IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 8, August 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208029 |

Design and Implementation of Energy Effectiveness Practices in Wireless Sensor Network over Simulation and Analysis of AOMDV in MANET

S. Vasanth [#1], L. Prakasam [#2], C.Thamilarasi [#3]

[#1] PG Scholar, Embedded System Technologies, PSV College of Engineering and Technology, Krishnagiri, India

[#2] Assistant Professor, Department of ECE, PSV College of Engineering and Technology, Krishnagiri, India

[#3] HOD, Department of ECE, PSV College of Engineering and Technology, Krishnagiri, India

ABSTRACT: Mobile Ad Hoc Networks (MANETs) suffer from flexibility, low power consumption, and lack of available support. Besides that, another problem of MANET is malware. The purpose of malicious nodes is to disrupt the operation of the routing protocol running on the network. Therefore, MANET needs to conduct an energy efficiency assessment. This is how we use the AOMDV routing protocol.The performance of the AOMDV routing protocol is evaluated using data collection methods and simulations using NS2, NAM. Quality of service (QoS) was not passed in this study, energy was used to control packet loss and efficiency of energy use. The simulations are run using malicious nodes that are assumed to occur at different times. As a result of this research, transmission efficiency was increased, the effect of packet loss was reduced and energy consumption was also evaluated.

KEYWORDS: energy efficiency, MANET, AOMDV, malicious nodes, throughput, packet loss.

I. INTRODUCTION

- Another problem with MANETs is the attack of malware. Malicious nodes can abuse the coordination of nodes to interfere with the operation of the network. Malicious nodes are also called selfish nodes.
- The purpose of malicious nodes is to interfere with the operation of the operating protocol and refuse to provide network services whenever possible.

Other issues with MANETs include flexible switching, low power consumption, and lack of support from existing infrastructure.

- The main problem is trying to save energy by using the AOMDV routing protocol in the presence of malicious nodes, using parameters of packet loss, throughput and power.

II. OBJCTIVE

Improve performance by comparing throughput, packet loss, or packet loss.

- Monitor the performance of the proposed algorithm AOMDV.
- Detect and prevent malicious attacks on MANETs using cache-based malicious node attack protection.
- Perform a reduction operation with the same delay without adding delay costs.
- Maintain the same performance even as the number of nodes and networks increases.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

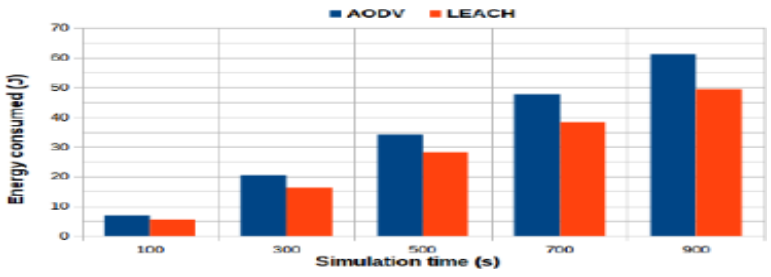
| DOI:10.15680/IJIRSET.2023.1208029 |

III. LITERATURE SURVEY

Mobile ad hoc networks (MANETs) are networks that use their nodes to send and receive existing packets. Nodes in MANETs are dynamic MANETs that can be built without using infrastructure. [1] Mobile Ad Hoc Networks (MANETs) have several transport protocols, one of which is the UDP transport protocol. A previous study by Bhavna Sharma on energy efficiency load balancing approaches to improve AOMDV routing protocol on MANET explained that UDP transport is unreliable for communication due to its connectionless nature. [2] Existing AOMDV multipath routing is more efficient than on-demand one-way routing. The proposed mechanism improves the routing behavior of AOMDV (which is called multipath multichannel energy efficient (MMEE)). It is based on load sharing based on node capacity and multi-channel communication. Node capacity is limited during the route request time. [3] Normal discovery routing, such as AODV and DSR, takes a long time to discover the path from the source to the destination due to the dynamic movement of a single path and node. Therefore, the AOMDV multipath routing protocol reduces the time consumption of the path discovery process. Each node provides information on queue length, residual energy, energy usage per packet, and bandwidth capacity. All the collected information is used to calculate the cost function at the destination node and select the three best paths based on the calculated cost function. [4] MANET properties such as dynamic topology and decentralized connectivity make routing a difficult task. While mobile nodes contain a large amount of data before transmitting it, ``unnecessary" data must be buffered. Overflow occurs when limited buffer space becomes full and excess data must be discarded. This accompanies the mutual dissipation of communication and assets such as node bandwidth, and at the same time hinders the reliability of event detection due to packet losses. As a result, they are considered necessary routing protocols that can consistently distribute data traffic between nodes and thus improve the performance of MANETs. [5]

III. EXISTING SYSTEM

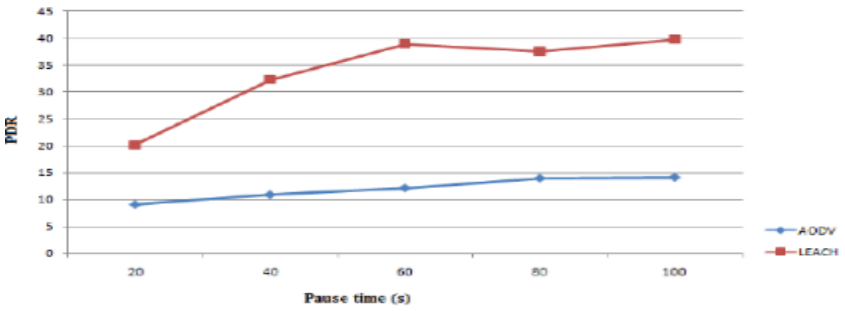
- This existing system is intended to provide a benchmarking analysis of the performance of routing protocols using ViSim, which integrates the Ns2 simulator.
- This work is done to analyze the performance of AODV and LEACH protocols including overall network performance such as throughput and packet delivery ratio of both protocols for different environment parameters for different environment parameters such as number of nodes and time simulation.
- Throughput, Goodput and Routing load (packet and packet size) are parameters to compare betweenrouting protocols for performance analysis.



|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208029 |



IV. PROPOSED SYSTEM

- In this proposed technique, we presenting the new approach for malicious node attack prevention in AOMDV.
- On the detection of node or misbehaving node, during the processing of path construction we have to get thenode id and pass it to add and path function of AOMDV.
- If the malicious node is appearing in path, we have to simply dump that path and add all rest of paths for the intended source destination pair communication. Also monitor the node energy efficiency etc.
- The results also show that throughput increases slightly when mobility of the nodes is increased in network.The increase speed of the nodes decreases both end-to-end delay and packet delivery ratio.

A. ADVANTAGES:

- This process is making use of normal time caching process only.
- Due this, delay is minimized as compared to previous malicious node attack detection mechanisms.
- Packet drop ratio is reduced drastically

V. ARCHITECTURE DESIGN

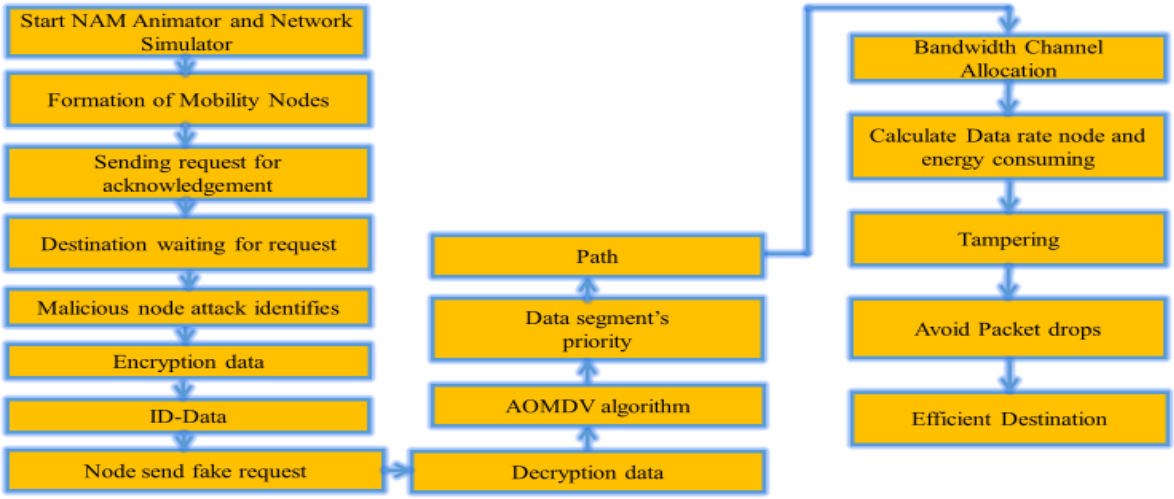


Fig no: 1 Block diagram for proposed method

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208029 |

VI. MODULE

There are 6 Modules in this system

- NS object and node creation module
- Detection of malicious nodes module
- AOMDV routing protocol algorithm
- Check node condition and data transmission module
- Encrypted data module
- Network animation module and X-graph

1. NS OBJECT AND NODE CREATION MODULE

In this module, the network simulator object is created and 45 nodes will be created and assigned initial position as well as the destination at each point in the simulation. Also, the size of each node is defined. The required variables will be set and assign with respective values.

2. DETECTION OF MALICIOUS NODES MODULE

In this module, the source node will request for the acknowledgement and based on the received acknowledgement, it will determine the correct destination and avoid all the other malicious nodes as they sent an inappropriate acknowledgement.

3. AOMDV ROUTING PROTOCOL ALGORITHM

The term AOMDV stands for Ad-hoc On-demand multi path distance vector. This protocol will determine the appropriate route for the construction of path for the purpose of data transmission from source to destination.

4. CHECK NODE CONDITION AND DATA TRANSMISSION MODULE

Then the condition of the node will be checked as whether it is in active state or inactive state. If it is in activestate, data will be transferred using TCP (Transmission Control Protocol). Otherwise, Node will be isolated.

5. ENCRYPTED DATA MODULE

In the middle of the data transmission, the malicious nodes in the network will try to connect in the transmission which may leads to data loss. In order to avoid such malicious node attack, the source node will generate encrypted key and the Destination node will accept the generated decrypted key for the purpose of security aspects.

6. NETWORK ANIMATION MODULE AND X-GRAPH

In this module, the simulated circuit will be displayed in the Network Animator (NAM) which is the end result of the simulation of the proposed circuit I.e., MANET (Mobile Ad-hoc Network). Finally, the x-graph will plot the throughput and packet loss.

VII. SYSTEM SOFTWARE

1. NS2

NS2 is short for Network Simulator Version 2. In Computer Communications, NS2 is a free-to-access real-time simulator designed for research projects.

2. SECURITY GOALS

All security systems should provide security mechanisms that can guarantee the confidentiality of the system. These functions are often referred to as the purpose of the security system. In this document, these objectives can be divided into the following three main groups: Privacy B. Trust C. Availability Data encryption in this document uses

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208029 |

symmetric cryptography algorithms to encrypt data transmission security between nodes. The system must encrypt the data or "systematically scramble the data so that it cannot be read without knowing the encoding key". This function is determined by a level of security system. The harder it is to crackan encrypted message, the safer it is. I recommend using, and symmetric ciphers

3. AOMDV ALGORITHM

TheAd Hoc Optional Multipath Distance Vector Routing (AOMDV) protocol is an extension of the AODV protocol for calculating multi-loop and link discreteness.The access path for each destination contains a list of next hops with the number of counters. All subsequent tabs have the same sequence number. This is useful for tracking the route. For each destination, nodes maintain a broadcast hop count, which is defined as the maximum hop count of each route used to deliver the broadcast to the destination. The node's degree of freedom of the node is provided by accepting the route to the destination if the node has fewer hops than the specified hop count for that destination.Because the maximum hop count is used, the reported hop count does not change for the same sequence number. When a route advertisement is received for a higher numbered destination, the next listing and ad skip count are reset. AOMDV can be used to find node-discrete or link- discrete paths. AOMDV's full name is Ad Hoc On-demand Multipath Distance Vector Routing, a proprietary routing protocol designed for wireless ad hoc networks. It is an extension of the well-known AODV (Ad Hoc On-Demand Distance Vector) routing protocol.AOMDV is mainly used to improve the reliability and performance of data transmission in mobile ad hoc networks (MANET).

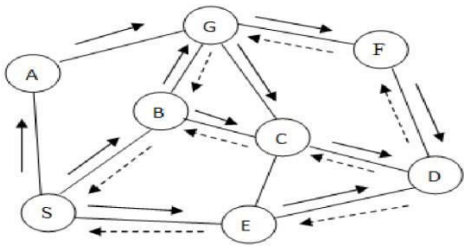


Fig no: 2 AOMDV Algorithm

4. NUM GRAPH

A graph is a non-linear document consisting of vertices and edges. Vertices are sometimes called nodes, and edges are lines or arcs that connect two nodes in a graph. Traditionally, a graph consists of a series of vertices (V) and a series of edges (E). Graph data models are powerful tools for representing and analyzing relationships between objects or entities. They are particularly useful in areas such as social analysis, consensus processes, and computer networks. In sports data science, graphs can be used to analyze and understand the effectiveness of teamwork and player interactions on the field. Think of a football game as a network where the players are the nodes and their interactions on the field are the edge. This network of connections is what image data represents and is key to understanding team performance and players' strength in the game.

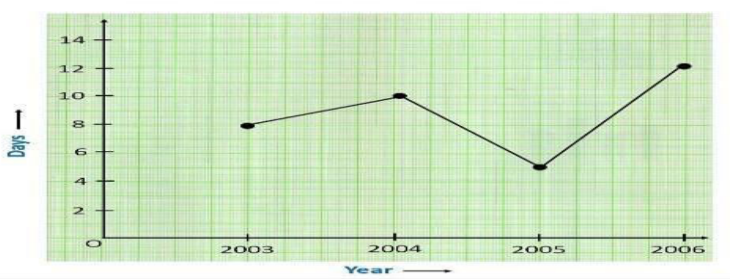


Fig no: 3Num Graph

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208029 |

PARAMETERS	VALUES
Area of Simulation	(1000 X 1000) m
Nodes number	45
Types of Routing protocol	DSRInternet protocol type TCP
Antenna Model	OmnidirectionalMax package 50
Type of the MAC	802.11
Transmission speed	1.2 Mbps
Bandwidth	20MHz

VIII. RESULTS

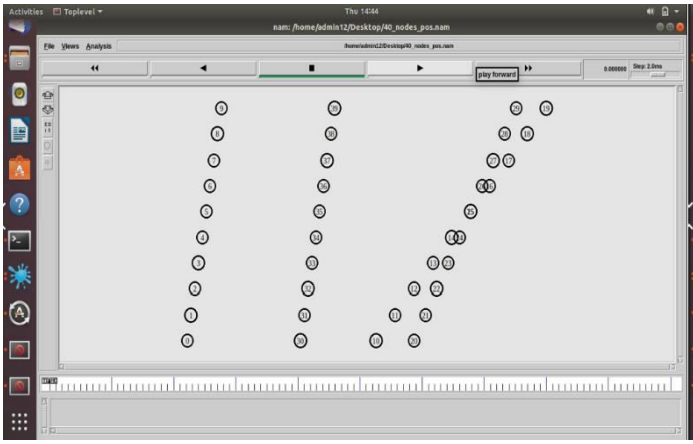


Fig no:4 Nodes in the source

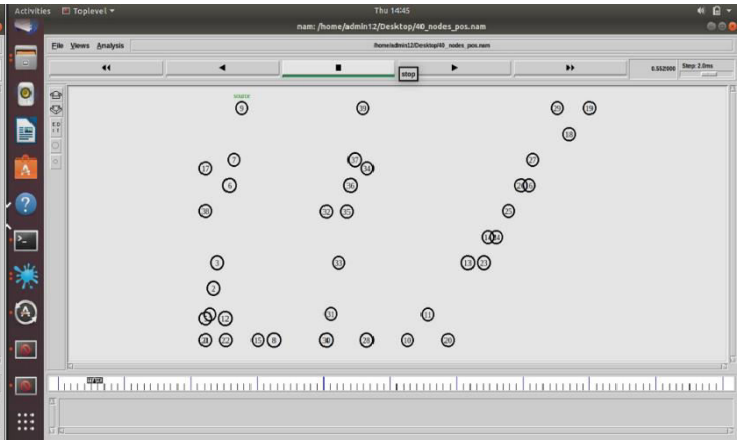


Fig no:5 Source node send ack request

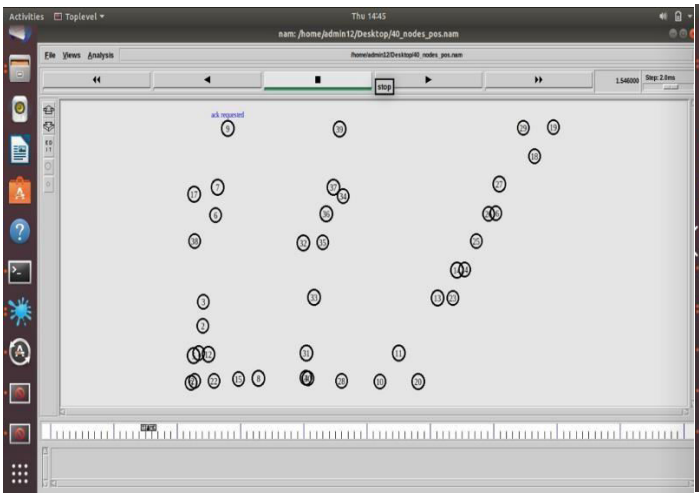


Fig no:6 Acknowledgement received node

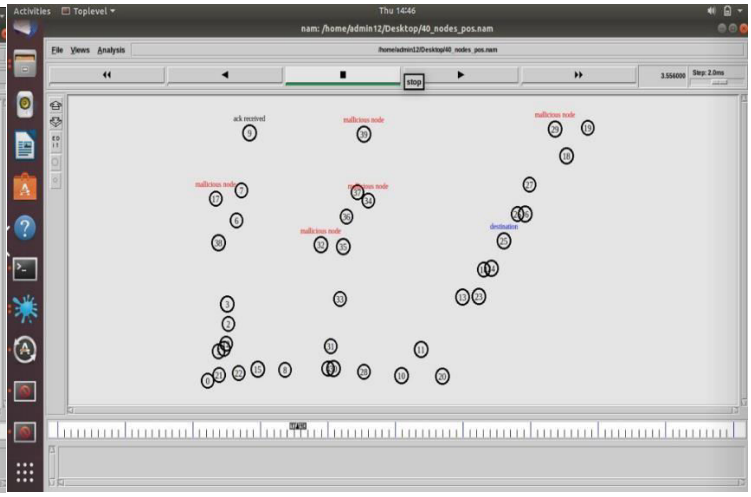


Fig no: 7 Data received in destination

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208029 |

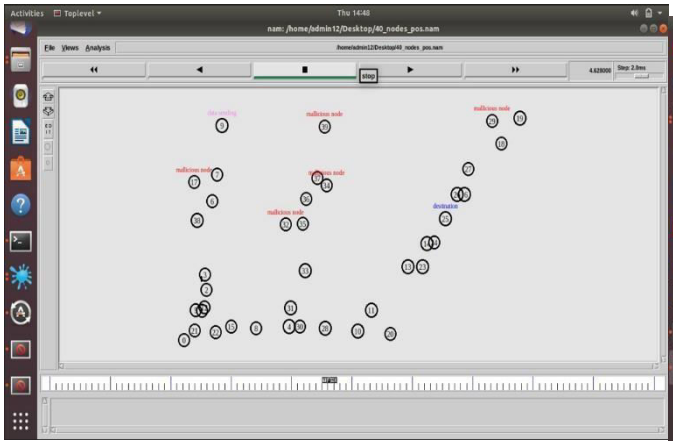


Fig no:8 Data received in node

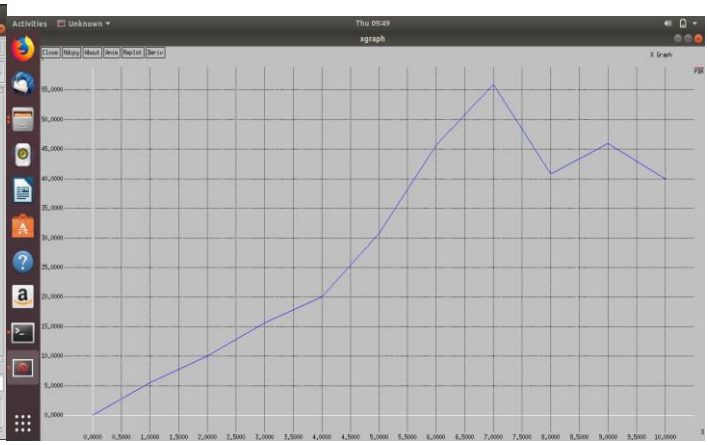


Fig no:9 Packet Delivery Ratio (PDR)

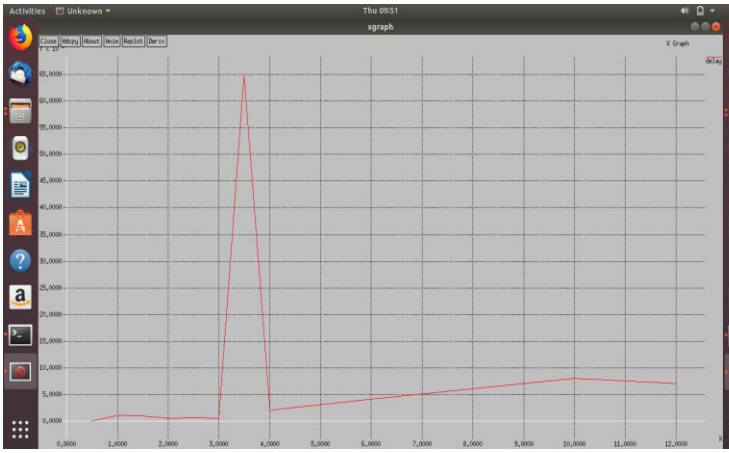


Fig no: 10 Delay

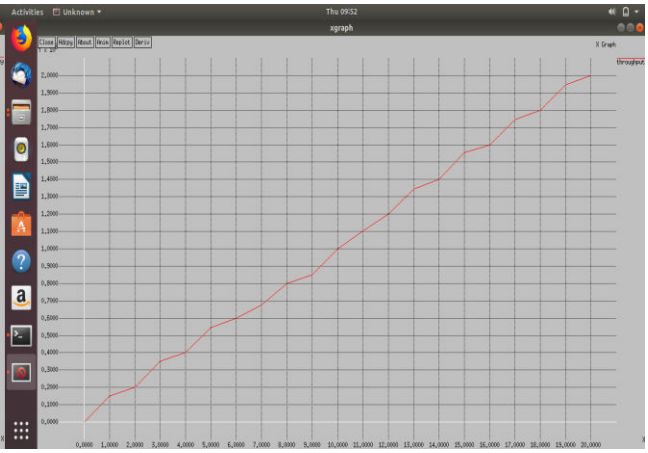


Fig no:11 Throughput

IX. CONCLUSION

In this project, we presented a new technique for detecting malicious node attacks in wireless network present in MANET. Our proposed system implements the AOMDV protocol as a routing protocol. It does not require additional hardware, node placement or sending any information to the base station. No further communication is used for node detection and isolation purposes. AOMDV is generally a more efficient routing protocol because it creates ideal paths that can be improved for communication purposes. This methodology further ensures security in the data transfer process and energy efficiency. The proposed technique is also applicable when nodes advertise good connection, strong transmitted power, etc. Even in such cases, our systemcan detect and isolate such attacks in wireless networks.

REFERENCES

1. Mishra, S. Singh, and U. Singh, “Detecting And Avoiding Of Collaborative Black Hole Attack On MANET Using Trusted AODV Routing Algorithm,” 2019.
2. Sharma, S. Chugh, and V. Jain, “Energy Efficient Load Balancing Approach to Improve AOMDV Routing in MANET,” 2020.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208029 |

3. L. M. Bendale, R. L. Jain, and R. L. Patil, "Study of Various Routing Protocols in Mobile Ad-Hoc Networks," 2021.
4. N. R. Patel, Bhupendra B., Thaker, Chirag S., Jani, "Analysis and Implementation of Malicious Node in AODV," 2019.
5. M. H. Alamsyah., Setijadi, Eko., Purnama, I Ketut Eddy., Purnomo, "AnalisisKinerjaProtokol Routing Reaktif dan Proaktif pada MANET," 2020.
6. S. U. Masruroh and K. U. Sabran, "Emergency-aware and QoS based routing protocol in wireless sensor network," in Proceedings of International Conference on Intelligent Autonomous Agents, Networks and Systems, INAGENTSYS , 2020, pp. 47–51.
7. S. Saputro, S. U. Masruroh, and N. Hakiem, "Comparative analysis of LEACH-C and pegasis routing algorithms in a wireless sensor network using network simulator-2," J. Telecommun. Electron. Comput. Eng., vol. 9, no. 2, pp. 91–94.
8. Abbas, Laraib, Muddesar Iqbal, Muhammad Shafiq, Saqib Rasool, and Azeem Irshad. "AComprehensive REVIEW OF SOME WELL KNOWN ROUTING PROTOCOLS FOR MANETS."2020.
9. Anuj K. Gupta, Harsh Sadawarti, Anil K. Verma, Performance analysis of MANET Routing Protocols in different mobility models, May 2020.
10. Ammar Odeh, EmanAbdelFattah and MuneerAlshowkan, Performance Evaluation Of AODV And DSR Routing Protocols In Manet Networks, International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, July 2021.
11. C.E Perkins, E.M. Royer, and S. Das, Ad hoc On-demand Distance Vector (AODV), RFC 3561, July 2019.
12. Elizabeth M. Royer and Chai-KeongToh, A review of current routing protocols for ad hoc mobile wireless networks , Technical report, University of California and Georgia Institute of Technology, USA, 2022.
13. G.VijayaKumar ,Y.VasudevaReddyr , Dr.M.Nagendra , Current Research Work on Routing Protocols for MANET: A Literature Survey, International Journal on Computer Science and Engineering,2019.
14. Mina VajedKhiavi, Shahram Jamali,PerformanceComparision of AODV and AOMDV Routing Protocols in Manet,International Research Journal of Applied and Basic Sciences, 2020.
15. Maveen Singh Chadha, Rambir Joon, Sandeep,Simulation and comparison of AODV ,DSR and AOMDV routing protocols in MANET International Journal of Soft Computing and Engineering,July 2021.
16. Krontiris, I., Giannetsos, T., Dimitriou, T.: Launching a Sinkhole Attack in Wireless Sensor Networks; The Intruder Side. 2018 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications. pp. 526–531. IEEE (2018).

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details