I J C T A, 9(24), 2016, pp. 145-152 ISSN: 0974-5572

A Trust Based Routing Protocol to Mitigate Denial of Service Attack in Manet

Alpa Sharma* and Sourav**

ABSTRACT

In Mobile Ad hoc Network attacks are a heavily researched area and draws a lot of consciousness in past years. The process that have ways of network node recovery is a topic of concern and new techniques have been evaluated along with the existing ones. The nodes present in the network are likely to be attacked and their data may be lost by isolating the node. This paper presents a novel ideal of acknowledgement based trust model in proactive routing protocol for prevention against Service Denial attack in MANET. Node in mobile environment have ability to pass through different clusters in its lifetime and its change count can be used in order to calculate its vulnerability towards various attacks. The results obtained were observed and compared and it was found to perform well when compared to traditional approach.

Keywords: MANET, Attacks, DoS, PDR, Adhoc.

1. INTRODUCTION

A mobile ad hoc network (MANET) is a progressively self-independent and infra structure-less network of mobile devices joined without wires. Every node in a MANET change its connection with other devices frequently and frees to move independently in any direction in the network territory. Every node should forwards traffic unconnected for its own account, and hence be a router [1]. A mobile ad hoc network (MANET) is called a mobile network that is interlinked, and is a self-trusted network of mobile nodes attached by telecommunication links. Application where MANET's are used is Military operations, Disaster relief, health care etc.

Routing protocols of MANET's have been built for to attain proficient routing In general, MANET routing protocols are split into two kind, table-driven routing protocols and on-demand routing protocols.

1.1. Proactive Routing Protocol (Table-driven)

In this table driven routing, every node prepares one or more table entries as per requirements that included updated information in row about path to any node within network [5]. These routing protocols maintain updated lists and information about the routes of destinations nodes and their route information is periodically being send throughout the network. The cons of such algorithms are particular amount of data and its preservation and time-consuming reaction on reorganization and non success. exemplar for proactive routing protocol is Destination Sequence Distance Vector (DSDV)

1.2. Reactive Routing Protocol (On-Demand)

In this type of protocol, route is exposed whenever it is required. Nodes initiate route discovery when asked. A route is formed by the initiating route discovery process by the source node. The main cons of such algorithms are High latency time in path finding and flooding in bulk takes to network congestion.

* M.E Scholar, *Email: alpasharma28@gmail.com*

** Assistant Professor Computer Science dept., Chandigarh University, Punjab, India, *Email: ssouravchhabra@gmail.com*

1.3. Hybrid Routing Protocol

In Hybrid routing protocol is a trade-off between on demand and table driven. Proactive protocols have large overhead and little latency while reactive protocols have little overhead and high latency.

1.4. Routing Attacks in Manet

Flooding attack: Flooding attack affects the network to interrupt the routing process. this attack affects the network resources like bandwidth, degrade performance level of the protocols. For example a malign node flood large no of packets in the network.

Black hole attack: Fake route is established to send a packets, A fake routing information is provided by malign node about the malign route, From that the packet in the network will go through malign route instead of optimum route. Those packets can be used by attacker .Attacker will have control on the traffic which can be misused.[5]

Worm hole attack: In the wormhole attack attackers fakes info about nodes that they are neighbor. But those nodes are non neighbor nodes. A tunnel is created between these nodes .And packets are forwarded through this route. Meanwhile the packets in the tunnel are recorded and replayed.

Denial of Service attack (Dos): In Denial of Service attack , a node is isolated from rest of the network so that it cannot be a part of communication process and thus to launch a attack. With effect to this victim node will not be able to send to or receive the packet but will remain in the network. The rest of the nodes in the network will not be able to build link with this victim node.[8]

This attack is only feasible when victim node is in transmission range. if it is not present then attack cannot be launched.

1.5. OLSR Protocol

OLSR (Optimized link State Link protocol) protocol comes under the category of proactive protocol. Exchange of messages takes pace periodically and therefore topology also changes. OLSR prevents from large no of transmission (flooding) by using the concept of multipoint relay(MPR).[8]

2. RELATED WORK

Biswas, S. et al [1] proposed a mobility locating checkpoint and formation of trust based rollback recovery algorithm to supply fault tolerance in MANET. Trust value of a mobile host based on four aspects: failure rate, availability in network, unused energy and recommendations from neighbor mobile hosts.

V. Deben, V. Divya Renga et al. [2] probabilistic rebroadcast protocol has been presented which is depending on neighbor exposure to reduce the routing overhead .The neighbor exposure information contains coverage ratio and association aspect in addition. A method is proposed to calculate the rebroadcast delay, which is used to evaluate the transiting manner and further efficiently utilize the neighbor exposure information.

Kejun Liu et. al [3] 2ACK technique is applied to get the acknowledgement from the receiver nodes to prevent against the misbehavior of selfish nodes.2ACK technique sends 2-hop acknowledgement packets in the reverse direction of the routing path. When the three consecutive nodes N1-N2-N3 are present in a route ,the N1 sends a data packet to N3 via N2.It is uncertain that N3 has received a packet. For the acknowledgement of the packets 2ACK technique is applied. which will be send by N3 to N1.

Kannhavong et. al [4] Node isolation attack is detected in the proposed mechanism. HELLO message and TC messages are verified after some interval of time. If these messages contain wrong information. The node will be supposed as malicious and can be detected. For example ,if a node T hears about transmission

from MPR due to wireless properties, it will know that the selected MPR node is malign. Selected MPR node sends TC message .Attacker will send HELLO message but not TC message. and will be declared as Malign.

Devesh Malik et. al [6] Secure network from node isolation attack is proposed. Standard OLSR protocol is identified.MPR selection is monitored carefully so that malicious node cannot be selected as MPR.VOTEFOR REQUEST and VOTEFOR REPLY messages are used in the selection process.

Schweitzer et. al [7] is tested for denial of service attack. The attacker obtains the topological information of the network and this information is used by the attacker to isolate the victim from the rest of the network. The OLSR protocol is implemented with the solution to defend the node by employing the same tactics used by the attacker.

Mohanapriya et. al [8] Defense against denial of service attack is proposed by enhancing existing OLSR protocol. Only authorized nodes took part in communication so that originator of packets can be identified and address of node cannot be spoofed. Authorization is done on the basis of trust factor by analyzing trust value for detecting malicious node.

The identity of HELLO messages are checked before assigning it as MPR. Along with HELLO and TC (Topology Control) messages 2 hop request and 2 hop reply with node query is which will verify the authenticity of the HELLO messages.

3. PROBLEM STATEMENT

Mobile Adhoc networks were built to communicate between two or multiple nodes but with the time it is realized that security is main concern to provide a reliable communication. With the increase in the threats and attacks to the wireless network ,it is a major challenge to protect the network from unwanted disruption. Several solutions are given by researchers on this issue. But it is difficult to say which protocol will perform best under given circumstances(threats).The objective of this work is to present a routing protocol which can prevent Denial of Service attack and can predict the route in real time by using the properties of proactive routing protocols. It is to be done by creating trusted environment but for reliable communication it is also necessary to follow acknowledgement based rule

The objective of this work is to propose a subsist proactive routing protocol

1) To detect Denial of service attack.
2) To build a trusted connection using trust based mechanism .
3) Use the proposed technique to prevent from denial of service attack.

4. PROPOSED METHODOLOGY

The presented approach retains an easy access memory which preserves the routing information in a row. Originally, every route in the network make use of reactive protocol which reduces the high bandwidth usage as compared to proactive protocol. and the information about the routes is placed in the memory that is restricted but retrieve the information fastly when compared to other memory. The routing information which is in the memory is timely , most common routes specified by reactive protocol can be easily observed but in case of proactive protocol ,routes are stationary and they are further saved in the memory. This helps to overcome drawback of reactive protocol in which flooding of network is not needed every time for the most common routes and delay for the route request. Every node in OLSR chose its MPR from the neighbor nodes. By selecting MPR unnecessary flooding is reduced because advertisement leads to have multiple replica of same messages at every node. Only those nodes can be selected as MPR which reaches maximum of its two hop neighbors. Only MPR nodes forward and advertise the messages

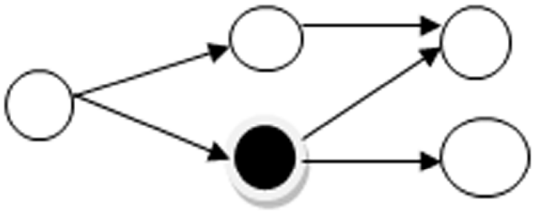

Figure 1:

From the fig 2. the colored node is selected as MPR because it is covering both 2 hop neighbors. OLSR protocol is best applicable in thick network. Trust factor is calculated for each node which further helps in isolating and DoS attacks. Two parameters are taken for calculating the trust factor i.e. frequency of its use and number of transmissions of the nodes. Frequency use of each node is saved in the memory with its route information. Trust factor is increased with the increase in frequency of use. The number of nodes retransmission depicts the loss of data when it transmitted from any node. The routing information managed in the memory which updates itself with respect to trust factor which decreases the routing overhead. A HELLO message is first sent to sense the nearby nodes and for selecting MPR. These HELLO messages are sent periodically after some time of interval (HELLO_INTERVAL). Depending on the trust values, the receiving nodes send an acknowledgement message. The total trust value of the nodes who have sent acknowledgement signal is calculated. When the trust value decreases from a certain threshold a DoS attack is detected. To isolate that node, a topology control message is used by calculating routes to neighboring nodes. The selected MPR nodes with highest trust values periodically send TC_INTERVAL) which carry address of MPR selector.TC messages are only send by MPR nodes. After learning the TC messages ,nodes can build the route with other nodes.

Pseudo code:

1: *Start*

2: *initialize* $n_{ci} \leftarrow 0$, *where* n_{ci} *is the nodecounto* fi^{th} *node*

3: *Route*(n_s, n_d), $\overline{Calculate}$ *the initial routes between* n_s *and* n_d,

where the source enode is denoted by n_s *and the destination node is denoted by* n_d

4: *for i: =* 0: *N, where the total no. of nodes in the network is denoted by N*

5: $NodeCache_i \leftarrow Route(n_i, n_d)$,

where Node Cache$_i$ *is the node cache of the source node i*

6: $n_{ci} \leftarrow n_{ci} + 1$, n_{ci} *is node counto* fi^{th} *node*

7: *for j*: = 0: *length* (m_i), *where*m_i *is the set of neigbbouring nodes of node i*

8: *if*(n_{cj} *is* maximum $\forall j$)

9: *Update Route*(n_i, n_d), n_i *in the route is trusted node*

10: *end if*

11: *Freq Route* (n_s, n_d), $\overline{stores}$ *the value of frequent route out of Route*

12: *end for*

13: *end for*

14: *end*

5. SIMULATION RESULT AND DISCUSSION

All the simulations are performed on system which has 4 GB RAM, 2.7 GHz processor and the tool used for it is MATLAB R2012b. The simulation outcomes are shown beneath. Above hitch is simulated for a state of 100 nodes distributed evenly in a 100 × 100 unit area

A Denial of service attack is simulated and the proposed algorithm is applied based on trust values and acknowledgements. The packet delivery ratio is calculated at each iterations and is plotted in Figure 3 when our algorithm is not applied. As it can be observed, with the DoS attack coming in place the Packet delivery Ratio (PDR) decreases drastically at around 11th epoch and continues to do so due to isolation of a critical node.

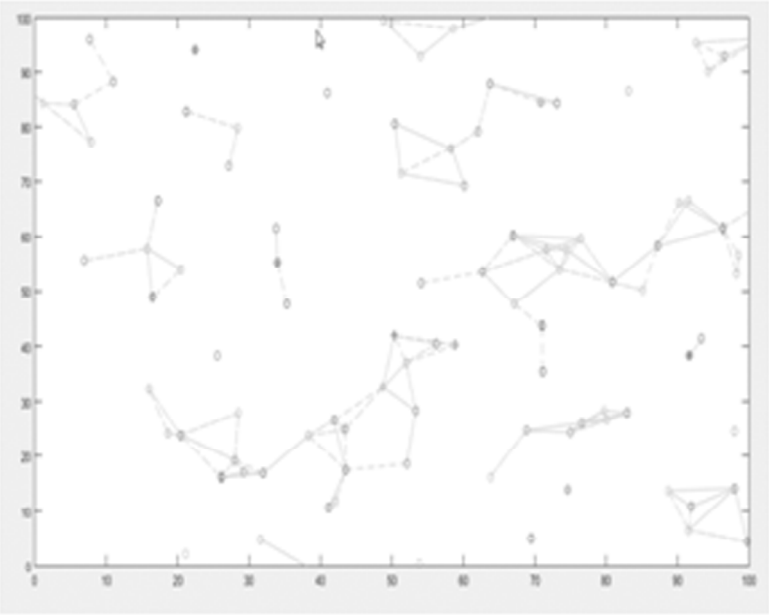

Figure 2: Mobile nodes in transmitting form

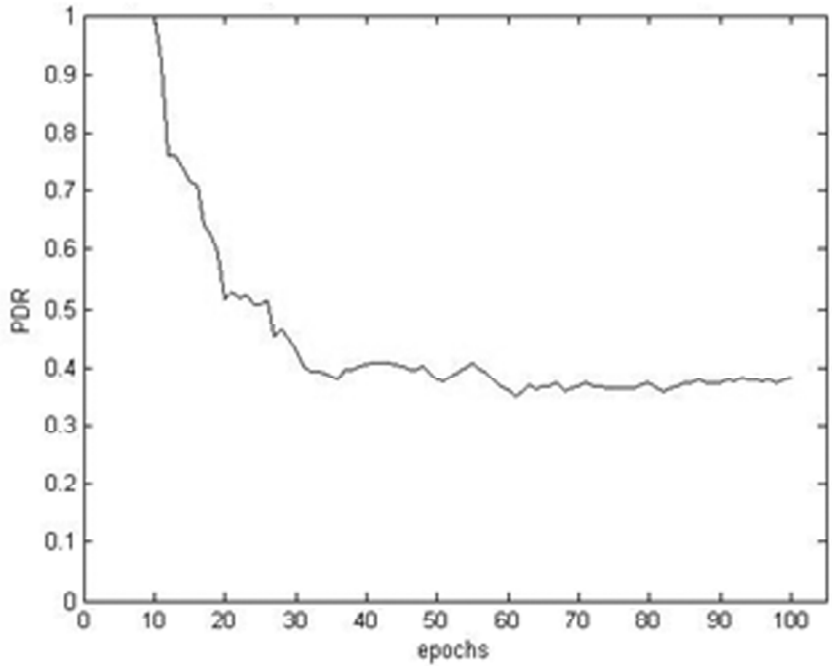

Figure 3: PDR without application of proposed algorithm

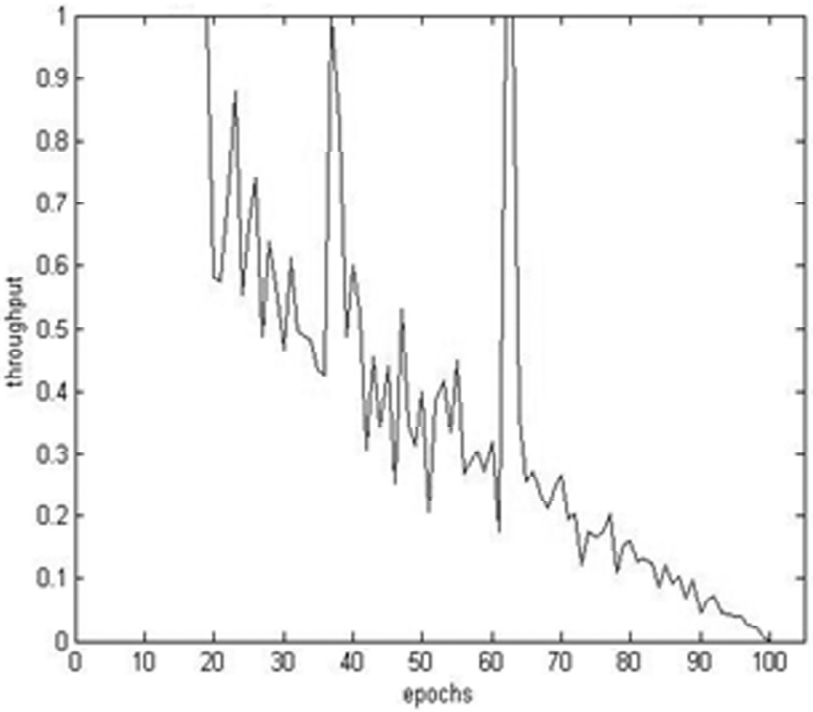

Figure 4: Throughput without proposed algorithm

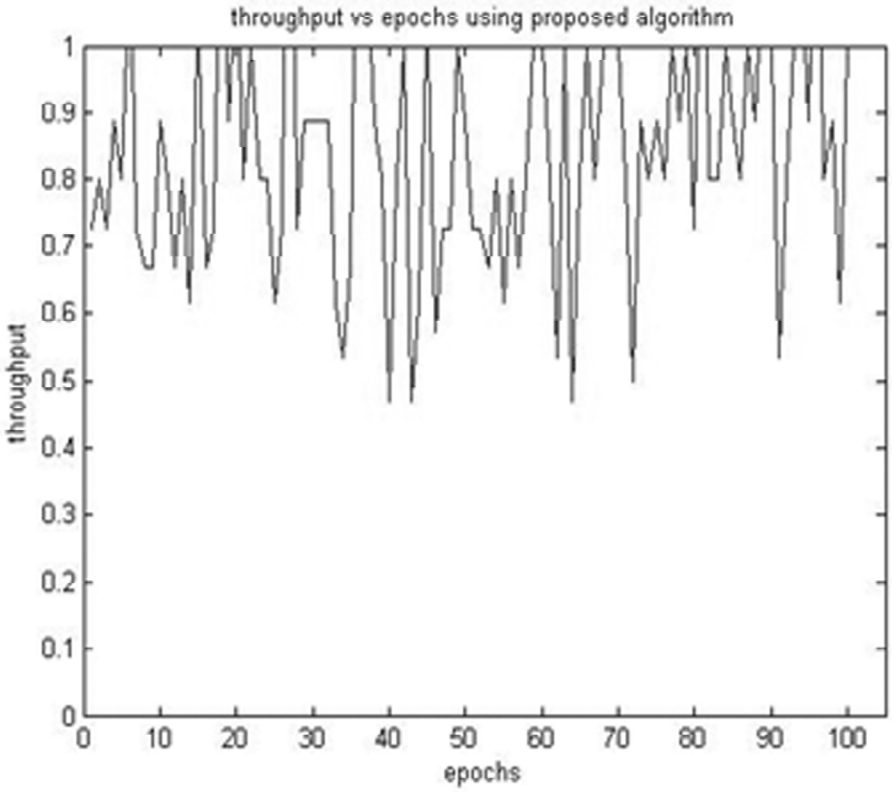

Figure 5: Throughput of proposed algo

Similarly, Figure 4 presents the throughput as a function of epoch which decreases with epoch when attack is in place without application of our detection algorithm.

Figure 6 and 7 presents the comparison of PDR and throughput when our algorithm is applied and in its absence. As is it is observed the algorithm performs better in finding the attack and improves the PDR and throughput.

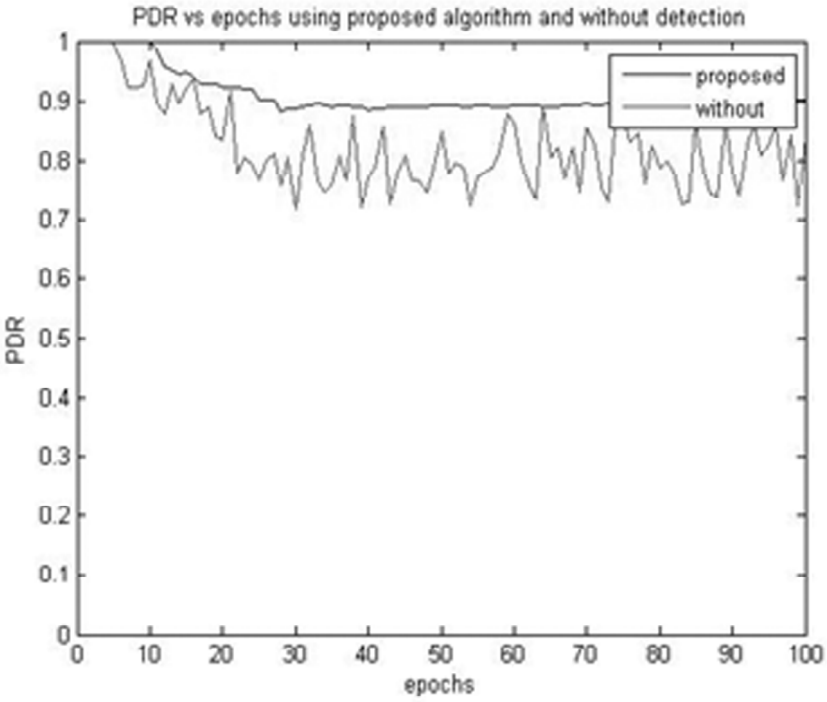

Figure 6: PDR Comparison

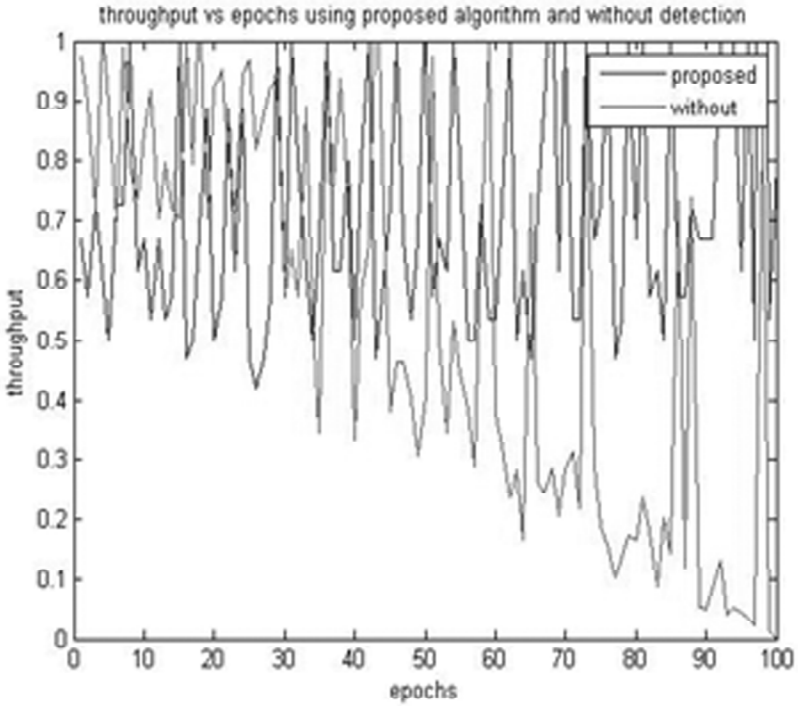

Figure 7: Throughput comparison

6. CONCLUSION AND FUTURE SCOPE

This paper presented a novel approach of trust mechanism and acknowledgment technique in proactive routing protocol in MANET for prevention of DoS attack. It was found to perform better in terms of throughput and PDR and is compared for performance.

For calculating the best route other algorithms like firefly in which firefly's attractiveness factor is taken as the energy and other packets during routing are attracted towards the nodes having the highest attractiveness value must also be used.

REFERENCES

[1] Biswas, Suparna, Sarmistha Neogy, and Priyanka Dey. "Mobility based check pointing and trust based recovery in MANET." *International Journal of Wireless & Mobile Networks* 4.4 (2012): 53.

[2] Biswas, Santosh, Prasenjit Dey, and Sarmistha Neogy. "Trusted check pointing based on ant colony optimization in MANET." *Emerging Applications of Information Technology (EAIT), 2012 Third International Conference on*. IEEE, 2012.

[3] Chakravarthy, V. Deeban, and V. Divya Renga. "A Neighbour coverage based probabilistic rebroadcast for reducing routing overhead in mobile ad hoc networks." *International Journal of Emerging Technology and Advanced Engineering Website: www. ijetae. com (ISSN 2250-2459 (Online), An ISO 9001: 2008 Certified Journal, Volume 3, Special Issue 1* (2013).

[4] Liu, Kejun, et al. "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs." *Mobile Computing, IEEE Transactions on* 6.5 (2007): 536-550.

[5] Kannhavong, Bounpadith, et al. "A survey of routing attacks in mobile ad hoc networks." *Wireless communications, IEEE* 14.5 (2007): 85-91.

[6] Malik, Devesh, Kalpesh Mahajan, and M. A. Rizvi. "Security for node isolation attack on olsr by modifying mpr selection process." *Networks & Soft Computing (ICNSC), 2014 First International Conference on*. IEEE, 2014.

[7] Schweitzer, N., Stulman, A., Shabtai, A., & Margalit, R. D. (2016). Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes. *Mobile Computing, IEEE Transactions on*, *15*(1), 163-172.

[8] Marimuthu, Mohanapriya, and Ilango Krishnamurthi. "Enhanced OLSR for defence against DOS attack in ad hoc networks." *Communications and Networks, Journal of* 15.1 (2013): 31-37.

[9] Dalal, Renu, Manju Khari, and Yudhvir Singh. "Different ways to achieve Trust in MANET." *International Journal on AdHoc Networking Systems (IJANS) Vol* 2 (2012

[10] Chakeres, Ian D., and Elizabeth M. Belding-Royer. "AODV routing protocol implementation design." *Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on*. IEEE, 2004.

[11] Al Ameen, Moshaddique, Jingwei Liu, and Kyungsup Kwak. "Security and privacy issues in wireless sensor networks for healthcare applications." *Journal of medical systems* 36.1 (2012): 93-101.

[12] Hoebeke, Jeroen, et al. "An overview of mobile ad hoc networks: applications and challenges." *Journal-Communications Network* 3.3 (2004): 60-66.

[13] Kannhavong, Bounpadith, et al. "A survey of routing attacks in mobile ad hoc networks." *Wireless communications, IEEE* 14.5 (2007): 85-91.

[14] Adnane, Asmaa, Christophe Bidan, and Rafael Timoteo De Sousa. "Trust-based countermeasures for securing OLSR protocol." *Computational Science and Engineering, 2009. CSE'09. International Conference on*. Vol. 2. IEEE, 2009.

[15] Jeon, Yuseok, et al. "LT-OLSR: Attack-tolerant OLSR against link spoofing." *Local Computer Networks (LCN), 2012 IEEE 37th Conference on*. IEEE, 2012.