IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115121

ML technique to improve the performance of Mobile Adhoc Network

Hamela K

Assistant Professor, Department of Computer Science, GFGC, Malur, Karnataka

Abstract: Mobile Adhoc Network (MANET) is one of the kinds of Wireless networks. The general nature of MANET comprises of non- fixed infrastructure, dynamic nodes, each node act as a router, it is an autonomous user which communicate through wireless links. Due to random movements, the network topology frequently changes, to find the route between source and destination nodes, we use a techniques namely Routing protocol. There are three types of routing protocols in MANET like proactive, reactive and hybrid. In this paper, we would like to improve the performance of one type of proactive routing protocol called Optimized Link State Protocol through Machine Learning (ML) techniques.

Keywords: MANET, OLSR, Machine Learning (ML)

1 INTRODUCTION

A network with self-governing, self-motivated in nature will be Mobile Ad-hoc Networks (MANET) which encompasses infrastructure-less feature connected wirelessly to mobile device. At any time, nodes can join in and leave out from the network and can move randomly and organize themselves arbitrarily [1]. The network topology becomes unforeseeable and may change quickly due to this element of oddness [1].

In MANET network, single hop and multi hop communication is possible that creates a direct and indirect type of communication. Multi-hop type of communication is the one in which nodes can indirectly communicate through intermediate nodes. The process of finding the nodes between the source S and destination D is known as routing. Routing is the basic functionality of any communication network. MANET does not require any fixed infrastructure and it is a decentralized network that requires a strong dynamic routing protocol. Based on routing update mechanism, there are 3 different types of protocols such as, proactive, reactive and hybrid are utilized to initiate a secure and efficient path from source to destination [2]. In MANETs, a standout amongst the most well-known routing protocols is Optimized Link State Routing (OLSR) in which nodes keep information about the routes in the network [3]. This is performed by control messages such as HELLO and Topology Control (TC) messages among nodes in the network [4,5]. Hello and TC messages are utilized to find and then spread link state information throughout the MANET.

OLSR encompasses few characteristics highly efficient, high Packet Delivery Ratio, minimal Energy Consumption per Packet, minimal Delay, increase in Network lifetime and less Packet loss rate, but security is challenge for OLSR routing protocol [6]. It is vulnerable to various attacks. To improve the security of OLSR and prevent the nodes from various attacks we have proposed a model in which trustworthiness of the nodes are maintained, due to that only the trustworthy node alone will be able to communication in routing path. To achieve trustworthiness among nodes, we have used Machine Learning approach to OLSR protocol.

This paper we have used one of the machine learning techniques to enhance the trust level of nodes in MANET taking in account of OLSR protocol. The paper is arranged as follows. Section 2 describe about the related work of previous existing work in the field of OLSR. In Section 3 we have focused on the concept of OLSR, and Section 4 will discuss about Machine Learning Techniques. Trust computation discussed in Section 5 and section 6 will deal with experimental results form the simulation. Finally, we have covered conclusion in Section 7.

2 RELATED WORK

A trust-based routing mechanism was introduced by Shuaishuai Tan et al. [7] to reduce numerous genuine security threats in both routing and data plane in OLSR-based MANET. In their examination to assess mobile nodes trust values, the trust reasoning model dependent on Fuzzy Petri Net was presented. Moreover, a trust-based routing algorithm was exhibited for path selection with the most extreme trust value of way among every single conceivable way, to dodge traded off/malicious nodes. At that point the exhibited OLSR was stretch out to FPNT-OLSR, trust-based routing algorithm. For FPNT-OLSR usage the creators plan an efficient trust data propagating technique and trust factor gathering strategy that don't produce additional messages for control. Test results demonstrate the FPNT-OLSR performs better as far as overhead, average latency and packet delivery proportion than existing trust based OLSR protocols.

DOI: 10.17148/IJARCCE.2022.115121

Robert. J.M et al.[8] introduced a new mechanism to extend the life of adhoc networks using the OLSR routing protocol by (1) partitioning the nodes in order to minimize and reduce the congestion of the multitude of selected relay (MPR) nodes due to their topological control (TC) messages and (2) to designate the relay nodes based on the cost of the Cost-to-Forwards relay.
K. S and J. R. Prathuri [9] proposes a concept comparing two machine learning techniques namely Support Vector Machine (SVM) and Back Propagation Neural Network (BPNN) and way to find the misbehaving nodes. This model was able to achieve parameters like packet Delivery Ratio (PDR), End-To-End delay, Average Throughput.

3 OPTIMIZED LINK STATE ROUTING (OLSR) PROTOCOL

In MANETs, a standout amongst the most well-known routing protocols is Optimized Link State Routing (OLSR) in which nodes keep up ways to all destinations in the network [10, 11]. This is finished by performing sporadic trade of control messages (HELLO and Topology Control (TC) messages) among nodes in the network [12]. Hello and TC messages are utilized to find and then spread link state information throughout the MANET. OLSR is identified by Internet Engineering Task Force's (IETF) MANET Working Group (WG) [13] as one of four base routing protocols for use in MANETs. OLSR is an IP routing protocol optimized for MANET.
OLSR is operates as a proactive, table-driven protocol that is, interchanges the information of topology with other nodes of the network continuously. Each node chooses a set of its neighbor nodes as multipoint relays (MPR) [14,15]. The OLSR protocol attains optimization by the help of MPRs which are selected and deputed by neighboring nodes. In OLSR, into the entire network, only nodes, selected as such MPRs are responsible for forwarding control traffic, deliberate for diffusion. By reducing the number of needed transmissions, MPRs yielded an efficient mechanism for flooding control traffic.

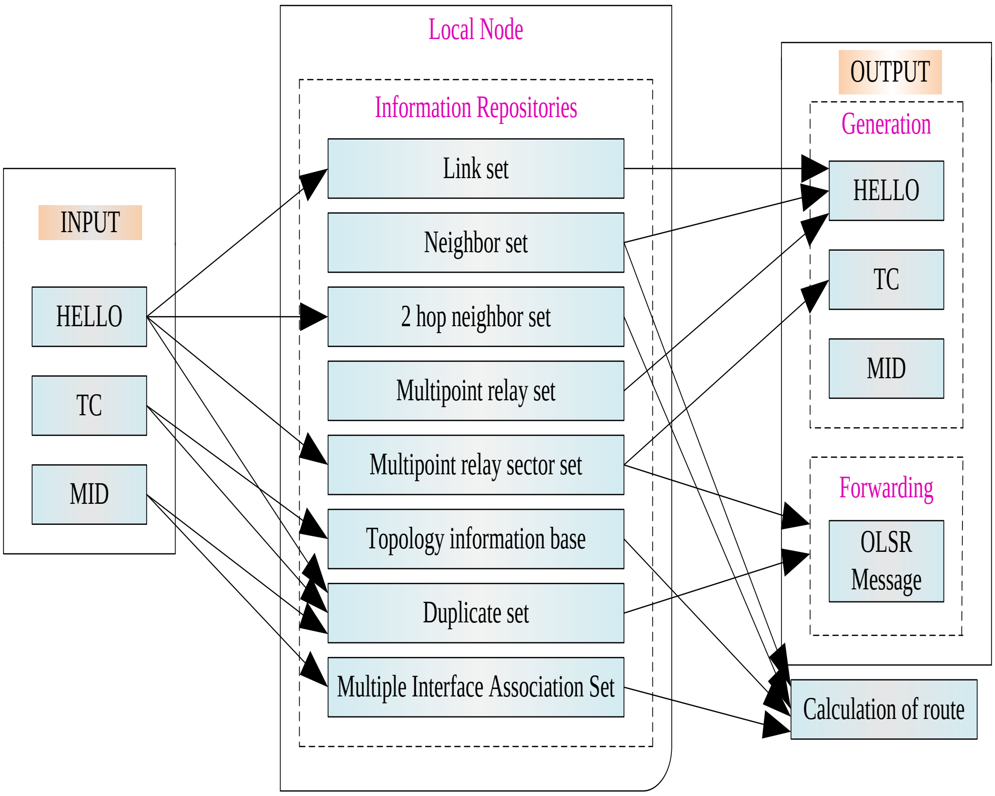

Figure 1: OLSR Data flow

The above Figure 1.4 shows the data flow diagram of OLSR. In OLSR, HELLO, TC and Multiple Interface Declaration (MID) messages are set as input. The input message functions as follows:

- HELLO-messages: Link sensing, MPR signalling and neighbour detection is executed.
- TC-messages: Topology declaration i.e., advertisement of link states is executed.
- MID-messages: Declaration of presence of multiple interfaces on node is executed.

Then the output message is produced and OLSR message is forwarded. In network, forwarding is related to retransmitting the same message for other nodes. The calculation of routing table is based on the information present in

DOI: 10.17148/IJARCCE.2022.115121

the topology information base and duplicate set. In the network, each node maintains a routing table that permits it to route data, destinated for other routes. Therefore, the routing table is recalculated to update the route information about each destination in the network when the sets are changed. When the OLSR control message is interchanged, each node gathers information about the network. This information is stored in the information repositories, and it contains eight sets [16].

4 MACHINE LEARNING

One area of research in artificial intelligence is machine learning (ML). Machine learning is a technique in which computer think and act smart. The computer will be able to learn from the data and make decision from the experiences. Using ML, we can also make our computer do analysis for our requirement. The various category of Machine learning are supervised learning, unsupervised learning, and reinforcement learning [17].

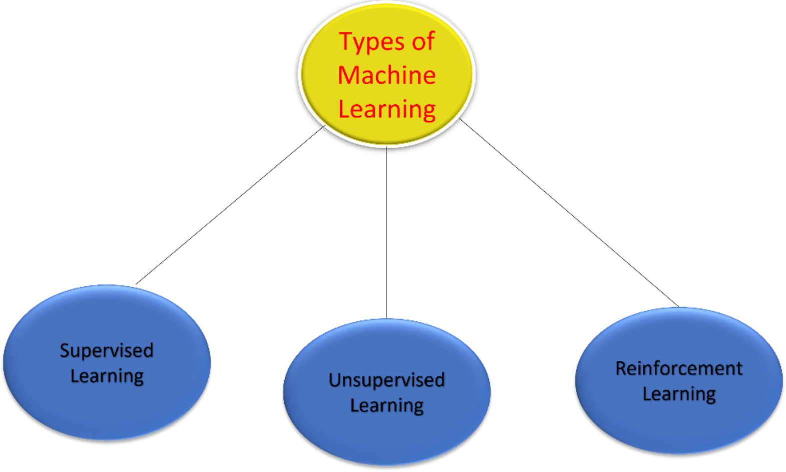

Fig 2: Types of Machine Learning

Types of Machine Learning:

Supervised learning:

The basic type of machine learning is supervised learning. In Supervised learning based on the labelled data, ML algorithm are trained. ML algorithm is provided with trail dataset based on the original dataset[24]. The characteristic and features of trail dataset will be like original data set. With the trail dataset, ML algorithm understand the problem, preform analysis, predict the relationship between parameters and try to identify the solution. The trail dataset will help the ML algorithm to understand the problem and find the necessary details about Input and Output. This Supervised learning method, will keep on improving its performance based on the new dataset[19].

Unsupervised machine

In case of handling unlabeled data set, then we can consider Unsupervised Machine learning algorithm as best choice. Without human interference, large dataset can be processed. Due to absence of labelling function in unsupervised learning, the datapoints are recognize by algorithm based on hidden structure[20]. The performance of algorithm in a abstract way, make this method more efficient.

Reinforcement learning

Like human beings' nature is to learn through experience, reinforcement learning also will from situation using trial and error method. In outcome result is favourable then it will be encouraged and similarly, if outcome result is bad, then it will be discouraged. If the programme finds the proper solution, the interpreter reinforces it by rewarding the algorithm[21]. If the result is unfavourable, the algorithm is obliged to repeat the process until a better result is found. In most circumstances, the reward system is directly proportional to the effectiveness of the outcome. This algorithm takes on a rating of effectiveness, expressed in a percent rate[23]. The better this percent rate is, the greater credential is given to the algorithm. Thus, the program is trained to give the best possible solution for the best possible reward[21].

In our work, we have used one of the reinforcement learning technique namely Q-learning to identify the trustworthiness of the node in MANET. Since Q-learning has got a nature to learn through experience, this algorithm can be very well used to identify the fake node and trustworthy node.

DOI: 10.17148/IJARCCE.2022.115121

5 TRUST COMPUTATION OF NODE

Towards use of Q-Learning strategies to solve our problem, we must first comprehend how to apply these concepts so that they are more suitable for our situation. In MANET, each node participating the structure is taken as agent. Every node participating in the MANET is considered as an agent. Each node is responsible for finding the safest and best next hop during routing. The Q-Learning agent in the node is accountable for establishing the trust of neighbour nodes so that trustworthy nodes are selected as MPR and Next hop nodes [23].
A methodology will be used in MPR computation to improve the trust. When computing the MPR set for a given node, the set of possible nodes that result in the highest trust will be selected. The MPR Computation method will be modified as stated below.
1. Start with an MPR set containing all neighbors of N with willingness greater than WILL_NEVER and having the highest q-value from the available nodes.
2. Calculate the degree of neighbors for all nodes in set N
3. Add to MPR set, nodes in N, which provide the only reachability to N2 nodes. Remove N2 neighbors that have access. Even if this type of MPR node has very low trust it has to be selected due to its unique reachability.
4. Continue this until all nodes in N2 are covered by MPR.
To enhance agree with, a technique might be hired in MPR calculations[23]. The set of possible nodes that bring about the best agree with might be selected while computing the MPR set for a given node. The MPR Computation approach might be modified withinside the following way.
1. Create an MPR set with all of N's neighbours who've a willingness large than WILL NEVER and the best q-values many of the to be had nodes.
2. For every node in set N, compute the scope of neighbours.
3. Add to MPR set, nodes in N, which provide the only reachability to N2 nodes. Remove N2 neighbors that have access. Even if this type of MPR node has very low trust it has to be selected due to its unique reachability.
4. Continue this until all nodes in network are covered by MPR
As discussed above, it will give priority to the most trusted node when selecting the MPR set. This will result in formation of trusted routing paths because MPRs are used in Routing Computation. In topology control (TC) messages, the neighbour node address is broadcasted by MPR. By advertising this information in TC messages, it is basically saying that it has access to these nodes. Our method will yield untrustworthy nodes and broadcast only the trustworthy nodes when computing the routing path.

6 SIMULATION MODEL AND PARAMETERS

The performance evaluation on the technique using extensive simulation is conducted and presented with the network simulator NS2 [10]. Simulation settings and parameters are summarized in table 1.

Parameters	Values
No. of Nodes	100
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	500 sec
Routing Protocol	MOLSR
Traffic Source	CBR
Packet Size	512
Speed	0 to 20m/s

Table 1 NS2 Simulation Parameter

6.1 Performance Evaluation

For performance evaluation of our proposed solution against existing model [22] and proposed model[24] under attack, we consider the following metrics and the comparison results are shown in Figs. 3–4.

DOI: 10.17148/IJARCCE.2022.115121

a) Packet Delivery Ratio

No of Attackers	Existing Trust based Model	Proposed Trust based model based on Reinforcement Learning
1	85	90
2	77	86
3	77	82
4	76	79
5	71	76

Table 2 Proposed method is contrasted with existing methods for packet delivery ratio.

The transmission of number of packets from source to destination node is known as Packet Delivery Ratio.

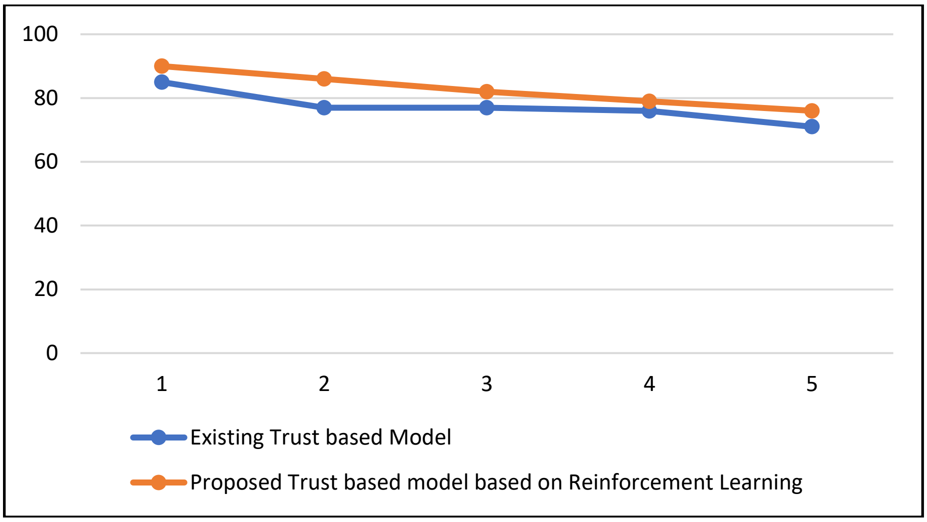

Fig 3 No. of attackers against Packet delivery ratio

The packet delivery ratio, when compared with existing model, the packet delivery ration seems to be high in this approach. When compared to existing methods, our proposed perform 5.4% increase in Packet Delivery Ratio.

b) Packet Loss Ratio

NO OF ATTACKERS	PACKET LOSS RATIO (%)	
	Existing Trust based Model	Proposed Trust based model based on Reinforcement Learning
1	17	12
2	18	15
3	22	19
4	27	23
5	30	25

Table 3 Proposed method is contrasted with existing methods for packet loss ratio.

The lose of packet during the transmission of packets is known as Packet Loss Ratio. The packet loss increases in comparison to the number of attacker nodes increase.

DOI: 10.17148/IJARCCE.2022.115121

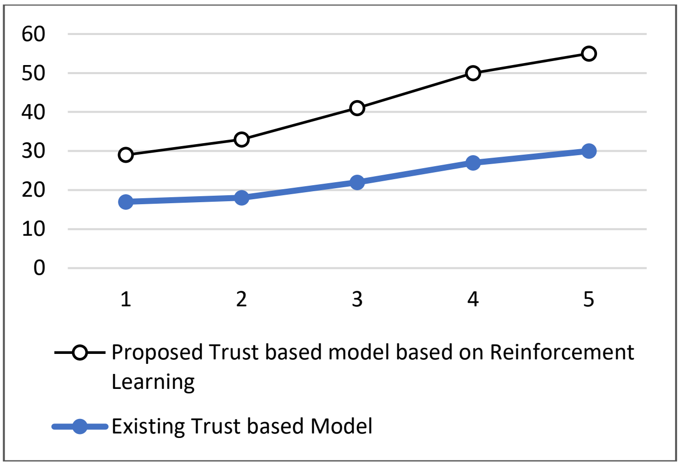

Fig 4 No. of attackers Vs Packet loss ratio

Figure 4 shows the packet loss percentages of existing and Proposed model. Contrasting with other techniques, 4% less than existing model.

7 CONCLUSION

This paper explains the trust based OLSR model for enhancing the performance against nodes in MANET using Machine Learning Technique. The proposed approach is simulated in NS2.35 along with existing OLSR mode. In terms of the packet delivery ratio and packet loss rate, performance of the method has been evaluated. In the end, we conclude that the proposed method has achieved enhance performance when compared with existing OLSR methods in Mobile Adhoc Network.

REFERENCES

1. Miriam Carlos-Mancilla, Ernesto López-Mellado, and Mario Siller, Wireless Sensor Networks Formation: Approaches and Techniques, Hindawi Publishing Corporation Journal of Sensors Volume 2016, Article ID 2081902, 18 pages http://dx.doi.org/10.1155/2016/2081902.
2. P. Meshram and N. Sambhe, "Routing protocols in mobile ad hoc network", Proceedings of the International Conference and Workshop on Emerging Trends in Technology - ICWET '10, 2010.
3. S. Lalar and A. Yadav, "Comparative Study of Routing Protocols in MANET", 2018.
4. Chaurasia, M. and Singh, B.P. "Prevention of DOS and Routing Attack in OLSR Under MANET", In Proceedings of International Conference on Recent Advancement on Computer and Communication, Springer, Singapore, April 2018, pp. 287-295.
5. S. A. Ade and P. A. Tijare, "Performance Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad Hoc Networks," Int. J. Inf. Technol. Knowl. Manag., vol. 2, no. 2, pp. 545–548, 2010.
6. Hamela Kanagasundaram, A. Kathirvel, "EIMO-ESOLSR: energy efficient and security based model for OLSR routing protocol in mobile ad-hoc network", IET Commun., 2019, Vol. 13 Iss. 5, pp. 553-559.
7. S. Tan, X. Li and Q. Dong, "Trust based routing mechanism for securing OSLR-based MANET", Ad Hoc Networks, vol. 30, pp. 84-98, 2015.
8. Robert. J.M, Otrok. H and Chriqi. A, "RBC-OLSR: Reputation-based clustering OLSR protocol for wireless ad hoc networks", Computer Communications, vol. 35, no. 4, pp. 487–499, 2012.
9. K. S and J. R. Prathuri, "Classification of Misbehaving nodes in MANETS using Machine Learning Techniques," 2020 2nd PhD Colloquium on Ethically Driven Innovation and Technology for Society (PhD EDITS), 2020, pp. 1-2, doi: 10.1109/PhDEDITS51180.2020.9315311.
10. Chaurasia, M. and Singh, B.P. "Prevention of DOS and Routing Attack in OLSR Under MANET", In Proceedings of International Conference on Recent Advancement on Computer and Communication, Springer, Singapore, April 2018, pp. 287-295.
11. S. A. Ade and P. A. Tijare, "Performance Comparison of AODV ,DSDV , OLSR and DSR Routing Protocols in Mobile Ad Hoc Networks," Int. J. Inf. Technol. Knowl. Manag., vol. 2, no. 2, pp. 545–548, 2010.
12. Ahmad, M., Chen, Q., Najam-Ul-Islam, M., Iqbal, M.A. and Hussain, S. "On the secure optimized link state routing (SOLSR) protocol for MANETs", In Intelligent Systems and Knowledge Engineering (ISKE), 2017 12th International Conference, Nov 2017, Nanjing, China, pp. 1-8.

DOI: 10.17148/IJARCCE.2022.115121

13. Thomas Clausen et.al, "Optimized Link State Routing Protocol", http://www.ietf.org/internet-drafts/draftietf-manet-olsr-11.txt , July 2003.
14. M. I. A. Fouzan Zulfiqar Mughal, “Comparative Analysis of Proactive, Reactive and Hybrid Ad Hoc Routing Protocols in Client Based Wireless Mesh Network,” Int. Conf. Inf. Emerg. Technol., 2010.
15. A Qayyum, L. Viennot and A. Laouiti, "Multipoint relaying for flooding broadcast messages in mobile wireless networks", Proceedings of the 35th Annual Hawaii International Conference on System Sciences.
16. P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum and L. Viennot, "Optimized link state routing protocol for ad hoc networks", Proceedings. IEEE International Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century.
17. P. Louridas and C. Ebert, "Machine Learning" in IEEE Software, vol. 33, no. 05, pp. 110-115, 2016. doi: 10.1109/MS.2016.114
18. B. Thuraisingham, "Trustworthy Machine Learning" in IEEE Intelligent Systems, vol. 37, no. 01, pp. 21-24, 2022. doi: 10.1109/MIS.2022.3152946
19. Richard S. Sutton and Andrew G. Barto, “Reinforcement Learning: An Introduction”, A Bradford Book The MIT Press Cambridge, Massachusetts London, England ©2014
20. Alloghani, Mohamed & Al-Jumeily Obe, Dhiya & Mustafina, Jamila & Hussain, Abir & Aljaaf, Ahmed. (2020). A Systematic Review on Supervised and Unsupervised Machine Learning Algorithms for Data Science. 10.1007/978-3-030-22475-2_1.
21. R. S. Sutton and A. G. Barto, "Reinforcement Learning: An Introduction," in IEEE Transactions on Neural Networks, vol. 9, no. 5, pp. 1054-1054, Sept. 1998, doi: 10.1109/TNN.1998.712192.
22. Hamela Kanagasundaram, A. Kathirvel,“Trust-Based Multipoint Relay Selection Algorithm for Enhancing Security in Mobile Adhoc Networks”, Global Journal of Engineering Science and Researches. [INIT: January 2017], ISSN 2348 – 8034,pg 142-150
23. K. S and J. R. Prathuri, "Classification of Misbehaving nodes in MANETS using Machine Learning Techniques," 2020 2nd PhD Colloquium on Ethically Driven Innovation and Technology for Society (PhD EDITS), 2020, pp. 1-2, doi: 10.1109/PhDEDITS51180.2020.9315311.
24. Rupasinghe P.L, Chamira Nawarathna, Kalpa Kalhara Sampath , Enhancing the Security of OLSR Protocol Using Reinforcement Learning, , conference on National Information Technology Conference, 2017, Sri Lanka
25. Network simulator: http:///www.isi.edu/nsnam/ns.