International Journal of Innovative Research in Technology and Science
ISSN: 2321-1156 www.ijirts.org Volume 11 Issue 4, July 2023

An Energy Optimised and Energy Efficient MANET application Using Routing Protocol

Mayank Soni, Jitendra Singh
Department of EC
Babulal Tarabai Institute of Research & Technology, Sagar (MP), India
sonimayank347@gmail.com, jitendra.btirt@gmail.com

Abstract: This research focuses on enhancing mobile ad hoc network (MANET) applications through an energy-optimised and energy-efficient MANET routing technology. The Internet of Vehicles (IoV) is a recent VANET application that combines the Internet and IoT. MANET is an infrastructure-less network where wireless devices can communicate and exchange information without a centralised administrator. It consists of mobile nodes wirelessly connected in a self-configured, self-healing network.

As technology advances, there is a growing demand for a traffic environment that facilitates collaboration among vehicles, leading to less traffic congestion, reduced chances of collisions, lower communication latency, fewer communication faults, and a higher message delivery ratio. Vehicular ad hoc networks (VANETs) are designed to enable vehicles to communicate in an infrastructure-free environment. In this context, vehicles in a MANET communicate with each other using a routing protocol to exchange messages and provide information, especially regarding hazardous situations.

In this study, we propose an energy-optimised and energy-efficient MANET application using the MAODV routing protocol. We compare this approach to the existing AODV protocol, which exhibits a lower packet delivery ratio, higher latency, and increased energy consumption. Through implementation in a network simulator, we demonstrate that our proposed technique utilising the MAODV protocol results in a higher packet delivery ratio, reduced delay, and lower energy consumption.

The primary objective of this research is to present commonly utilised metrics in various proposals and their corresponding application scenarios. By utilising the routing protocol (MAODV), our proposed approach aims to improve the performance of MANET applications.

Keywords: MANET, Wireless, Vehicular Ad Hoc Network, Routing Protocol, AODV Protocol, Clusters, Cluster Head, Network Area, Delay, PDR, Energy Optimized, Energy Efficient.

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a collection of mobile nodes without a fixed infrastructure, allowing them to change their geographic locations dynamically. These networks possess dynamic topologies, random mobility, and limited resources and may experience network partitioning. MANETs are self-organised multi-hop systems consisting of mobile wireless nodes [1]. In MANETs, nodes that are out of direct communication range require intermediate nodes to forward their messages, as shown in Figure 1. For instance, Sender S communicates with

Receiver R through intermediate nodes A, and B. Common applications of MANET include military or police networks, business operations like oil drilling platforms or mining operations, and emergency response operations in the aftermath of natural disasters such as floods, tornadoes, cyclones, and earthquakes.

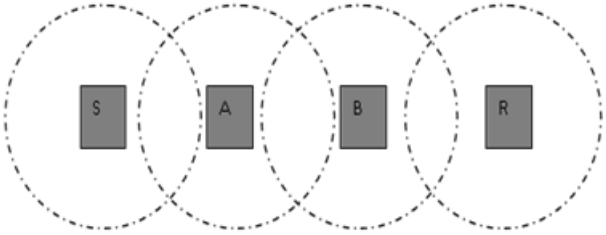

Figure 1: Example of MANET

However, due to the multi-hop routing and open operating environment, MANETs are susceptible to attacks from self-seeking or malicious nodes, such as packet-dropping (blackhole) attacks and selective forwarding (grey-hole) attacks. A blackhole attack disrupts the established path between the sender and receiver [2]. In this case, the black hole offender creates an immediate node link to the sender, resulting in a black hole attack between them. This means more trusted nodes are needed to achieve higher successful communication rates.

We propose a detection and prevention technique against blackhole attacks to address this issue. We use a profile-based detection technique to obtain information about the offender node, such as node type, number of attack packets, attack time, etc. [3]. Subsequently, we prevent blackhole attacks using a neighbour trust-based technique to secure the mobile ad-hoc network communication. Our proposal aims to provide secure and reliable communication and simulate it using Network Simulator-2 to analyse the network behaviour in attack and prevention scenarios. Additionally, we will evaluate the network's performance based on parameters such as throughput, packet delivery ratio, and routing load.

1.1 Security Aspect in MANET

In order to ensure a secure AODV (Ad Hoc On-Demand Distance Vector) protocol, it is essential to understand security features and mechanisms. Security is achieved through a combination of processes, procedures, and systems that guarantee confidentiality, authentication, integrity, availability, access control, and non-repudiation [4]. Since MANETs operate in an open medium, all nodes within the communication range can access data. Therefore, the following security aspects need to be addressed:

i. Confidentiality: Prevent unauthorised nodes from accessing data.
ii. Authentication: Verify the identity of nodes to ensure that senders and neighbour nodes are legitimate, preventing unauthorised access to resources and confidential information, as well as interference in other nodes' operations.
iii. Integrity: Prevent malicious nodes from altering and resending data, which can lead to replay attacks like the wormhole attack.
iv. Non-repudiation: Ensure that a node cannot deny sending a message, providing accountability for its actions [5].

Vulnerabilities in MANETs primarily target the routing layer, including physical, MAC, and network layers, which play a crucial role in the routing mechanism during packet delivery. Other vulnerabilities, such as application, network, and data security, are also present but are not covered in detail here. Attacks in the networking layer of the wireless ad hoc network generally serve two

purposes: not forwarding packets and manipulating routing messages, including sequence numbers and destination addresses. Using cryptographic mechanisms or authentication in a network is a preventive approach against attackers. However, even if keys are protected by tamper-proof hardware in a battlefield scenario where MANETs are used, captured vehicles may exhibit different behaviours. Additionally, failing or self-seeking nodes can impact network performance, affecting the proper processing of network packets in the routing mechanism. Hence, an intrusion detection system is needed to understand possible attacker actions and develop appropriate countermeasures.

In order to defend against passive attacks, traditional approaches like digital signatures, encryption, authentication, and access control are considered. Active attacks can be mitigated using intrusion detection systems and cooperation enforcement mechanisms to reduce selfish node behaviour. Encryption and authentication rely on asymmetric and symmetric cryptography, while data integrity and authentication are ensured using hash functions and digital signatures [7].

1.2 Need for Security in Ad Hoc Network

Despite the widespread use of mobile ad hoc networks, they still have vulnerabilities that require security measures [1, 6]. Intruders exploit these weaknesses to gain knowledge about network processes and launch attacks. The following are some contributing vulnerabilities in ad hoc networks:

i. Mobility: Each node can move freely, joining or leaving the network without informing other nodes, creating opportunities for intruders to enter and participate in operations.
ii. Open Wireless Medium: Communication between nodes occurs through the air, allowing intruders to eavesdrop on or intercept the communication.
iii. Resource Constraint: Nodes in ad hoc networks have limited resources like battery, processing power, and bandwidth, making them susceptible to resource depletion attacks.
iv. Dynamic Network Topology: Since nodes are highly mobile, the network topology changes frequently during communication, providing opportunities for intruders to infiltrate any path.
v. Scalability: Ad hoc networks can have a variable number of nodes, and intruders can exploit this lack of limitation on the number of participating nodes.
vi. Reliability: Wireless communication is limited to around 100 meters, requiring an intruder to be within this range to attack a specific node.

1.3 Routing

There are primarily three types of routing protocols in networks:

Proactive Protocols: Networks utilising proactive routing protocols have each node maintaining one or more tables representing the complete topology of the network. These tables are updated regularly to keep the routing information up-to-date from each node to every other node. While this ensures that routes are always available, it results in relatively high overhead on the network due to the frequent exchange of topology information between nodes.

Reactive Protocols: Unlike proactive routing protocols, reactive routing protocols do not initiate a route discovery process until a route is required. This leads to higher latency compared to proactive protocols but lower overhead. The route is only established when needed, reducing the amount of routing information that needs to be maintained and exchanged among nodes.

Hybrid Protocols: Hybrid protocols combine features of both proactive and reactive protocols. Each node maintains the topology information within its zone and the information regarding neighbouring zones. This results in proactive behaviour within a zone, allowing routes to each destination within the zone to be established instantaneously. However, a route discovery and maintenance procedure is required for destinations located in other zones.

The choice of routing protocol depends on the specific requirements and characteristics of the network. Proactive protocols are suitable for scenarios where routes must be readily available, and overhead is not a major concern. Reactive protocols are more appropriate for limited resources, and reducing overhead is a priority. Hybrid protocols strike a balance between the two and can be used to optimise routing efficiency in certain network configurations.

II. LITERATURE SURVEY

The literature survey provides information on various security schemes and proposals related to Mobile Ad hoc Networks (MANET). Some of the mentioned schemes are as follows: Kiran Afzal et al. [2]: This work focuses on the latest application of VANET called the Internet of Vehicles (IoV). They propose a VANET model involving Unmanned Aerial Vehicles (UAVs) for efficient data delivery and better performance. They compare traditional routing protocols with UAV-based protocols and demonstrate the superiority of their proposed drone-assisted routing protocols in terms of packet delivery ratio and throughput. Hussain et al. [9]: In this work, a Denial of Service (DoS) attack is applied in the AODV protocol in MANET. They propose an Intrusion Detection System (IDS) based on Support Vector Machine (SVM) to detect and prevent such attacks with high accuracy and minimal false positives. Jing-Wei Huang et al. [10]: This work introduces a trust-based multi-path AOMDV routing scheme called T-AOMDV, which uses soft encoding for secure message transmission. The proposed approach involves message encoding, routing, and decoding to ensure secure and reliable communication. Shreenath et al. [11]: The authors focus on enhancing the Secure Enhanced-On Demand Multicast Routing Protocol (EODMRP) to defend against flooding and blackhole attacks in MANETs. Their proposed mechanism protects against regional attacks. Sujatha et al. [12]: The authors present a Genetic algorithm-based Intrusion Detection System (IDS) for AODV in MANETs. They analyse the behaviours of nodes using genetic algorithms and identify attacks like region attacks based on features such as Request Forwarding Rate and Reply Receive Rate. Konate et al. [13]: This paper reviews various attacks and countermeasures in MANETs, especially focusing on denial of service (DoS) attacks. The authors discuss different types of DoS attacks, their operational methods, and the protocols to counter them. Gandhewar et al. [14]: The authors address the sinkhole attack problem in AODV protocol in MANETs and propose a mechanism for its detection and prevention. Sinkhole attacks aim to attract network traffic and degrade network

performance. P.K. Singh et al. [15]: This work proposes a solution to the black hole attack in the AODV routing protocol for MANETs. They use the promiscuous mode to detect malicious nodes (black holes) and propagate this information to all other nodes in the network.

III. SIMULATION TOOL

A network simulator is software or hardware that predicts the behaviour of a computer network in the absence of a physical network. Machines are typically modelled on the data network; traffic is generated in simulators, etc., and performance is evaluated. Users would then generally customise the simulator to match their testing requirements. Today's more widespread protocols and networks, such as WLAN, Wi-Max, TCP, WSN, cognitive radio, and so on, are frequently supported by simulators. The Network Simulator version 2, abbreviated as NS2, is an event-driven simulation tool for analysing the dynamic life of communication networks. NS2 can mimic wired and wireless network features and protocols (e.g., routing algorithms, TCP, and UDP). In general, NS2 allows users to describe network protocols and simulate their related behaviours. Since its inception in 1989, NS2 has become prominent in the networking research community due to its simplicity and compact architecture. Since then, several revolutions and alterations have highlighted the instrument's rising complexity, thanks to significant contributions from regional musicians. Among these are the University of California and the University of Cornell, which developed the Actual Network Simulator 1 on which NS is based. Since 1995, the Defense Advanced Research Projects Agency (DARPA) has funded NS development through its Interactive Internetwork Test Bed (VINT) initiative. The National Science Foundation (NSF) has joined the progress movement. Last but not least, the community group of scientists and engineers is always working to keep NS2 efficient and scalable Network Simulator-2 (ns-2) version 2.35.

IV. RESULT ANALYSIS

The primary issue in the field of MANET. A new research study in the Mobile ad hoc network (MANET) highlights numerous obstacles in the field. The study's primary goal is to observe several network performance measures, such as the recognised packet delivery ratio, enhancing routing performance. This measure represents the number of bits forwarded to higher tiers per second. It is measured in bits per second (bps) and considers the quantity of data packets transmitted per unit time.

(b) Now, PDR between both techniques should be calculated.

The packet delivery ratio (PDR) analysis is shown for the existing work using the AODV routing protocol and the proposed methodology using the modified AODV routing protocol in the PDR analysis graph. The PDR performance of the existing work is low, but the PDR performance of the proposed methodology is high. This shows how the recommended methodology improves PDR.

6.6.2 Delay Analysis

In the delay analysis, senders transmit a certain number of packets to the destination, and some packets are dropped in the network for various reasons. The number of packets received on time implies no data delay; however, packets may arrive late due to an attacker or other circumstances. Additionally, some senders may send data on time, but it reaches its destination late due to

network data delays. Suppose the delay analysis graph represents the delay analysis for the existing work using AODV routing and the suggested methodology utilising the modified AODV routing protocol. In that case, the delay performance of the existing work is high, indicating significant delays.

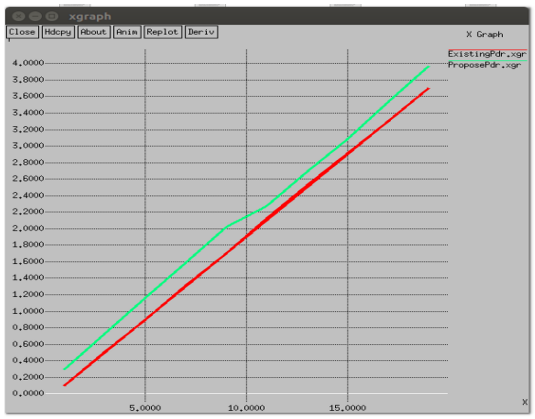

Figure 2: PDR Analysis between EM and PM Techniques

On the other hand, the delay performance of the proposed methodology is low, suggesting reduced delays. The recommended methodology appears to be effective in reducing delays in data transmission, making it a promising approach for improving overall network performance. Further investigation into the specific modifications made to the AODV routing protocol and their impact on delay reduction would be valuable for better understanding the benefits of the proposed methodology.

6.6.3 Energy Usage Analysis

Suppose the energy usage analysis graph represents the energy use analysis for the existing work using AODV routing and the proposed methodology using the modified AODV routing protocol. In that case, the energy used in the existing work is high, whereas the energy used in the proposed methodology is low. The number of routing packets transmitted in real-time from sender to receiver is a key factor in the recommended methodology.

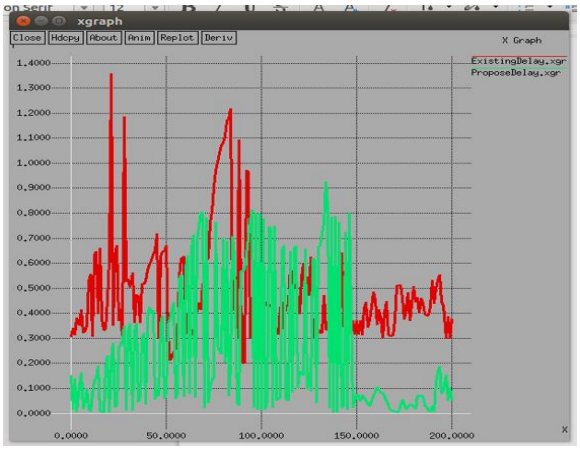

Figure 3: Delay Analysis between EM and PM Techniques

The proposed methodology demonstrates significant improvements in energy usage, making it an energy-efficient network. The network can optimise energy consumption using the modified AODV routing protocol while maintaining effective data transmission. Further investigation into the specific changes made to the AODV routing protocol and their impact on energy efficiency would provide valuable insights into the benefits of the proposed methodology.

Overall, the energy-efficient characteristics of the proposed methodology make it a promising approach for enhancing the sustainability and performance of communication networks.

6.6.3 Energy Usage Analysis

Suppose the energy usage analysis graph represents the energy use analysis for the existing work using AODV routing and the proposed methodology using the modified AODV routing protocol. In that case, the energy used in the existing work is high, whereas the energy used in the proposed methodology is low. The number of

routing packets transmitted in real-time from sender to receiver is a key factor in the recommended methodology.

The proposed methodology demonstrates significant improvements in energy usage, making it an energy-efficient network. The network can optimise energy consumption using the modified AODV routing protocol while maintaining effective data transmission. The reduction in energy consumption is attributed to the optimised routing mechanisms and better utilisation of network resources.

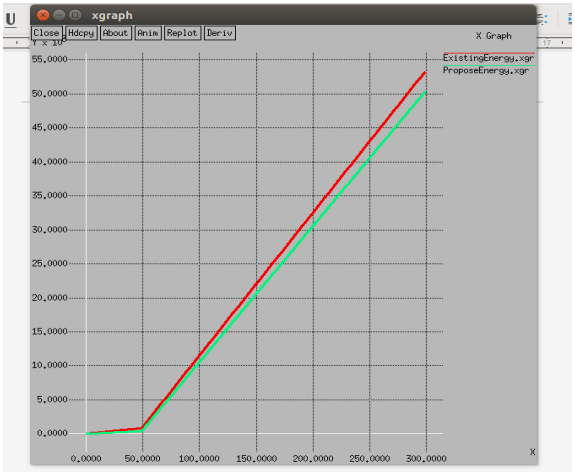

Figure 4: Energy Used Analysis between EM and PM Techniques

The graph in Figure 4 depicts the energy usage comparison between the existing work (EM) using the traditional AODV routing protocol and the proposed methodology (PM) employing the modified AODV routing protocol. It visually demonstrates the lower energy consumption of the proposed methodology compared to the existing work. The proposed energy-efficient network is eco-friendly, as it helps conserve energy, prolong the network's lifespan, and reduce the environmental impact. Additionally, the improved energy usage contributes to better network performance and reliability, making the proposed methodology a promising choice for future communication network designs.

CONCLUSION

In this study, we have explored the application of an energy-optimised and energy-efficient routing protocol for Mobile Ad Hoc Networks (MANETs). The Internet of Cars application can be significantly improved by adopting the proposed technique, which involves the modified AODV protocol. The proposed approach extends the network's lifespan and discovers the best path from the source to the destination.

The existing work utilising the AODV protocol has shown a lower packet delivery ratio, increased delay, and higher energy consumption. In contrast, the proposed approach using the modified AODV protocol (MAODV) demonstrates a higher packet delivery ratio, reduced delay, and lower energy usage. These improvements make MAODV a more efficient and viable option for MANET applications.

Mobile Ad Hoc Networks (MANETs) possess distinct characteristics that set them apart from other wireless or wired networks. The absence of a fixed infrastructure allows mobile nodes to move freely, leading to frequent topology changes and link failures, which can affect route stability. Moreover, nodes in MANETs have limited resources such as electricity, bandwidth, and computational capacity, and the absence of centralised trust introduces additional challenges.

The Internet of Vehicles (IoV) represents a new type of Vehicular Ad Hoc Network (VANET) that combines the Internet and the Internet of Things (IoT). Due to vehicles' dynamic and mobile nature on the road and the increased risk of packet loss, mobile ad-hoc networks have become increasingly

important in the current era. Various strategies have been proposed to improve the overall efficiency of IoT, focusing on metrics such as packet delivery ratio, end-to-end delay, packet drop ratio, and energy consumption.

The proposed methodology using the modified AODV protocol (MAODV) addresses these challenges and provides an energy-efficient routing protocol. It has been shown to enhance the packet delivery ratio, optimise energy usage, and reduce delays. The performance evaluation of the proposed methodology, which combines the best aspects of AODV, has shown promising results compared to existing work.

In conclusion, the modified-AODV protocol (MAODV) presents an effective and energy-efficient solution for mobile ad-hoc networks and the Internet of Vehicles. It holds the potential to significantly enhance the overall performance and reliability of communication networks in dynamic and resource-constrained environments.

References:

[1]. J. Wang, X. Xiao, and P. Lu, "A survey of vehicular ad hoc network routing protocols," Journal of Electrical and Electronic Engineering, vol. 7, no. 2, pp. 46–50, 2019.

[2]. Afzal, K., Tariq, R., Aadil, F., Iqbal, Z., Ali, N., & Sajid, M., "An optimised and efficient routing protocol application for IoV. Mathematical Problems in Engineering, 2021.

[3]. Oscar F. Gonzalez, Godwin Ansa, Michael Howarth, and George Pavlou. "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks," Journal of Internet Engineering, Vol. - 2, no.1, 2008.

[4]. Sunil Taneja and Ashwani Kush, "A Survey of Routing Protocols in Mobile Ad Hoc Networks," International Journal of Innovation, Management, and Technology, Vol. 1, No. 3, August 2010.

[5]. Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks," Journal of Computing, Volume 3, Issue 1, January 2011.

[6]. K.P.Manikandan, Dr. R.Satyaprasad, Dr. K.Rajasekhararao, "A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks," International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011.

[7]. . Yi and R. Kravets, "Composite Key Management for Ad Hoc Networks." Proceedings of the 1st Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'04), pp. 52-61, 2004.

[8]. K. Sivakumar, Dr. G. Selvaraj, "Overview of Various Attacks in MANET and Countermeasures for Attacks", International Journal of Computer Science and Management Research Vol 2 Issue 1 January 2013.

[9]. Husain, Shahnawaz, Gupta S.C., Chand Mukesh "Denial of Service Attack in AODV & Friend Features Extraction to Design Detection Engine for the Intrusion Detection System in Mobile Adhoc Network," International Conference on Computer & Communication Technology (ICCCT-2011), pp. 292-297, 2011.

[10]. Jing-Wei Huang, Isaac Woungang, Han-Chieh Chao, Mohammad S. Obaidat, Ting-Yun Chi, Sanjay K. Dhurandher, "Multi-

Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks," Proceedings of IEEE Global Telecommunications Conference (GLOBECOM 2011), pp. 1-5, 2011.

[11]. Dr. N. Sreenath, A. Amuthan, & P. Selvigirija "Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs," International Conference on Computer Communication and Informatics (ICCCI - 2012), pp. 1-7, 2012.

[12]. K. S. Sujatha, Vydeki Dharmar, R. S. Bhuvaneswaran "Design of Genetic Algorithm-based IDS for MANET," International Conference on Recent Trends in Information Technology (ICRTIT), pp. 28-33, 2012.

[13]. Dr Karim KONATE, GAYE Abdourahime "Attacks Analysis in mobile ad hoc networks: Modeling and Simulation," 2011 Second International Conference on Intelligent Systems, Modelling and Simulation, pp. 367–372, 2011.

[14]. Gandhewar, N., Patel, R. "Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network," Fourth International Conference on Computational Intelligence and Communication Networks (CICN), pp. 714–718, 2012.

[15]. P.K Singh, G. Sharma, "An Efficient Prevention of the Black Hole Problem in AODV Routing Protocol in MANET," IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 902–906, 2012.

[16]. R. A. Nazib and S. Moh, "Routing protocols for unmanned aerial Vehicle-Aided vehicular Ad Hoc networks: a survey," IEEE Access, vol. 8, pp. 77535–77560, 2020.

[17]. N. Lin, L. Fu, L. Zhao, G. Min, A. Al-Dubai, and H. Gacanin, "A novel multimodal collaborative drone-assisted VANET networking model," IEEE Transactions on Wireless Communications, vol. 19, no. 7, pp. 4919–4933, 2020.

[18]. M. Dixit, R. Kumar, and A. K. Sagar, "VANET: architectures, research issues, routing protocols, and its applications," in Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA), pp. 555–561, IEEE, Greater Noida, India, April 2016.

[19]. Hinds, Alex, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi. "A review of routing protocols for mobile ad-hoc networks (manet)." International Journal of Information and education technology 3, no. 1: 1, 2013.

[20]. Saudi, Nur Amirah Mohd, Mohamad Asrol Arshad, Alya Geogiana Buja, Ahmad Firdaus Ahmad Fadzil, and Raihana Md Saidi. "Mobile ad-hoc network (MANET) routing protocols: A performance assessment." In Proceedings of the Third International Conference on Computing, Mathematics, and Statistics (iCMS2017) Transcending Boundaries, Embracing Multidisciplinary Diversities, pp. 53-59. Springer Singapore, 2019.

[21]. Corson, Scott, and Joseph Macker. Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations. No. rfc2501. 1999.

[22]. Ramphull, Dinesh, Avinash Mungur, Sheeba Armoogum, and Sameerchand Pudaruth. "A review of mobile ad hoc NETwork

(MANET) Protocols and their Applications." In 2021 5th international conference on intelligent computing and control systems (ICICCS), pp. 204-211. IEEE, 2021.