History-Aware Selfish Node Detection on Mobile Ad-Hoc Network

Abraham Teklu (ab01te@yahoo.com)
Asossa University

Getachew Biratu
Asossa University

Research Article

Keywords: History Aware, OLSR, Proactive Approach

Posted Date: January 31st, 2023

DOI: https://doi.org/10.21203/rs.3.rs-2528219/v1

Abstract

MANET are a kind of flexible, infrastructure less, decentralized wireless network, and there is no any boundary that the nodes to manage during joining and leaving from and to the network. Due to their nature MANET is vulnerable to various kinds of attacks, and this paper discus on attacker node by awarding the previous history of each node on proactive protocol. Since there are a number of attackers in MANET, the proposed algorithm covers on packet drop attack. Attackers can be broadly classified in two categories: routing attacks and data forwarding attacks. We address the “Packet Drop Attack”, is a serious threat to operational mobile ad hoc networks. To handle the addressed attacker, we develop and adapt Algorithm for tracking the attacker .By using the proposed algorithm, it minimizes 3 % on end to end delay, increases throughput 2.005% and PDR increases 2.11%, by using Network Simulator 2 (ns-2).

1. Introduction

Mobile ad hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Ad Hoc networks do not have a certain topology or a central coordination point. Therefore, sending and receiving packets are more complicated than infrastructure networks. MANETs are infrastructure less and self-organized; all nodes have to cooperate between themselves in order to provide the best performances and offer necessary network functionalities. Nowadays, with the immense growth in wireless network applications like handheld computers, PDAs and cell phones, researchers are encouraged to improve the network services and performance. One of the challenging design issues in wireless Ad Hoc networks.

The MANET is attractive for applications such as disaster relief, military service, robot networks, emergency operations, maritime communications, casual meetings, campus networks, vehicle networks, and so on. Unlike conventional network, a MANET is characterized by having a high dynamic nature, continuously changing network topology due to mobility of nodes. Several efficient routing protocols have been proposed. These protocols can be classified into three categories: [1,2,3].

- Reactive routing protocols such as, AODV, DSR
- Proactive routing protocols such as, OLSR, DSDV
- Hybrid routing protocols such as ZRP

There are different studies for misbehavior node which traps by developing of algorithm, model on different layers the work on [4] they use Detection of Selfish node using Game Theory, by using Least Total Cost Factor (LTCF), data packets will be transmitted from source to destination node through least cost path only. Due to the presence of selfish nodes in the network, if a path has been broken, then the next best path will be automatically selected for data transmission.

The study on [5] Security services are needed to make sure that the data is transferred over the network with reliability and also the keeping the resources of the system protected. To attain the objectives, the categorizations of security services are: availability, confidentiality, authentication, integrity and non-repudiation. To reach the objective the researchers focuses on reactive routing protocols and in order to transmit the packets safely a secured approach using triple factor has been proposed for collecting information of neighbor node and after deciding they use uses cryptographic algorithm to ensure security. The intention of this paper is increasing the performance of Network in proactive routing protocol for ad hoc network by misbehavior node. Selfish nodes are unwilling to forward a packet via it's, that is packet drop node, to overcome the misbehavior node we develop an algorithm which captures and understands the historical background of every participant nodes and Integrate in OLSR to improve security by imbedding the proposed algorithms, which is one of proactive routing protocol. To maximize their life (utility) and due to their behavior selfish nodes may not forward the message to their neighbor node. This motivated as to propose a new technique of performance improvement mechanism using multipath routing protocol. Link failure prediction is a useful technique in ad hoc network for minimizing the repetition of route discovery process [5].

2. Related Works

MANET are self-organized nodes without using infrastructure and these nodes form a cluster on the fly [1,2]. Sivavakeesar and Pavlou [3] describe about how to improve quality of service in multimedia traffics by supporting in multi-hop MANET, by creating virtual cluster model of those mobile nodes which are wirelessly communicated to each other. On [7] In OLSR routing protocol, one of the most essential key concepts used is the use of multipoint relays (MPRs). The main purpose of the MPRs is to forward the broadcast messages in the network. OLSR mainly uses two kinds of control messages. The first one is the periodic HELLO messages while the second type is the Topology Control (TC) messages. The HELLO messages are used for discovering the information about the link status or in other words it carries out the task of neighbour detecting. The second type, which is the Topology Control (TC) messages are used for the purpose of information declaration about the multipoint relay. The work of Korsnes et al. [5] predicts the life time of the network and they compare the performance of Ad hoc On-Demand Distance Vector (AODV), Optimized Link State Routing (OLSR), DSR (Dynamic Source Routing), and TBRPF (Topology Broadcast Based on Reverse Path Forwarding) routing protocols. Based on the generated result the recommend to use AODV routing protocol.

In [4] The scope of the intrusions in mobile ad hoc networks is considerably proportionate to the growth of the mobile ad hoc network scope in the use of technology in general strategic facilities of the human life. The intruders intended to downgrade the performance scope of the target network often performs black hole attacks. The other frequent method of intrusion in ad hoc networks is denial of service, which is often evincing through the gray hole and warm hole attacks. The nodes compromised to perform these attacks are insensitive to identify. This manuscript contributed a novel evolutionary approach to establish an optimal route between source and target nodes that eliminates the scope of the nodes compromised to denial of service attacks through performing black hole, gray-hole and warm-hole activities. The performance of the contribution is scaled by comparing the experimental results of the proposal with other contemporary models.

Minimizing and removing of selfish node is an important step for packet accessibility and stability of a link for end-to-end communication. The work of Kumar and Bahadhur [6] minimize selfish node in MANET, by using Reputation-Based Technique. This technique is used to control node to node communication by knowing and observing its neighbours node such that all the nodes collect and have a full information about their neighbour and each node has the responsibility to discover the path before sending a packet. The proposed scheme of Nair and Muniraj [7] calculate link stability before link failure happens, called Prediction based Link Stability Scheme (PLSS), since MANET have dynamic topology. They use this scheme for making a correct balance of stability of path, neighbours node and total mobile nodes to the extent of the network lifetime.

The study [8] studies the effect of Packet drop or Black hole attack are evaluated in MANET routing protocols namely AODV as reactive and OLSR as a proactive routing protocols by using performance metrics delay, network load, throughput and data dropped using OPNET Modeller 17.5 network simulator tool. By keeping network area 1000m x 1000m, simulation time 1800 second, IEEE 802.11g using data rate 24 mbps and mobility model Random way point are constant. In this study black hole node is a malicious node with less buffer size of 64Kb. In OPNET, simulation result show that comparatively reactive routing protocol like AODV is more vulnerable than proactive routing protocol OLSR under varying number of black hole node attack. Having related problem is solved on [9], Ad hoc routing technology has been developed primarily for networks of mobile nodes. In many cases the operational life of a node will be limited by its power source, so power consumption can be a critical issue. All the layers of communication are coupled in power consumption. Ad hoc routing protocols may consume different amounts of power and their routing decisions may be conditioned. Power consumption must be distributed on the nodes of the network and the overall transmission power for each connection must be minimized. MANET Attackers and Their Issues Attacker is one big issue in ad-hoc network (MANET) research area [10, 11, 12], and it is one of important task for personal computer user both in infrastructure and in infrastructure-less network. Since studding attacker is a vast task because they upgraded their behavior from time to time, so this study covers on MANET specified with link discovering from source to destination including the intermediate node.

The features of the selfish nodes are as follows

- Non-participation in routing
- No transmission or reply to HELLO messages
- Data packet dropping

There are a number of attackers in ad-hoc network, because of the different weak points observed in MANET. Due to its decentralization it is vulnerable for attack, especially the routing procedure, on upper and lower layers for disturbing a whole network (End-to-End communication).Since the packet is dropped they cause for link failure this leads for low packet delivery ratio, throughput, and delay. Based on their behavior, MANET attackers join to the network [12];

- To consume resources uselessly
- To interfere with any system resource's intended function like attack in the middle
- To save their resources and stabling their life for long time.

So based on this concept the detail description of attackers in MANET are:

1. **Dropping Attacker**: The malicious node drops the packet which is not intended for the attacker/for themselves. From their behaviour during end-to-end communication they act as a normal node, but they drop packets, then they cause a reduction in network performance [10] for the purpose of saving its own resource like power.
2. **Ad-hoc Flooding Attack** (AHFA): AHFA is a type of DoS (Denial of Service) attacker to denial End-to-End communication when the network uses On-demand type of routing protocol like DSR and AODV. These attackers sends a lot of broadcast route request packet message to slow down the communication with none existed node ID, so the valid communication minimize the throughput, increase delay with high packet dropping ratio.
3. **Gray Hole Attack**: The aim of Gray Hole attacker is to drop a packet/message sent by a source to target node. To this end, the attacker node acts as a legitimate node to forward a packet, but it drops a packet intentionally because of its maliciousness. Source node wants to communicate with the target node, if control message are passed through the attacker, then the connection is lost to reach to the destination because the attacker drops the message, and the process repeat again and again by sending RREP messages[12].
4. **Black Hole Attack**: Another type of attacker is Black Hole attacker, which causes to absorb all packets to itself [10, 12].
5. **Worm Hole Attacker**: An attacker type which spy and disturb the whole network intentionally is worm hole attacker. This attacker tries to combine itself with selective forwarding and eavesdropping. Due to the presence of worm hole attack in MANET; it is difficult to analyze, authenticate and non-repudiation the traffic that is going on [13].

3. Material And Method

Mobility models are key factors that are used to control the mobility and activity of hosts in ad-hoc networking studies with the integration of routing protocol. In MANET, mobility models are used to define and manage the movement of nodes like location, speed of each node related to the period time that is specified in simulation model by the developer. In this study we use the most known model for ad hoc network which is RWP (Random Waypoint Model) model. In this mobility model, the entities are selected a random destination in specified coordinate and at a random speed. This model is widely used in

MANET research studies [6]. In RWP model, when the node reaches to destination area, it alerts a pause time randomly pause time between two movements of interval. Since the work is empirical study it simulates the proposed new technique on Network Simulator version 2. Selecting and using of routing algorithm is a big task, because it depends on the type of network, number of nodes, type of application and where the network is deployed.

3.1 Proactive Approach

The approaches which is used to describe the post condition methods of the nodes, the nodes in the network have same behavior and learns activities. Each node in the network follow the proactive methods for transmitting a packets with understanding the regular time interval and a given rule, and the control messages that are used in MANET with having knowledge of a routing protocol. The capability or activities to covered and discussed are monitoring the network health by configuring model and algorithms, fault management strategy by using the specified rule like configuring power aware routing algorithm, pro-actively triggered network configuration

3.2 Simulation Techniques and Tools

Different researchers are conducted their research work on OLSR for different related problems on MANET, these related work are reviewed. Review and analyzing of previous related works, specifically on MANET on types of selfish nodes by using different metrics. For implementation different tools are used such as: NS-2(Network simulator version 2), object oriented programing language; C++ is used. According to the research problem for generating the result, analyzing and deciding the node behavior is by using different data sources such as; assigning limited constant bit rate, and specified number of the nodes.

3.3 Working with RSSI Value

For this paper we use RSSI type to adapt Two Ray Ground model for calculating the signal strength of the given network;

The formula is given below based on Two Ray Ground model [21]:

$$P_r(d) = \frac{P_t * G_t * G_r * h_t^2 * hr^2}{d^4 L}$$

Pr: Power received at distance d

Pt: Transmitted signal power

Gt: Transmitter gain

d: Distance from the transmitter

ht: Transmitter antenna height

hr: Receiver antenna height

Gr: Receiver gain

Received signal strength can vary due to multi-path, interference or other environmental effects, it may not give a true indication of communication performance, because these factors tend to fluctuate the RSSI values [21].

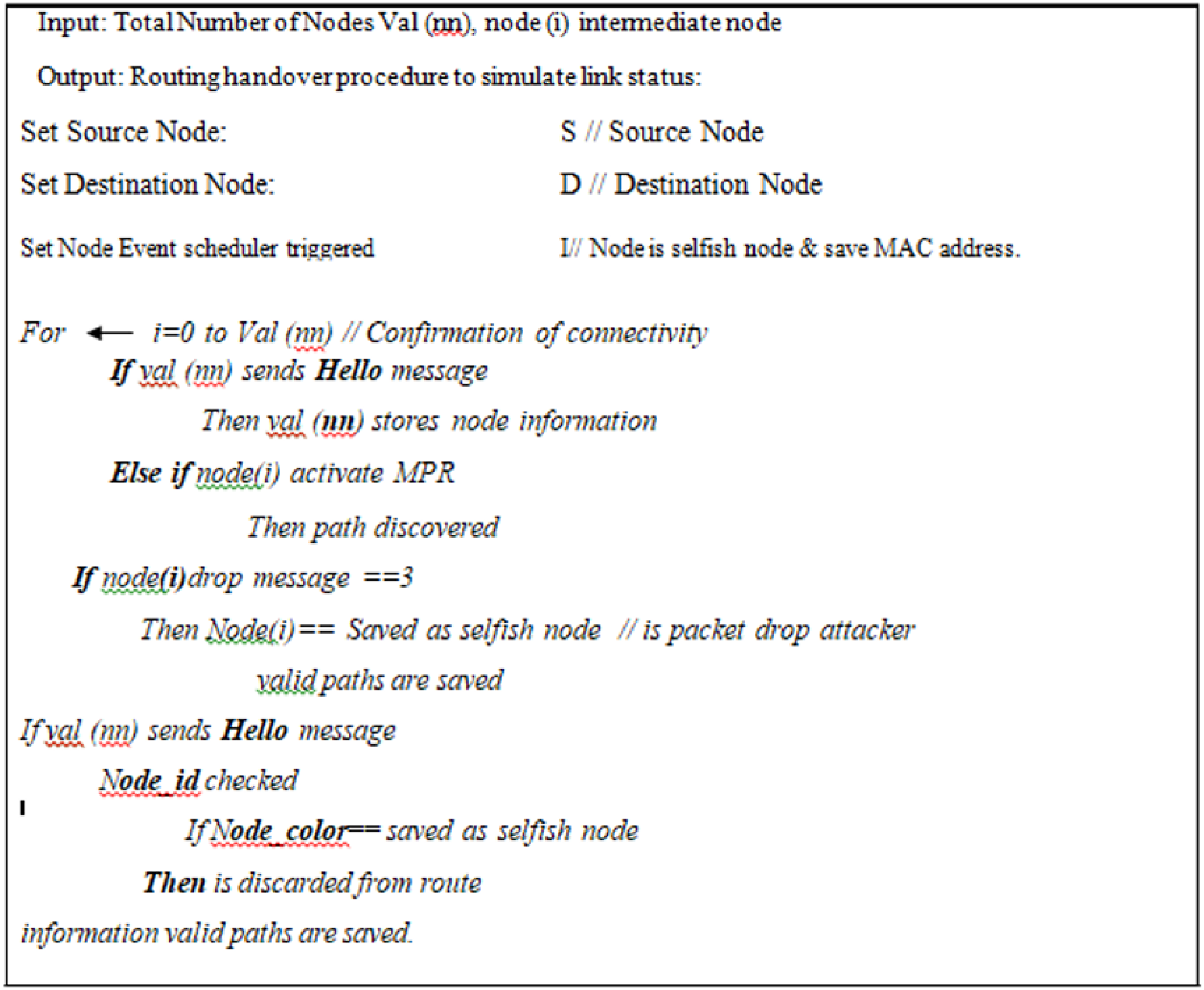
3.4 Proposed Algorithm

This section discuses on the new algorithm that we proposed based on the gap identified in the declaration the problem that manages the participants of misbehavior node by designing an algorithm that enables the algorithm for capturing and eradicating the selfish node from the network, and every participant node store the characteristics of each node, such misbehaving nodes cause high amount of packet drop rate, useless bandwidth consumption, disturbance of the whole network. The proposed algorithm manages the participants of misbehavior node in undeserved area that cannot exchange information based on the specified routing caches information.

Table 1 MANET Control Messages on OLSR protocol

No	Control Message Type	Function
1	**Hello**	Confirmation of connectivity, also used for route update
2	**Topology Control**	For information declaration about the multipoint relay
3	**Multiple interface declaration (MID)**	MID messages include the list of all IP addresses used by any node in the network.

Algorithm 1: Proposed Algorithm



```
  Input: Total Number of Nodes Val (nn), node (i) intermediate node
  Output: Routing handover procedure to simulate link status:
Set Source Node:                          S // Source Node
Set Destination Node:                     D // Destination Node
Set Node Event scheduler triggered        I// Node is selfish node & save MAC address.

For ← i=0 to Val (nn) // Confirmation of connectivity
        If val (nn) sends Hello message
                Then val (nn) stores node information
        Else if node(i) activate MPR
                    Then path discovered
     If node(i)drop message ==3
            Then Node(i)== Saved as selfish node // is packet drop attacker
                    valid paths are saved
If val (nn) sends Hello message
       Node_id checked
ı
              If Node_color== saved as selfish node
           Then is discarded from route
information valid paths are saved.
```

In MANET, source node sends Hello message to all of the neighbors' node, then each node that receives the message stores node information in their routing table. Good characteristics of OLSR protocol is a modular proactive hop by hop routing protocol. Then the source node cheeks its routing table to send or to rebroadcast Hello message. If the node drops the message for 3 consecutive time it marks as packet drop attacker and assigning of red color for identification to be understand for human being, but in the source code red mean that the node is selfish node, then the source node saves MAC address of the selfish node and sends broadcast message to save each participant node in the network, for eradicating the route which is discovered before and refresh their route and develop another modified path on the trusted node.

4 Simulation Environment

In this paper the effect of Packet drop attack is evaluated in MANET routing protocols namely OLSR as a proactive routing protocols by using performance metrics delay, packet delivery ratio, throughput and data dropped using and the proposed algorithm was adapted and implemented, tested on NS-2simulator tool and Ubuntu (14.04 version) operating system, for discussing result we evaluate the generated data set on running the node participants.

4.1 Simulation Evaluation and Parameters

For deciding the behavior of nodes in this study, the nodes in the network was pre-set to read their Maliciousness value for identifying its amount of dropped packets (see figure 2), based on which maliciousness of the node was evaluated.

The proposed algorithm also have also a tacking mechanism which node is nearest to another node by visualizing to user/researchers.

For evaluating the proposed algorithm and design, in is conducted and the result is analyzed and evaluated by the given below parameters metrics.

All the mobile nodes moving at a constant speed of 10 meter per second, in this research work each node in the network reads a non-real data type/text value for comparing the result after running using NS-2.35 simulator. Number of nodes were varied and simulation time was taken 1800 seconds. Simulation area taken is 1000 x 1000 sq. meters.

The data rates of mobile nodes are 24 Mbps with the default transmitting power of 0.005 watts. Random way point mobility is selected with constant speed of 10 meter/seconds.

Accordingly each node generates their value and each node knows the neighbors node result, based on the result the normal node select another route.

Table 2 Measurement metrics

Parameters	Values
Simulator Tool	Network Simulator Version 2(NS-2)
Simulation Area	1200*1200
Number of Nodes	16, 25, 50 Nodes
Routing Protocol	OLSR
Packet Size	512 bytes
Traffic Type	CBR
Mobility Model	RWM
Simulation Time	1800 Sec

Packet Delivery Ratio (PDR): PDR is determined based on the received and generated packets as recorded in the trace file. It is the ratio of packet that are delivered to the destination and generated packets by the source node. Mathematically packet delivery ration (PDR) is computed as follows.

Average End-to-End Delay: is defined as the average time taken for the generated packet to reach to the destination. It includes all possible delay causes such as route discovery, queuing and retransmission delay. Packet drop is discussed in detail on [2,8].

Throughput: in Ad-hoc networks there is a node to maximize total network throughput by using all available nodes for routing and forwarding. However a node may misbehave to forward packets. Misbehaving nodes can be a significant problem that affect throughput.

Discussion Result

In this section we discuss the simulation result of the proposed algorithm for improving the amount of three performance measurement metrics on OLSR protocol. For generalizing the result based on the proposed algorithm and procedures for three scenarios with number of nodes are 16, 25 and 50 nodes are randomly distributed. To measure and compare the efficiency of the OLSR protocol and the proposed algorithm is integrated/adapted using different tools and scripts, such as trace graph generator tool and Perl script. Table 2 below shows the result of End-to-End delay, dropped packet, and Packet delivery ratio of the old and the proposed algorithm with having of running time period for each scenario.

The proposed algorithm also identifies a malicious node by knowing their neighbor node to discover the path by knowing direct link between nodes, here node 2 acts a malicious behavior because this node is found in same transmission range and and its Next hope to visualize the neighbor of each nodes in the network.

Result for node #1

Node #0: Packets sent = 164 - Packets confirmed = 153

Node #5: Packets sent = 132 - Packets confirmed = 148

Result for node #2

Node #1: Packets sent = 342 - Packets confirmed = 290

Node #5: Packets sent = 73 - Packets confirmed = 69

Result for node #6

Node #0: Packets sent = 104 - Packets confirmed = 53

Node #4: Packets sent = 100 - Packets confirmed = 98

Node #7: Packets sent = 149 - Packets confirmed = 99

Result for node #4

Node #0: Packets sent = 62 - Packets confirmed = 62

Node #5: Packets sent = 94 - Packets confirmed = 93

Node #6: Packets sent = 503 - Packets confirmed = 311

Node #12: Packets sent = 11 - Packets confirmed = 11

Based on the above traced file, hence node 2 is as acting as malicious node then the other participant node cannot sent and receive any packet by node 2, Because a during route discovery node drops topology control packet.

Table 3 Average result for each scenario on the old and modified protocol

Simulation	Average	Average	Average	Average	Average
Result	Packet	Packet	Dropped	Packet	End-to-End
	sent	Received	Packet	Delivery ratio	Delay
Old OLSR Protocol	5967	2071	2276	0.6186	1.9235
Modified OLSR Protocol	5954	3926	2008	0.9616	0.9208

The generate result which is found compares table 2 the result between the proposed algorithm which is the modified protocol and existed protocol, not only these figures but also as we view in.

Conclusion

OLSR is a table driven (proactive) routing protocol is based on the link state algorithm. Link state messages are flooded or broadcasted periodically to maintain the consistency in the routing information throughout the network. For our work, considering its futures of maintaining routing information, we have chosen Optimized Link State Routing (OLSR) which is a type of proactive link state protocol and uses Hello and Topology Control (TC) messages. The determination of this study is designing a algorithm for detecting misbehavior node. This is critical for forming stable communication/routing table modification for OLSR and for having of long life during data dissemination. To detect the misbehavior node by counting amount of confirmed dropped packets in one scenario in the given amount of time.

The proposed algorithm is implemented by modifying the C++ files of OLSR on NS-2 simulator tools, on different amount of node with having of similar running time and each node which are distributed randomly for tracing their behavior from the trace file (.tr) and integrating the TCL file with other external file.

Declarations

Acknowledgment

I would like to express my deep, sincere and grateful thanks to my Advisor Dr. Million his constant encouragement, honest support, and dedicating their time from starting time till finalizing the work.

We declare that this article is our original work and it is submitted for first publication to Journal of Network and Systems Management. The article has not been published and is not being submitted or considered for publication elsewhere. The text, illustrations, or any other materials included in the article contains no violation of any existing copyright and does not infringe any rights of third parties. All authors participated in the work in a substantive way are prepared to take public responsibility for the work, in addition to that the paper is determined and evaluated by evaluator committee of Assosa University and the Acknowledged scholar by Dr. Million Meshesha.

Author contributions

Mr. Abraham Teklu MSc in Computer Networking, develops the algorithm for the proposed research problem and developed the initial idea. Mr. Getachew Biratu MSc in Information Technology, contributed to analyses and interpretations of the results. All authors wrote the manuscript together.

Additional information

Competing interests: The authors declare no competing interests

Funding

Since we academic Lecturer’s and Researchers we develop the research paper and all documents for our future education status and value, and for promotion without any fund of our employer institution .

References

1. Grover, D., Saini, S.: A Survey on Unicast Routing Protocols in Mobile Ad-Hoc Networks. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **5**(5), 697–702 (2015)
2. Bakht, H.: “Survey of Routing Protocols for Mobile Ad-hoc Network,”International Journal of Information and Communication Technology Research, vol. 1, no. 6, (2011)
3. Sivavakeesar, S., Pavlou, G.: “A_Prediction-Based Clustering Algorithm to Achieve Quality of Service in Multihop Ad-hoc Networks,”Ad-hoc networks, vol. 0

4. Debjit Dasa, K., Majumdera, Dasgupta, A.: Selfish Node Detection and Low-Cost Data Transmission in MANET using Game Theory", Elsivier. Procedia Comput. Sci. **54**, 92–101 (2015)
5. Zahedi, K., Ismail, A.S.: Route Maintenance Approach for Link Breakage Predicttion in Mobile Ad-hoc Networks. Int. J. Adv. Comput. Sci. Appl. **2**(10), 23–30 (2011)
6. Kumar, A.K., Bahadhur, S.: Selfish Node Detection in Replica Allocation over MANETs. IOSR J. Comput. Eng. (IOSR-JCE). **13**(5), 7–13 (2013)
7. Mohamad, T., Sultan, Zaki, S.M.: "evaluation of energy consumption of reactive and proactive routing protocols in MANET,"International Journal of Computer Networks & Communications (IJCNC)Vol.9, No.2, (2017)
8. Xia, H., Xia, S., Yu, J., Jia, Z., Sha, E.H.: Applying link stability estimation mechanism to multicast routing in MANETs. J. Syst. Archit. **60**(5), 467–480 (2014)
9. Biradar, R., Manvi, S., Reddy, M.: Link stability based multicast routing scheme in MANET. Comput. Networks. **54**(7), 1183–1196 (2010)
10. Sevil, Å., Clark, J.A., Tapiador, J.E.: "Security Threats in Mobile Ad-hoc Networks,"University of York Department of Computer Sceicnce.Vol.1,pp.1–22
11. Yi, P., Dai, Z., Zhang, S., Zhong, Y.: "A New Routing Attack in Mobile Ad-hoc Networks,"International Journal of Information Technology, vol. 11, no. 2, pp.83–94
12. Issue, V., Issn, P.A.-.: Performance Evaluation of Black hole Attack in MANET and Intrusion Detection System. Int. J. Sci. Res. Educ. **2**(8), 1546–1551 (2014)
13. Kumar, S.: Wormhole attack in Mobile Ad-hoc Networks: A Review. Eng. Sci. Technology: Int. J. (ESTIJ). **2**(2), 268–275 (2012)
14. Gayathry, S.S., Gaur, R.N.: Handling Selfishness in MANETs – A Survey,International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Issue 11, (2014)
15. Prasath, P., Scholar, P.G.: Detecting Selfish nodes in MANET using Record-Trust based- Detection with Collaborative Watchdog, International Journal of Engineering Research & Technology (IJERT), COCODANTR – 2016 Conference Proceedings
16. Prof, S., Lolge, N., Baheti: Detecting and Managing SelfishNodes over MANET, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 9, September (2014)
17. K RAMA ABIRAMI, M.G., SUMITHRA: Preventing the impact of selfish behavior under MANET using Neighbor Credit Value based AODV routing algorithm. Indian Academy of Sciences (2018)
18. Ravi Singh Pippal:, efficient selfish node management method for MANET, international journal of computer sciences and engineering · (2018)
19. Ms, L., Odedra, P.A., Revar, P., Munindra, H., Lunagaria: An Effect of Selfish Nodes on Network Performance in MANET,International Journal of Advanced Research in Computer and Communication EngineeringVol. 5, Issue 6, (2016)

20. Muhammad Altaf Khan et, Al: A Survey on the Noncooperative Environment in Smart Nodes-Based Ad Hoc Networks: Motivations and Solutions, Hindawi, Security and Communication Networks Volume (2021)
21. Arvindkumar, P.N., Paliwal, A., "SINR and, Based Optimized, R.S.S.I.: AODV Routing Protocol for MANET using Cross Layer Interaction. Int. J. Sci. Res. **3**(6), 2012–2015 (2014)
22. Goyat, N., Anand, A.: Improvement Of Path In DSR In MANET Using An Inverted List Based Node Analysis. Int. J. Comput. Sci. Inform. Technol. Res. **2**(2), 427–432 (2014)

Figures

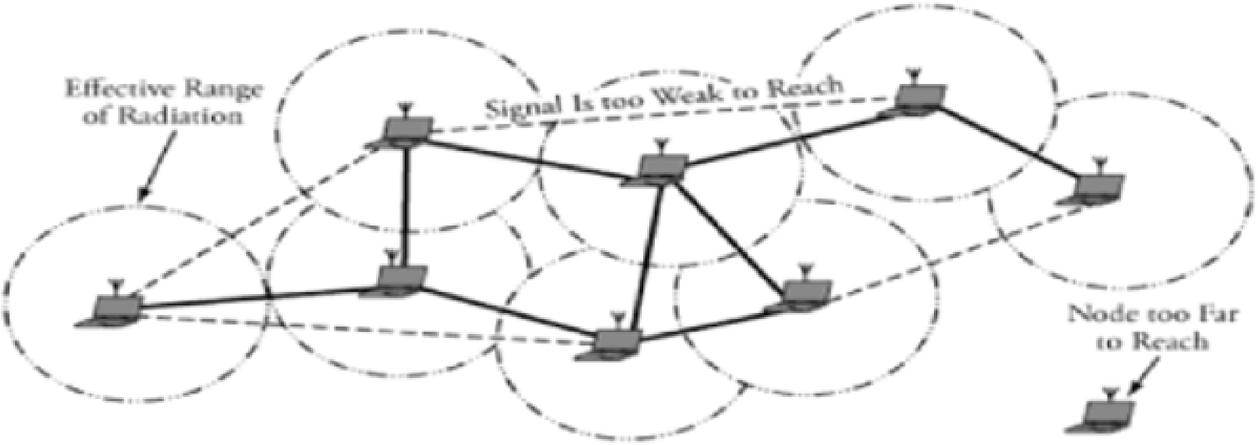


Figure 1

MANET Architecture [1,2,4]

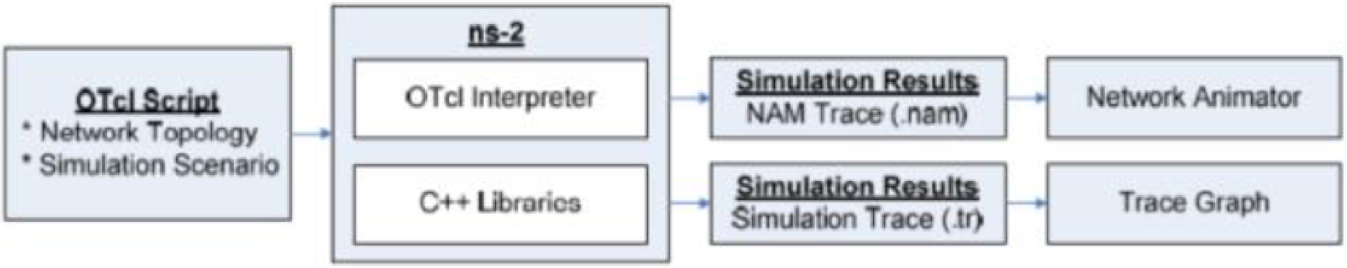


Figure 2

4.2 NS-2 Schema [22]

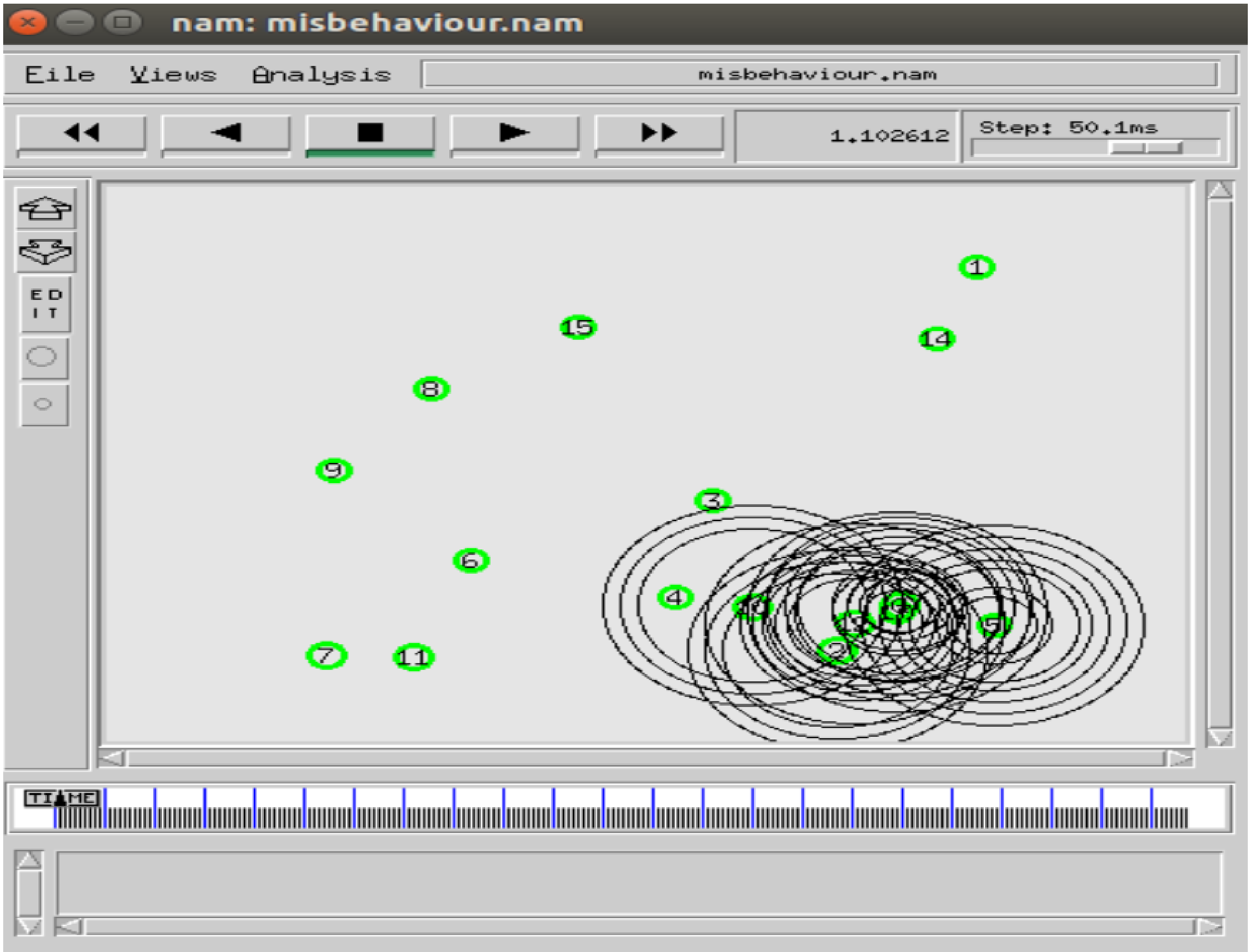


Figure 3

Figure 2 Communicating Between S and D via Node 12, 2, 0

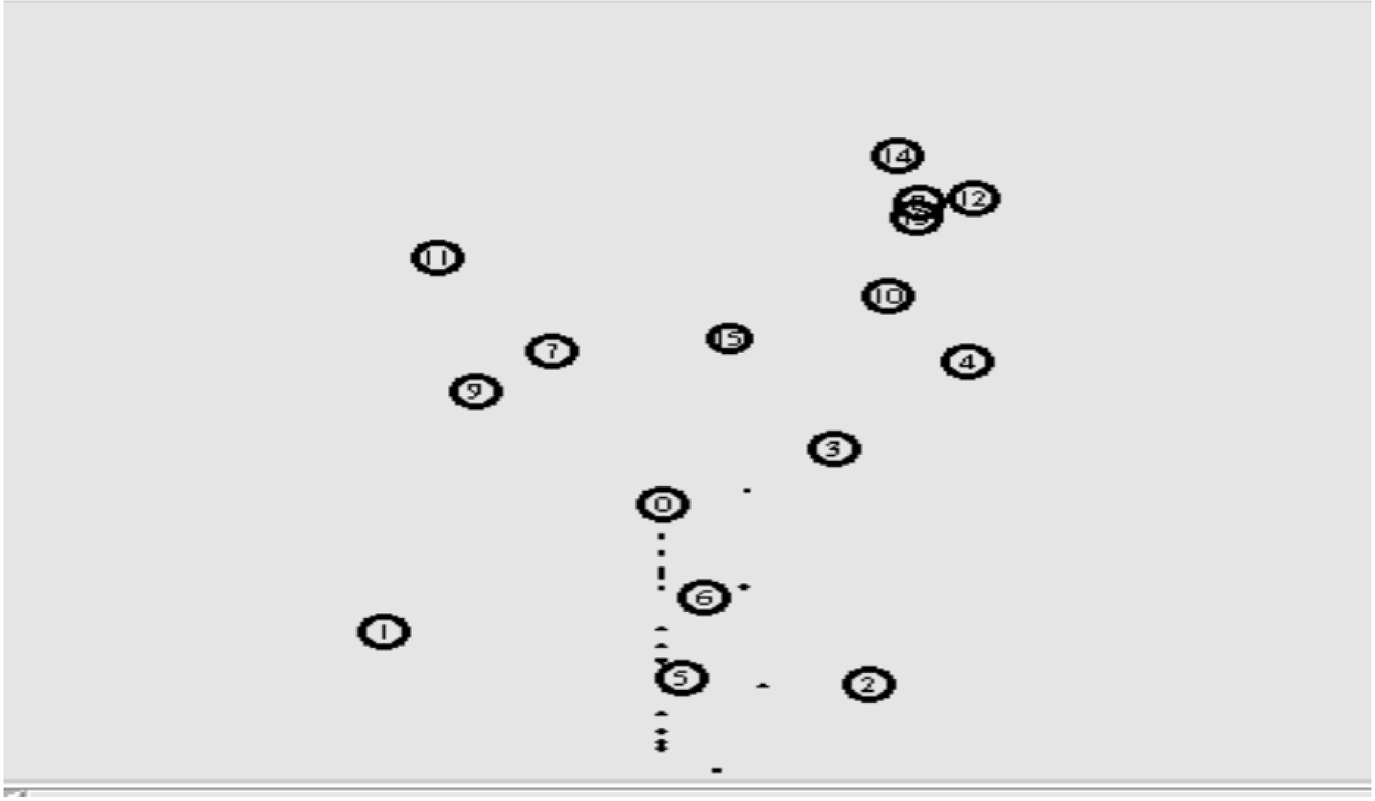
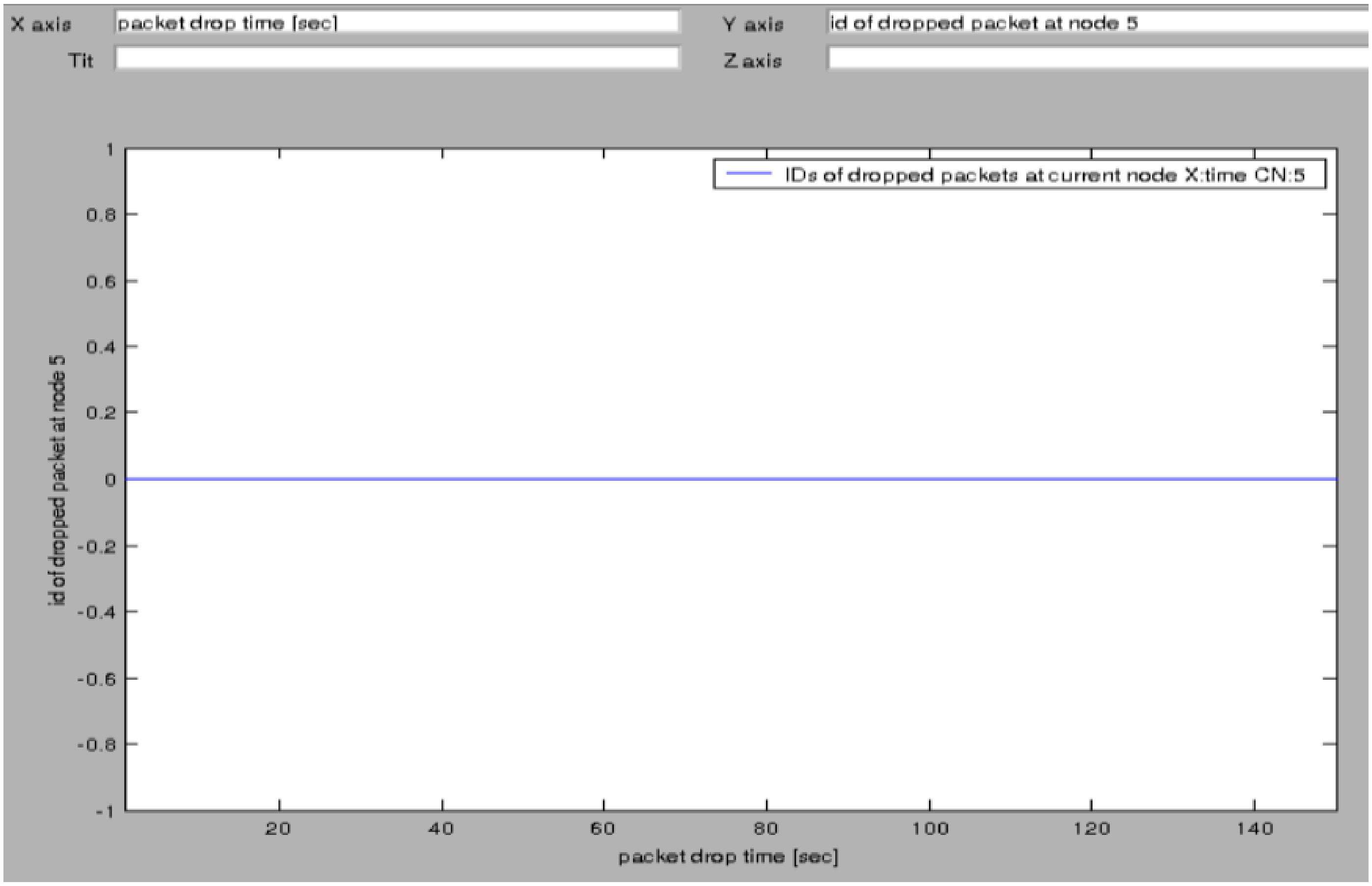


Figure 4

Figure 3 Sample of Packet Drop Node



X axis: packet drop time [sec]

Y axis: id of dropped packet at node 5

Tit:

Z axis:

Figure 5

Figure 3 Packet Drop Rate of Misbehavior Node on the Modified Protocol