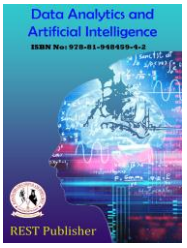
Data Analytics and Artificial Intelligence

Vol: 3(3), 2023

REST Publisher; ISBN: 978-81-948459-4-2

Website: http://restpublisher.com/book-series/daai/



Network Traffic and Energy Monitoring in MANET Using AODV Routing Protocol

***Lavanya.A, Vijay Aravinthan N, Vimalkarthik J, Vyshak Vasudevan Nair V**

Adhiyamaan College of Engineering, Hosur, Tamil Nadu, India.

**Corresponding Author Email: vijaykcc123@gmail.com*

ABSTRACT - *A Mobile Ad-hoc Network (MANET) is an infrastructure-less wireless network and it does not require a previously defined structure including an Access point (AP) or a router. Wireless mobile node networks are deployed and they create a network among themselves for the sake of the transfer of data. To find the appropriate or approximate route from the sender to the receiver, we need routing protocols. There are various routing protocols for mobile ad-hoc networks. One of the main routing protocols is the Ad-hoc On-demand Distance Vector routing protocol (AODV). Multipath routing methods are dependable on nearby nodes for finding the shortest path. And several data packets have dropped to the network traffic. The performance of these protocols can be decided based on different criteria and parameters such as End-to-End delay, Packet delivery ratio, etc. In this project, we analyze the performance of these protocols based on the Energy they consumed. We create various types and different mobility scenarios as well as different traffic scenarios and observe the performance of these protocols in terms of the consumption of energy during the simulation process. The network topology of the network changes dynamically and there is a change in energy consumption.*

1. INTRODUCTION

When mobile nodes come together as needed in order to share data or files amongst themselves without any support from the Access Point or any other fixed station, a Mobile Ad-hoc network is formed. In this network, each node on its own serves both as receiver as well as sender. The nodes can freely move and transfer their position from one point to another within the network. As we know that each node is wirelessly connected to another through a topology in order to transfer data, therefore, the movement can bring about a drastic change in the topology of the links and even the whole network.

MANET contains nodes that can move the network with help of their mobility factors. It is very useful in terms of flexibility factor and capable of forwarding the packets to other nodes. The wireless network has communication range that is based on multi-hop source to destination or sender to receiver within their communication range. Performance of the network is a vital part of wireless networks. In wireless networks, communication or transmission range is also considered as an important factor for successful packet delivery including multi-hop networks. Transmission range has partial effects on the performance of the network by adjusting the height of the antenna (omni antenna). If the transmission range is minimized or maximized, that frequently has various effects on the network performance such as packet delivery ratio, end to end delay and routing load. Furthermore, especially in an overloaded network where nodes are frequently changing. However, the aim of the research is to observe that the transmission range effects on the network performances such as throughput, packet delivery ratio, and end to end delay. Various routing protocols (AODV, DSDV and DSR) have been used to examine the network performance using transmission range. Routing protocol's reliability and scalability across VANETs environment are currently the subject of intense research because routing protocols are basically the heart of wireless networks.

2. OBJECTIVE

- The Routing Protocol is used to find suitable routes between communicating nodes. They do not have to use any access points to connect to other nodes.
- Every mobile node maintains the routing table, which contains the destinations to which it currently has a

route.

- In AODV, when a source node desires to send packets to the destination but no route is available, it initiates a route discovery process.so this is why we can avoid the network traffic.

3. LITERATURE SURVEY

An examination of sensor networks.The open nature of wireless communication channels, the scarcity of infrastructure, the quick deployment techniques, and the hazardous surroundings where sensor nodes are deployed, however, render them susceptible to a variety of security assaults. A 2020 study by E. C. H. Ngai, J. Liu, and M. R. Lyu.

In Wireless Networks, On the Anonymous analysis for Sinkhole Attack. Because the base station is involved in the detecting process using this method, the protocol has a high communication cost. The IDs of the impacted nodes are included in a request message that the base station sends out to the whole network. The impacted nodes send a message to the base station in response that contains their IDs, ID of the next hop and the associated cost. The occurred data is then used from the base station to make a network flow graph for finding the sinkhole. To avoid tampering of packets during transmission, encryption and path redundancy is proposed. B. G. Choi, E. J. Cho, J. Ho Kim, C. S. Hong, and J. H. Kim [2019].

A Sinkhole Attack Analyzing Mechanism for LQI based Mesh Routing in WSN. They Suggested a detection scheme for sinkhole attacks based on Link Quality Indicator in sensor networks. The suggested method can find a sinkhole attack. It Uses LQI based routing and several detecting nodes. General nodes collect NS2 minimum link cost between neighborhood nodes and detecting nodes compute the minimum path cost with surrounding detector nodes in the proposed method. It can detect an abnormally strong signal from the actions of the malicious node by referring to the minimum link cost table. N.K. Sreelaja, G.A. Vijayalakshmi Pai [2020].

Swarm intelligence-based method for attack analyzing in wireless networks. In WSN, the node misbehaves due to compromised or selfish intentions. Thereby various attacks happen in WSN because of free and unprotected communications channels, broadcast transmission, hostile environment and limited resources. Leovigildo Sánchez-Casado, Gabriel Maciá-Fernández, PedroGarcíaTeodoro,Nils Aschenbruck[2020].

Existing System: The simulation results reveal that the secure communication using certificate revocation approach, traffic-aware secure routing for VANETs using Hybrid Enhanced Glowworm Swarm Optimization (HEGSO), and trust model for secure communication in VANETs is ensuring the security in VANETs. When compared to existing routing protocols, the proposed scheme will reduce the packet failure ratio, response time, and throughput. When compared to ARIOR and I-AREOR, the HEGSO technique shows delays by 20% and 34%, respectively. In this project, traffic-aware secure routing using HEGSO for urban VANETs has been proposed to establish traffic-aware routing in urban scenarios. Here, the traffic parameters like the average speed along with TD were optimized using the HEGSO algorithm. This paves a way for better route acquisition and also better connectivity.

Disadvantages: In existing methods preferred and for higher traffic DSDV protocol is preferred . The existing one was also compared with the prevailing works. This work can well be additionally enhanced by considering more traffic parameters.

4. PROPOSED SYSTEM

The working of this protocol also happens on a need basis and the route from the sources to the destination is officiated only up till it is needed. In order to recognize changes and up gradations in the routes in case of link failure, etc, sequence numbers are used in this scheme. A network of 35 mobile nodes is simulated. Different mobility and traffic scenarios are used and the energy consumption of the network is monitored at regular intervals. Omni-directional antenna, TCP/FTP link layer were used. Simulating area is large i.e., 1000 * 1000. The protocol is free of looping, starts automatically and is used for large scaled networks in which many nodes are deployed. The working process is carried out by the packets. Similarly at very high mobility, for low traffic AODV protocol It is also observed that the value of the residual energy is dependent on the topology of the network. This means that the residual energy will have different values for when the nodes are kept static and then mobilized. Less traffic suggests less consumption of energy and more energy is consumed when the traffic is increased. The results will show the throughput and decrease slightly when mobility of the nodes is increased in the network. The increase in the speed of the nodes decreases both end-to-end delay and packet delivery ratio.The status of the node can be detected as dead and alive. Energy Consumption is low and less traffic suggests less consumption of energy

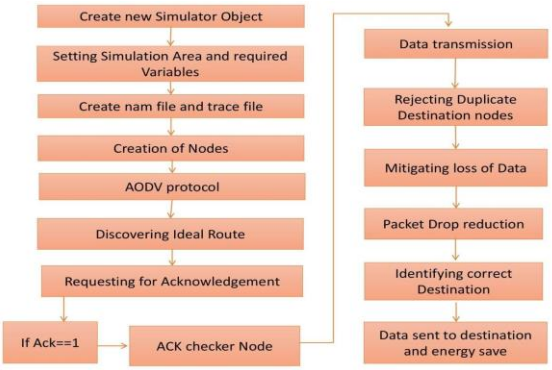


FIGURE 1. Architecture design

Modules:

There are 4 modules used in this project:

- AODV routing protocol algorithm
- Check node condition and data transmission module
- Network animation module
- Graph module

Module Description:

Network animation module:

The network animation module typically provides a variety of visualization tools and features, such as the ability to display network traffic, link utilization, and packet routing paths. It may also include tools for configuring and customizing the appearance of the GUI, such as the ability to change the color and size of nodes and links, or to add labels and annotations to the network topology.

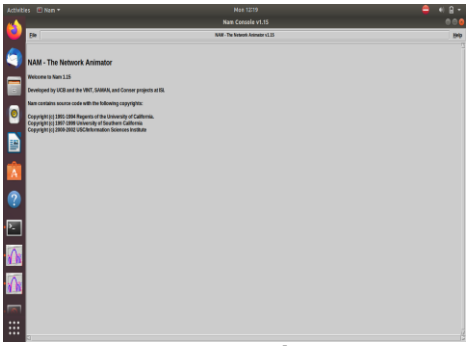


FIGURE 2. Network Animator

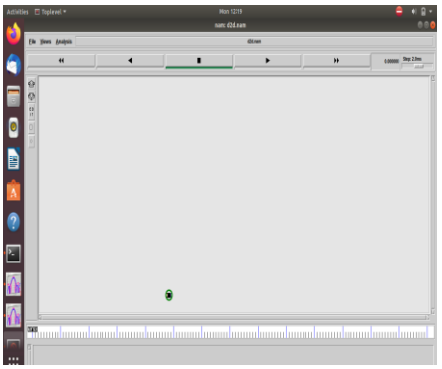


FIGURE 3. Initial Node in NAM

Aodv routing protocol algorithm:

Ad hoc On-Demand Distance Vector (AODV) is a reactive routing protocol designed for wireless ad hoc networks. AODV works by broadcasting route request packets (RREQ) to discover a route to the destination node. When a node receives a RREQ, it checks its routing table to see if it has a valid route to the destination. If it does, it unicasts a route reply packet (RREP) back to the source node with its route information. If it doesn't have a valid route, it broadcasts the RREQ packet to its neighbors.

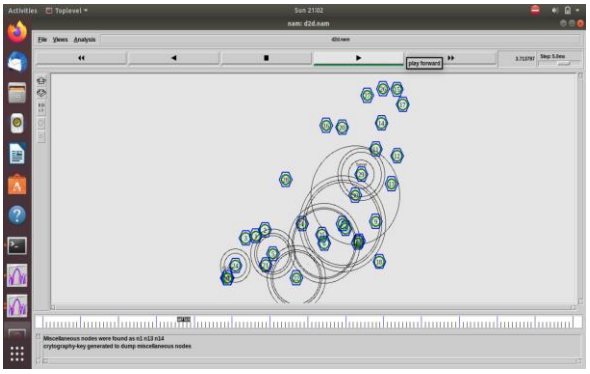


FIGURE 4. Checks miscellaneous nodes

Check node condition and data transmission module

In network simulation, node condition checking is an important aspect of simulating a realistic network environment. Node condition checking involves monitoring the status of individual network nodes to identify any changes or issues that may impact the overall network performance. One key aspect of the data transmission module in NS-2 is the ability to specify the characteristics of the simulated communication channel.

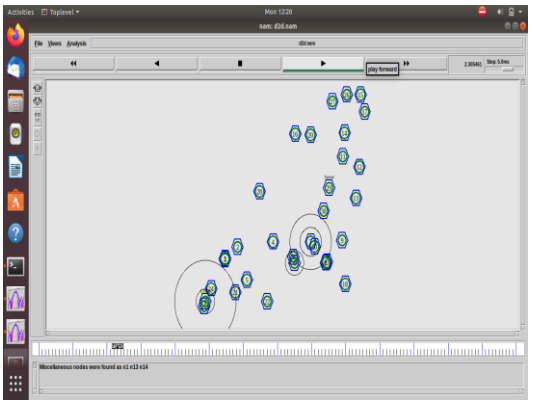


FIGURE 5. Full energy level (Green)

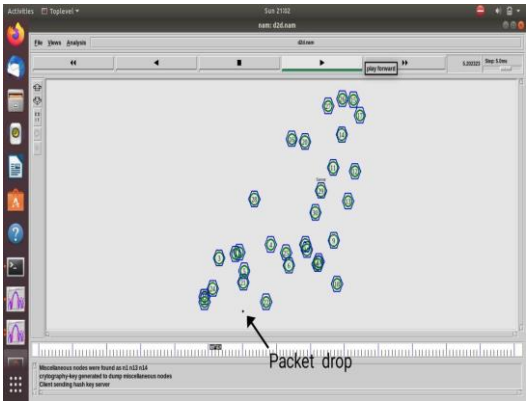


FIGURE 6. Packet Drop

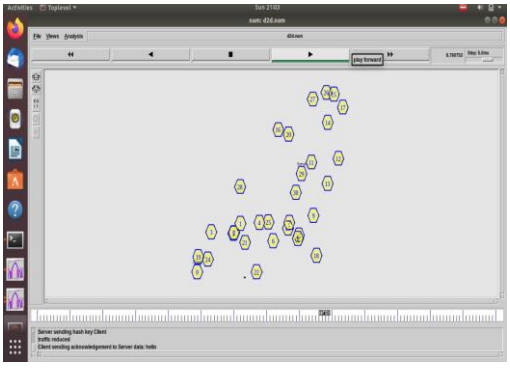


FIGURE 7. Medium energy level (Yellow)

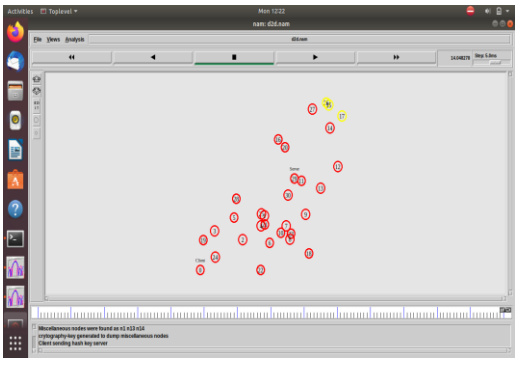


FIGURE 8. Low energy level (Red)

Graph module

The graph module in network simulation is a component of network simulation software that provides tools for visualizing and analyzing data generated during network simulation. The module allows users to plot and graph various performance metrics, such as throughput, packet loss rate, and latency, in order to evaluate the behavior and performance of the simulated network.

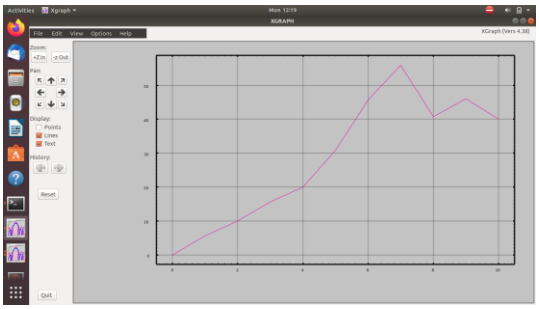


FIGURE 9. Packet loss rate

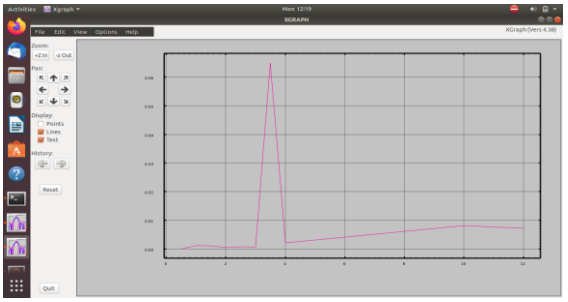


FIGURE 10. Latency

5. SYSTEM FUNCTION

Enter the commands in the terminal to access the network simulator to initiate the process.The network simulator starts with initially the nodes set by the user ,here 35 nodes are used and time latency is set to 4-5ms.the nam animator checks for the miscellaneous nodes and the packet drop takes place.the energy level of the nodes varies and drop where it can identified through changing color of the nodes.The graphs would be executed as a result after the execution of the process.

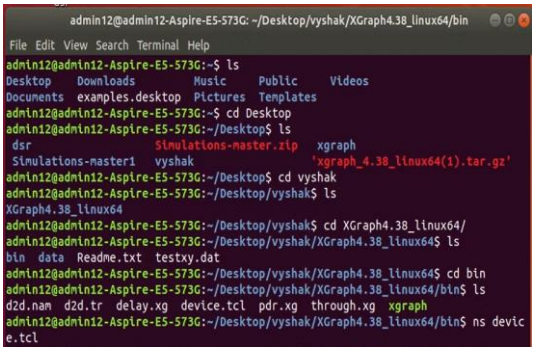


FIGURE 11. Terminal Commands

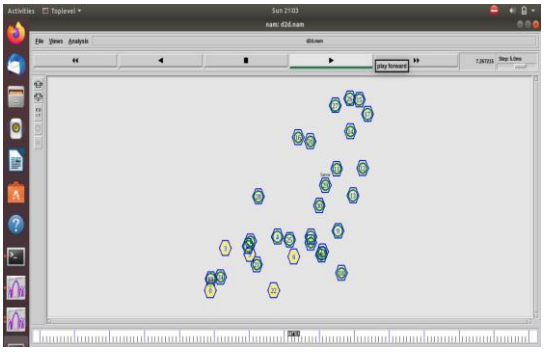
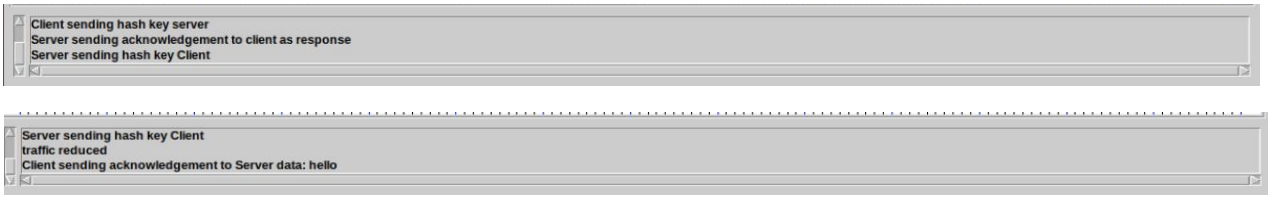
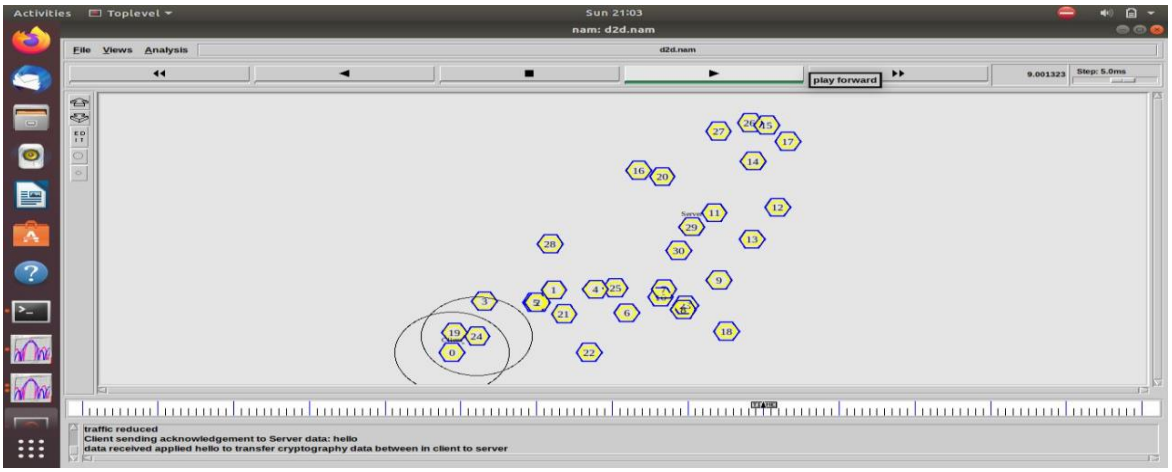


FIGURE 12. Change in energy level



6. RESULT

In this paper, through network simulation the ns-2 tool detects the fake nodes and check for the miscellaneous node. It sends an encrypted hash key to receiver from sender to prevent the malicious attack that takes place. Then the traffic is reduced between the node transmission and the message is received in the server side and acknowledgement is received in the client side and here the energy level drops at slow rate.



7. CONCLUSION

In this project we used the AODV protocol to analyze the node energy level and monitor the traffic. This can be done by the network simulator tool which will give complete representation and the animation view of the nodes. The transmission data from sender to receiver then the packet drop of each node will be easily captured . Acknowledgement plays the main role in this project.

REFERENCE

[1]. Rong, C., Eggen, S., Cheng, H.: A novel intrusion detection algorithm for wireless sensor networks. 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE). pp. 1–7. IEEE (2019).

[2]. Chen, C., Song, M., Hsieh, G.: Intrusion detection of sinkhole attacks in large-scale wireless sensor networks. IEEE International Conference on Wireless Communications, Networking and Information Security. pp. 711–716. IEEE (2018).

[3]. Teng, L., Zhang, Y.: SeRA: A Secure Routing Algorithm Against Sinkhole Attacks for Mobile Wireless Sensor Networks. 2010 Second International Conference on Computer Modeling and Simulation. pp. 79–82. IEEE (2019)

[4]. Sharma, K., Ghose, M.: Wireless sensor networks: An overview on its security threats. Int. J. Comput. Their Appl. 42–45 (2018)

[5]. Ngai, E.C.H., Liu, J., Lyu, M.: On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks. 2006 IEEE International Conference on Communications. pp. 3383–3389. IEEE, Istanbul (2018).

[6]. G. Singh, M. Prateek, S. Kumar, M. Verma, D. Singh, and H. Lee,‘‘Hybrid genetic firefly algorithm-based routing protocol for VANETs,’’IEEE Access, vol. 10, pp. 9142–9151, 2022.

[7]. P. Chithaluru, S. Kumar, A. Singh, A. Benslimane, and S. K. Jangir,‘‘An energy-efficient routing scheduling based on fuzzy ranking scheme for Internet of Things,’’ IEEE Internet Things J., vol. 9, no. 10,pp. 7251–7260, May 2022.

[8]. P. Chithaluru, F. Al-Turjman, T. Stephan, M. Kumar, and L. Mostarda,‘‘Energy-efficient blockchain implementation for cognitive wireless communication networks (CWCNs),’’ Energy Rep., vol. 7, pp. 8277–8286,Nov. 2021.

[9]. P. K. Chithaluru, M. S. Khan, M. Kumar, and T. Stephan, ‘‘ETH-LEACH:An energy enhanced threshold routing protocol for WSNs,’’ Int. J. Commun.Syst., vol. 34, no. 12, Aug. 2021, Art. no. e4881.

[10]. A. Polisher, L. Kant, Y. Gottlieb, “Portable Programmable Layer 3 QoS for Tactical MANETs: A P4/PSA-Based Architectural Approach”, Proc.IEEE MILCOM 19, Norfolk, Virginia, November 2019.

[11]. J. He, M. Suchara, M. Bresler, J. Rexford and M. Chiang, “Rethinking Internet Traffic Management: From Multiple Decompositions to a Practical Protocol”, CoNEXT’07, December 10-13, NY, USA.

[12]. He, J., Zhang-Shen, R., Li, Y., Lee, C., Rexford, J., & Chiang, M. (2008). DaVinci: dynamically adaptive virtual networks for a customized internet. CoNEXT '08.

[13]. K. Xu, H. Liu, J. Liu and J. Zhang, “LBMP: A Logarithm-Barrier-Based Multipath Protocol for Internet Traffic Management”, IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No. 3, March 2011.

[14]. Clausen, T., Dean, J., and C. Dearlove, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 6130, April 2011.

[15]. Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg, "The Optimized Link State Routing Protocol Version 2", RFC7181, April 2014.