitter is the measure of variation/difference in end-to-end delay and it must be less for the better performing protocol. As shown in figure 7, performance of AODV is better as compared to DSR.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

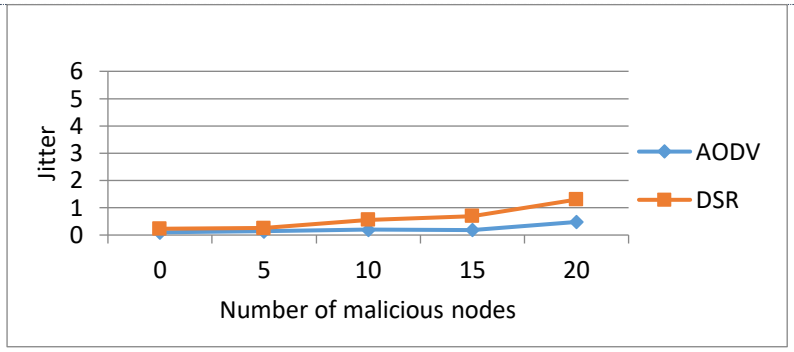


***Figure 7: Number of malicious nodes vs. Jitter***

### *THROUGHPUT*

Throughput is one of the important metrics to account for network's performance. It is computed by taking total number of data packets received at destinations in one second. Figure 8 shows the comparison of AODV and DSR in terms of throughput. Like PDR, protocol depicting higher throughput should be considered, a better performer. Results clearly show that, AODV performs better as compared to DSR under RREQ flooding attack. DSR trails behind in performance because most of the bandwidth here is wasted in maintaining routes.

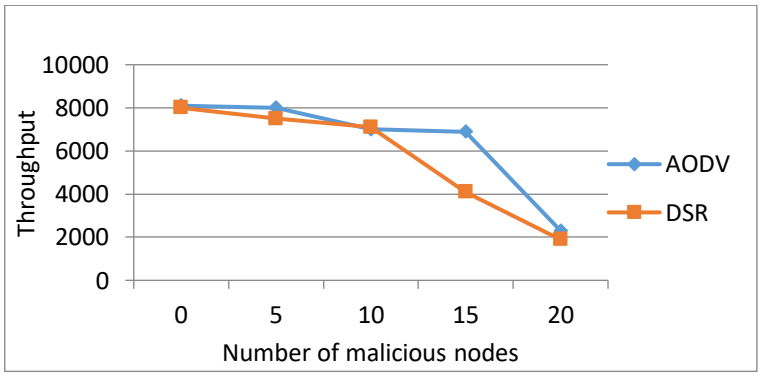


***Figure 8: Number of malicious nodes vs. Throughput***

## IX. CONCLUSION

This paper briefly provides an overview of AODV and DSR reactive routing protocols along with their simulation based performance study. The simulations are performed in NS-2 simulator. Route Request (RREQ) flooding attack is implemented in NS-2 and the performance of both the reactive protocols are observed in terms of average end-to-end delay, packet delivery ratio, jitter and throughput. It is observed that with the increase in number of flooding nodes, AODV routing protocol performs better than DSR protocol in terms all the four parameters taken into consideration.

In future, the work carried in this paper can be extended by enhancing the performance of AODV protocol by devising a RREQ flooding detection and isolation mechanism in it to enhance the security of wireless mobile ad hoc networks. The study could include additional parameters such as end-to-end energy consumption, malicious-node-detection ratio etc.

## X. REFERENCES

[1] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", Internet Request for comment RFC 2501, Jan 1999.
[2] Ramanathan, Redi J, "Abrief overview of ad hoc networks: challenges and directions", IEEE communication magazine, pp. 20-22, 2002
[3] Wu, B., Chen, J., Wu, J., and Cardei, M., "A survey of attacks and countermeasures in mobile ad hoc networks", Wireless network security, Springer US, pp. 103-135, 2007.
[4] Muhammad O Pervaiz, Mihaela Cardei and Jei Wu, "Routing security in ad hoc wireless networks", Department of Computer Science and Engg, Florida Atlantic University, Boca Raton, FL 33431.
[5] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", Proc. of Wireless Communications, IEEE, Oct 2007, Issue 5, pgs 85-91.
[6] R. H. Khokhar, M. A. Ngadi, S. Mandala, "A Review of Current Routing Attacks In Mobile Ad Hoc Networks", International Journal of Computer Science and Security (IJCSS), Volume 2, Issue 3, pp. 18-29, June 2008.
[7] Alokparna Bandyopadhyay, Satyanarayana Vuppala and Prasenjit Choudhury, "A Simulation Analysis of Flooding Attack in MANET using NS-3", in Proc. of the International Conference on Wireless communications, Vehicular Technology, Information Theory and Aerospace & Electronic System Technology (WVITAE2011), March 2011.
[8] C. Perkins, E. Royer, "Ad-hoc On-Demand Distance Vector Routing", Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications, 1999, pp. 90-100.
[9] D.Johnson, D. Maltz, "Dynamic Source Routing in AdHoc Wireless Networks", Mobile Computing, Editors: T. Imielinski and H. Korth, pp. 153 – 181, Kluwer, 1996.
[10] I. Chakeres and C. Perkins, "Dynamic MANET On-Demand (DYMO) Routing," IETF Internet-Draft, draft-ietf-manet-dymo-17.txt, Mar. 2009.
[11] M.Jiang, J. Ji and Y.C. Tay, "Cluster based routing protocol", Internet Draft, draft-ietf-manet-cbrp-spec-01.txt, work in progress, 1999.
[12] R.Dube, C. Rais, K. Wang and S. Tripath, "Signal Stability based Adaptive Routing 9SSA0 for Ad hoc Networks", IEEE Personal Communcation, Vol. 4. No. 1. pp. 36-45,1997.
[13] J. Broach, D. A. Maltz, D. B. Johnson, Y. C. Hu and J. Jetcheva, "A performance comparision of multi-hop wireless ad hoc network routing protocols", In Proceeding 4th Annual ACM/IEEE International conference on Mobile Computing and Networking, pp.85-97, Oct 1998.
[14] S.R Das, R. Castaneda, J.Yan and R. Sengupta, "Comparative performance evaluation of routing protocols for mobile ad hoc networks, in Proceedings of the 7th International conference on Computer Communications and Networks (ICCCN), pp. 153-161, Oct 1998.
[15] T. Dyer and R.V. Boppana, "A comparison of TCP performance over three routing protocols for mobile ad hoc networks, In proceedings of ACM Mobihoc, October 2001.
[16] Perkins C.E., Terminology for Ad-Hoc Networking, Draft-IETF-MANET-terms-00.txt, November 1997.
[17] Perkins, C., Belding-Royer, E., & Das, S. (2003).Ad hoc on-demand distance vector (AODV) routing(No. RFC 3561).
[18] N. Karthikeyan, B. Bharathi, S. Karthik, "Performance Analysis of the Impact of Broadcast Mechanisms in AODV, DSR and DSDV" in IEEE Proceedings of the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering, February 2013.
[19] Ping Yi, Futai Zou, Van Zou, Zhiyang Wang, "Performance analysis of mobile ad hoc networks under flooding attacks", Journal of Systems Engineering and Electronics, Vol 22, Issue 2, BIAI Journals & Magazines, pp. 334-339, 2011
[20] Rohit Chourasia and Rajesh Kumar Boghey,"Novel IDS security against attacker routing misbehavior of packet dropping in MANET", IEEE 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence, pp. 456-460, 2017
[21] Hoang Lan Nguyen and Uyen Trang Nguyen, "A study of different types of attacks in mobile ad hoc networks", 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), pp. 1-6, 2012
[22] Kriti Chadha and Sushma Jain, "Impact of black hole and gray hole attack in AODV protocol", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), pp. 1-7, 2014.

[23] R. V. Boppana and S. Desilva, "Evaluation of a statistical technique to mitigate malicious control packets in ad hoc networks", IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks(WoWMoM'06), pp. 563, 2006.

[24] Houda Moudni, Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi, "Performance analysis of AODV routing protocol in MANET under the influence of routing attacks", IEEE International Conference on Electrical and Information Technologies (ICEIT), pp. 536-52, 2016

[25] S. Desilva; R. V. Boppana, "Mitigating malicious control packet floods in ad hoc networks", IEEE Wireless Communications and Networking Conference, pp. 2112-2117, 2005.

[26] Dong-Won. Jin-su Park. Y. ChoA, B. Cheon, "Performance analysis of AODV and DYMO routing protocols in MANET", IEEE CCNC proceedings, pp. 1-5, 2010

[27] http://www.isi.edu/nsnamlns/

[28] http://www.isi.edu/nsnamlns/tutorial/

[29] Mohammed O., A. Dahou, "Simulation comparison and analysis of DSR and DYMO protocols in MANETs", IEEE, International Conference on Industrial Informatics and Computer Systems (CIICS), pp. 1-6, 2016.