AODV-based Defense Mechanism for Mitigating Blackhole Attacks in MANET

Idriss Moumen[1], Najat Rafalia[1], Jaafar abouchabaka[1]and Youssef Chatoui[1]

[1]Laboratory of Research in Informatics, Faculty of Sciences, Ibn Tofail University, Kenitra, Morocco

Abstract. Mobile Ad hoc Networks (MANETs) are decentralized and self-configuring networks composed of mobile devices that communicate without a fixed infrastructure. However, the open nature of MANETs makes them vulnerable to various security threats, including blackhole attacks, where malicious nodes attract and discard network traffic without forwarding it to its intended destination. Mitigating blackhole attacks is crucial to ensure the reliability and security of communication in MANETs. This paper focuses on the development and evaluation of AODV (Ad hoc On-Demand Distance Vector)-based defence mechanisms for effectively mitigating blackhole attacks in MANETs, while simultaneously addressing energy efficiency and environmental sustainability. AODV is a widely used routing protocol in MANETs due to its on-demand nature and low overhead. However, it lacks built-in security mechanisms, making it susceptible to attacks. We incorporate energy-aware route selection, solar-powered routing, collaborative energy sharing, energy-efficient intrusion detection, green routing optimization, and energy harvesting from environmental sources. By considering energy consumption and environmental factors in the route selection process, our defense mechanism not only enhances the security of the network but also contributes to energy conservation and reduced environmental impact. To evaluate the effectiveness of the proposed defence mechanisms, extensive simulations and performance analyses are conducted using network simulation tools. Through simulation-based evaluations, we demonstrate the effectiveness of our approach in achieving robust blackhole attack mitigation while extending the network's lifetime and minimizing its carbon footprint. Our research offers valuable insights into the development of energy-efficient and environmentally sustainable solutions for securing MANETs in the face of evolving security threats.

Index Terms— Mobile Ad hoc Networks, Blackhole attacks, Ad hoc On-Demand Distance Vector, Energy efficiency, Environmental sustainability, Routing protocol, Security threats, Simulation analysis.

1. Introduction

Mobile Ad-Hoc Networks (MANETs) are known for their dynamic topology, absence of centralized management, and cooperative nature [1]. These unique characteristics make MANETs susceptible to various security attacks, including blackhole attacks [2-5], where malicious nodes selectively drop packets, leading to significant disruptions in communication. Ensuring the security of MANETs is crucial for maintaining the availability, confidentiality, and integrity of network services and data [6, 7]. Traditional

security solutions designed for wired networks are not directly applicable to MANETs due to the absence of infrastructure, lack of trust relationships among nodes, and the dynamic nature of the network. Therefore, specialized defense mechanisms are required to mitigate security threats and protect MANETs from blackhole attacks. This paper focuses on AODV-based defense mechanisms for mitigating blackhole attacks [4-6] in MANETs. The Ad-hoc On-Demand Distance Vector (AODV) routing protocol [5, 8, 9] is a widely used on-demand routing protocol in MANETs. It dynamically establishes routes between nodes based on demand, making it susceptible to attacks like blackhole attacks. The vulnerability of MANETs stems from several factors, including the lack of centralized management [10], scalability challenges, cooperativeness assumptions [11], the presence of adversaries within the network, and the absence of a predefined secure boundary [12]. These factors create a challenging environment for ensuring the security of MANETs and highlight the need for robust defense mechanisms [13, 14]. Various attack types pose a significant threat to MANETs, including the wormhole attack, gray hole attack [15], jellyfish attack [16], flooding attack, modification attack, impersonation attack, rushing attack, and blackhole attack [6, 15, 17]. Each attack exploits different vulnerabilities in the network, compromising its functionality and disrupting communication [10, 18]. To counter these attacks, several defense mechanisms have been proposed. For example, the Packet Leash mechanism can prevent wormhole attacks by limiting the maximum transmission distance of packets [19]. Blacklisting malicious nodes can help detect and remove gray hole nodes, while the JAM (Jellyfish Attack Mitigation) mechanism can mitigate the impact of jellyfish attacks [16]. Secure routing protocols, such as Authenticated Routing for Ad hoc Networks (ARAN) and the Secure Efficient Adhoc Distance Vector (SEAD) protocol [20], provide authentication, non-repudiation, and tamper-proofing capabilities to defend against modification and impersonation attacks. Additionally, generic mechanisms such as secure Neighbor Detection and randomized ROUTE REQUEST forwarding can be employed to mitigate rushing attacks. This paper aims to enhance the security of MANETs while addressing energy efficiency and environmental sustainability concerns [21]. By incorporating energy-aware route selection techniques, the mechanism prioritizes paths that minimize energy consumption, optimizing the utilization of limited energy resources in the network. This approach extends the lifetime of the network and reduces the need for frequent battery replacements, leading to improved energy efficiency. Furthermore, the defense mechanism integrates energy-efficient intrusion detection techniques, minimizing the energy consumption associated with continuous monitoring of network traffic[22, 23]. Techniques such as selective packet sampling and adaptive monitoring intelligently manage the monitoring intensity, ensuring effective intrusion detection while conserving energy. This paper aims to explore the effectiveness of AODV-based defense mechanisms in mitigating blackhole attacks in MANETs. It will examine the advantages and limitations of these mechanisms and provide insights into their applicability and performance. The evaluation will consider factors such as packet delivery ratio, end-to-end delays, network scalability, and resilience to attacks. In conclusion, securing MANETs against blackhole attacks and other security threats is a challenging task due to the unique characteristics of these networks. AODV-based defense mechanisms offer promising solutions to mitigate blackhole attacks in MANETs. By understanding the vulnerabilities and employing effective defense mechanisms, the security and reliability of MANETs can be significantly enhanced, ensuring the seamless operation of communication in dynamic and resource-constrained environments.

2. Methodology and Implementation

The performance measures of a Mobile Ad hoc Network (MANET), such as throughput, packet delivery ratio, and packet loss, are assessed under different scenarios: absence of malicious nodes, presence of a single malicious node resulting in a single blackhole, and presence of multiple malicious nodes leading to multiple blackhole attacks. The metrics are compared across these scenarios, and graphs are generated to illustrate the findings. The network's behavior is visualized using the Network Animator (NAM) tool, and the number of packets consumed by the blackholes is presented. To counter blackhole attacks from both single and multiple blackhole nodes, a solution is proposed employing the Fake routing protocol. Simulation results demonstrate that the suggested protocol enhances performance by improving packet delivery, throughput, and packet loss even in the presence of blackholes. Additionally, the proposed protocol aids in the detection of blackholes.

2.1. Overview of Blackhole Attacks and their Impact

A blackhole attack in MANETs occurs when a malicious node falsely claims to have the best route to a destination. It attracts traffic but discards packets instead of forwarding them, disrupting communication and causing packet loss. Multiple blackhole nodes may collaborate for a more severe attack. Detecting and mitigating blackholes is vital for network integrity.

Black hole attacks can have significant consequences, resulting in the following impacts:

2.1.1. Decreased packet delivery ratio

Packet delivery ratio (PDR) is a crucial performance metric in wireless networks, including MANETs, as it quantifies the ratio of successfully delivered packets to the total number of packets sent. A lower packet delivery ratio indicates a higher number of lost or undelivered packets, reflecting the effectiveness of the routing protocols and network applications.

When a blackhole attack occurs, the packet delivery ratio is adversely affected. The presence of malicious nodes that attract and discard network traffic without forwarding it to the intended destination causes a gradual increase in packet loss. This phenomenon leads to a reduced packet delivery ratio, as a higher percentage of packets fail to reach their intended recipients.

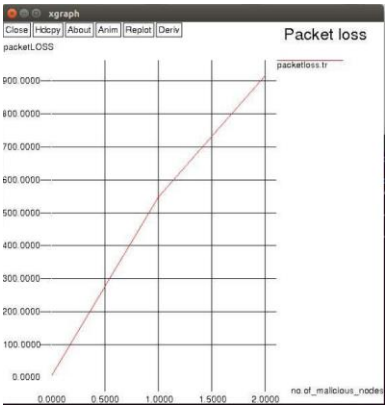

Figure 1: Packet Loss Variation with Increasing Malicious Nodes

The impact of blackhole attacks on the packet delivery ratio can be visualized in Figure 1, which illustrates the variation in packet loss with an increasing number of malicious nodes. Initially, when the network is free from malicious nodes, the packet loss remains minimal, approaching zero. However, as a single malicious node enters the network, the packet loss starts to increase gradually. The number of lost packets rises, reaching approximately 500 packets.

As additional malicious nodes are introduced into the network, the packet loss escalates rapidly. With the presence of two malicious nodes, the packet loss value reaches 900, indicating a significant deterioration in the packet delivery ratio. This trend emphasizes the detrimental impact of blackhole attacks on the reliable and efficient delivery of packets within MANETs.

2.1.2.Increased end-to-end delay

End-to-end delay (E2E delay) in a MANET refers to the duration taken by a packet to travel from the source node to the destination node, passing through multiple intermediate nodes in the network. In the presence of a blackhole attack, the end-to-end delay experiences a noticeable rise due to the disruption caused by the malicious node.

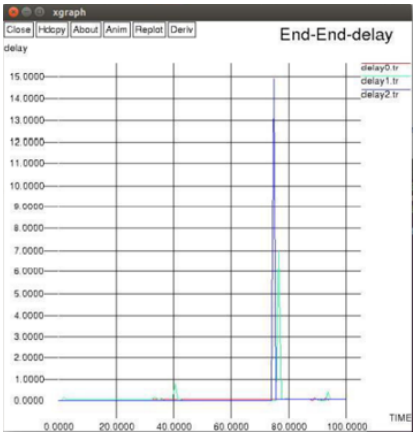

Figure 2: Variation in end-to-end delay caused by black hole nodes

Figure 2 depicts the variation in end-to-end delay caused by the presence of black hole nodes. The graph showcases the delay experienced by messages within the network over time. The red line graph represents the end-to-end delay when no malicious nodes are present in the network, indicating minimal delay based on the graph. However, when a single malicious node exists in the network, as depicted by the green line graph, there is an observable delay in packet transmission. The presence of the black hole node causes packets to take longer routes, resulting in increased end-to-end delay.

Furthermore, with the addition of two malicious nodes, as illustrated by the blue line graph, the delay in network communication significantly escalates. The extended routing paths caused by the black hole nodes lead to substantially high delays in packet delivery. This delay in reaching the intended destination hampers the overall efficiency and responsiveness of the network.

The increased end-to-end delay resulting from blackhole attacks emphasizes the need for effective defense mechanisms to mitigate such attacks in MANETs. By detecting and mitigating the presence of black hole nodes, it becomes possible to reduce the routing path lengths and minimize the delay experienced by packets. This, in turn, enhances the overall performance and responsiveness of the network, ensuring timely and efficient communication within MANETs.

2.1.3.Reduced throughput

The presence of a black hole node within a Mobile Ad-Hoc Network (MANET) can lead to a significant reduction in the network's overall throughput. This decline occurs as packets are lost before they can be successfully transmitted, resulting in decreased efficiency and slower data transfer rates. Throughput in a MANET refers to the quantity of data that can be effectively transmitted across the network within a given time frame. It serves as a critical performance measure for assessing the capacity and efficiency of wireless networks.

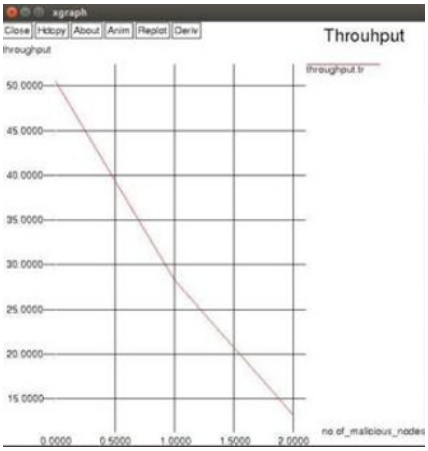

Figure 3: impact of black hole nodes on the network's throughput

Figure 3 illustrates the impact of malicious nodes, particularly black hole nodes, on the network's throughput. Throughput is inversely related to the time it takes for a packet to reach its destination. As the time increases, the throughput decreases accordingly. In the absence of any malicious nodes, the network's throughput is significantly high, reaching approximately 50. However, with the presence of a single malicious node, the throughput experiences a considerable decline, dropping to 28. Furthermore, when two malicious nodes are present, the available throughput decreases further, falling below 15. This substantial reduction in throughput highlights the adverse impact of blackhole attacks on the network's data transfer capabilities.

2.2. Implementation of AODV-Based Security Mechanism

The proposed AODV-based security mechanism aims to detect and mitigate multiple blackhole nodes in MANETs. It utilizes the following steps:

1. Fake RREQ Packet Broadcast: The source node initiates the detection process by broadcasting a fake Route REQuest (RREQ) packet. This packet includes the source node's own source sequence number and address.
2. Sequence Number Comparison: Legitimate nodes receiving the fake RREQ packet compare the source sequence number of the packet with the stored sequence number of the source node. If the received sequence number is more recent, indicating that it is distinct from intermediate nodes, they do not reply with a Route REPly (RREP) packet.
3. Malicious Node Response: However, blackhole nodes within the network reply to the fake RREQ packet with an RREP packet. These malicious nodes claim to have the highest source sequence number and shortest path to the destination.
4. Blackhole Node Identification: The source node identifies the presence of blackhole nodes by analyzing the received RREP packets. It recognizes that the blackhole nodes have responded with false information, indicating their malicious behavior.
5. ALARM Packet Broadcast: To alert other nodes in the network about the detected blackhole nodes, the source node sends an ALARM packet. This packet contains information listing the identified blackhole nodes.

3. Experimental Setup and Evaluation

To evaluate the effectiveness of the AODV-based security mechanism, simulations are conducted using NetSim2. The simulated MANET consists of a variable number of nodes ranging from 50 to 100, communicating wirelessly. The network includes intentionally added malicious nodes, ranging from 1 to 4, to assess their impact on packet loss and throughput. Different attack strategies, including blackhole attacks, are employed to disrupt the network.

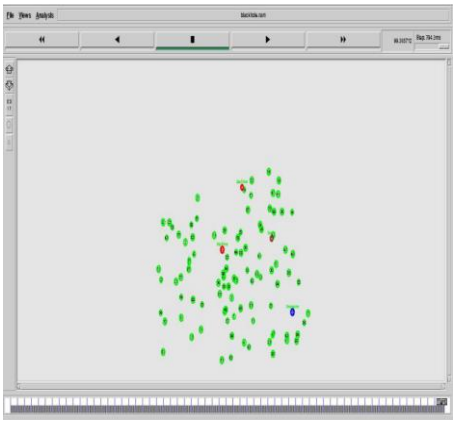

Figure 4: Visualization of Mobile Ad hoc Network (MANET) with Malicious Nodes

The simulation was conducted using a network of 100 mobile nodes. The results are depicted in Figure 5, where various node types are represented by different colors. In the simulation, normal nodes, which do not engage in malicious activities, are represented by the color green. These nodes maintain regular communication within the network and follow the established routing paths. Malicious nodes, responsible for initiating blackhole attacks, are marked in red. These nodes intentionally disrupt network communication by attracting and discarding network traffic without forwarding it to the intended destination. Their presence poses a significant threat to the reliability and security of the MANET. To differentiate the source node and destination nodes from the rest, they are colored in blue. These nodes play a crucial role in initiating and receiving communication in the network.

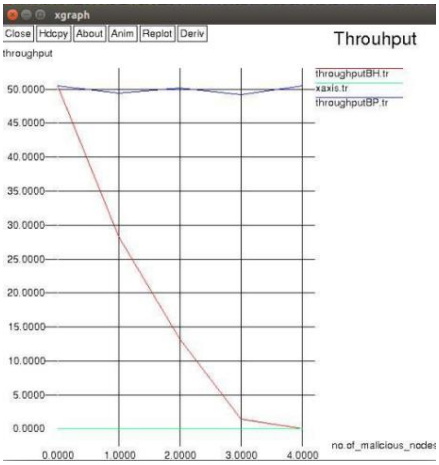

Figure 5: Effectiveness of AODV-based mechanism: Throughput Analysis

Figure 4 analyzes the impact of the AODV-based mechanism on network throughput during a blackhole attack. The graph demonstrates the relationship between throughput and the presence or absence of preventive measures. In the presence of a blackhole attack (red line), there is a decrease in throughput. However, when the AODV-based mechanism is deployed (blue line), the throughput improves compared to the scenario without the mechanism. This improvement is due to the mechanism's ability to detect and mitigate the blackhole attack, resulting in a more reliable and efficient data transmission process.

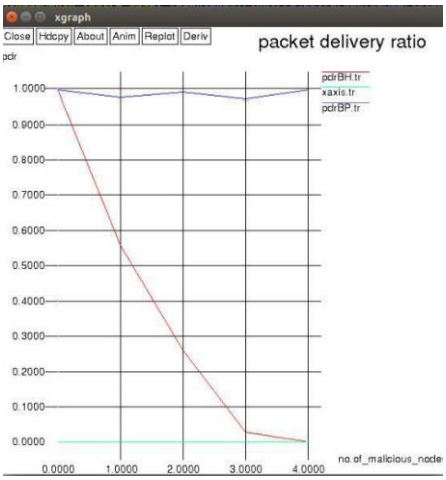

Figure 6: Effectiveness of AODV-based mechanism Packet delivery ratio Analysis

Figure 5 evaluates the effectiveness of the AODV-based mechanism in maintaining packet delivery ratio during a blackhole attack. The graph shows that the presence of the attack leads to a decline in the packet delivery ratio (red line), indicating decreased reliability of data transmission. However, implementing the AODV-based mechanism improves the packet delivery ratio (blue line) by detecting and mitigating the attack, preventing packet loss and enhancing successful delivery.

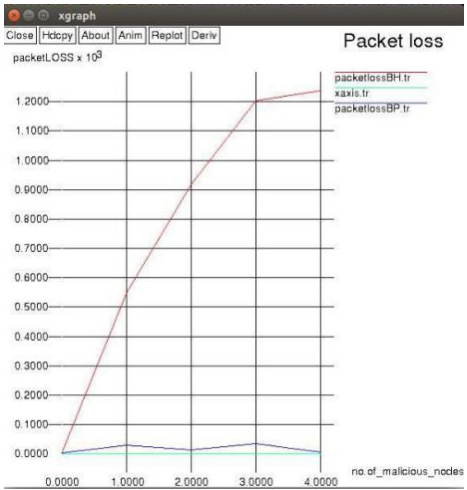

Figure 7: Analysis of Packet Loss in AODV-based Mechanism

Figure 6 examines the impact of the AODV-based mechanism on packet loss during a blackhole attack. The graph shows that the attack leads to increased packet loss (red line), indicating compromised data transmission reliability. However, implementing preventive measures significantly reduces packet loss (blue line), ensuring minimal loss of packets. This highlights the effectiveness of the AODV-based mechanism in mitigating packet loss and improving the overall integrity of data transmission in the network.

Table 1. Impact of Blackhole Attacks on Packet Loss, Packet Delivery Ratio, and Throughput with and without AODV-based Mechanism

		Blackhole	**AODV-based mechanism**
Packet Loss	1 Malicious node	550	2
	2 Malicious nodes	910	4
Packet delivery ratio	1 Malicious node	55%	98%
	2 Malicious nodes	25%	99%
Throuput	1 Malicious node	27	50
	2 Malicious nodes	13	50

Table 1 provides a comprehensive comparison of the impact of blackhole attacks on packet loss, packet delivery ratio, and throughput with and without the implementation of the AODV-based mechanism. In the presence of 1 malicious node, the packet loss reaches 550 packets without the mechanism, while with the AODV-based mechanism, the packet loss is significantly reduced to only 2 packets. Similarly, the packet delivery ratio improves from 55% without the mechanism to 98% with the mechanism. When there are 2 malicious nodes in the network, the packet loss escalates to 910 packets without the mechanism, but with the AODV-based mechanism, it is reduced to just 4 packets. The packet delivery ratio also shows a substantial improvement, increasing from 25% without the mechanism to 99% with the mechanism.

Furthermore, the throughput remains consistent at 27 units with 1 malicious node, regardless of the mechanism. However, in the presence of 2 malicious nodes, the throughput drops to 13 units without the mechanism, but with the AODV-based mechanism, it is maintained at 50 units. These results clearly demonstrate the effectiveness of the AODV-based mechanism in mitigating the impact of blackhole attacks. By significantly reducing packet loss, improving packet delivery ratio, and maintaining a consistent throughput, the mechanism ensures more reliable and efficient network communication in the face of malicious nodes.

4. Conclusion

Defense mechanisms based on the AODV routing protocol have been proposed to address security vulnerabilities in Mobile Ad-Hoc Networks (MANETs). These mechanisms prioritize energy-efficient route selection by considering the energy levels of nodes, optimizing the utilization of limited energy resources. They also incorporate energy-efficient intrusion detection techniques, minimizing energy consumption while effectively monitoring network traffic. Additionally, these mechanisms employ green routing optimization, considering environmental factors during route selection to reduce the

network's ecological impact. Overall, these defense mechanisms improve network security, enhance energy efficiency, and contribute to the environmental sustainability of MANETs in the face of evolving security threats.

5. References

[1] N. Goyal, A. J. I. J. o. C. T. Gaba, and Applications, "A new approach of location aided routing protocol using minimum bandwidth in mobile ad-hoc network," vol. 4, no. 4, p. 653, 2013.

[2] A. Vinay, K. Hansitha, N. Jayanth, and S. P. Sreeja, "PREVENTION OF BLACKHOLE ATTACK IN MANET'S."

[3] A. M. Eltahlawy, H. K. Aslan, E. G. Abdallah, M. S. Elsayed, A. D. Jurcut, and M. A. J. E. Azer, "A Survey on Parameters Affecting MANET Performance," vol. 12, no. 9, p. 1956, 2023.

[4] R. Gotti, A. Polagani, G. S. L. Posina, S. Veerapaneni, and T. Prasanth, "Detection and Analysis of Single Blackhole Node with TCP Connection in MANETs using Machine Learning Algorithms," in 2023 International Conference on Inventive Computation Technologies (ICICT), 2023, pp. 1704-1710: IEEE

[5] S. Shafi, S. Mounika, and S. J. P. C. S. Velliangiri, "Machine Learning and Trust Based AODV Routing Protocol to Mitigate Flooding and Blackhole Attacks in MANET," vol. 218, pp. 2309-2318, 2023.

[6] S. Lu, L. Li, K.-Y. Lam, and L. Jia, "SAODV: a MANET routing protocol that can withstand black hole attack," in 2009 international conference on computational intelligence and security, 2009, vol. 2, pp. 421-425: IEEE

[7] P. Kamboj, N. J. I. J. o. E. R. i. M. Goyal, and Technology, "Survey of various keys management techniques in MANET," vol. 4, no. 6, 2015.

[8] D. G. Fragkoulis, N. D. Kouvakas, F. N. Koumboulis, N. I. J. A.-I. J. o. E. Georgiou, and Communications, "Modelling and Modular Supervisory Control for the AODV Routing Protocol," p. 154761, 2023.

[9] B. Patel and R. Patel, "Study of Denial of Service Attack On AODV Routing Protocol in Mobile Ad-hoc Network," in 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), 2023, pp. 66-77: IEEE

[10] N. Shanthi, L. Ganesan, K. J. J. o. T. Ramar, and A. I. Technology, "Study of different attacks on multicast mobile ad hoc network," vol. 6, 2009.

[11] E. M. Royer and C.-K. J. I. p. c. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," vol. 6, no. 2, pp. 46-55, 1999.

[12] D. B. Roy, R. Chaki, and N. J. a. p. a. Chaki, "A new cluster-based wormhole intrusion detection algorithm for mobile ad-hoc networks," 2010.

[13] S. Vijayalakshmi, S. Bose, G. Logeswari, T. J. C. S. Anitha, and Applications, "Hybrid defense mechanism against malicious packet dropping attack for MANET using game theory," vol. 1, p. 100011, 2023.

[14] T. Bhatia and A. J. I. J. Verma, "Security issues in MANET: a survey on attacks and defense mechanisms," vol. 3, no. 6, 2013.

[15] S. Banerjee, "Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks," in proceedings of the world congress on engineering and computer science, 2008, vol. 2008

[16] F. Samad, Q. Abu Ahmed, A. Shaikh, and A. Aziz, "Jam: mitigating jellyfish attacks in wireless ad hoc networks," in Emerging Trends and Applications in Information Communication Technologies: Second International Multi Topic Conference, IMTIC 2012, Jamshoro, Pakistan, March 28-30, 2012. Proceedings 2, 2012, pp. 432-444: Springer

[17] T. S. Vamsi, E. P. Kumar, T. J. I. J. o. E. R. Sruthi, and Applications, "Performance Analysis of Aodv Routing Protocol in Manet under Blackhole Attack," vol. 9, no. 5, pp. 58-63, 2019.

[18] K. Sivakumar, D. G. J. I. J. o. C. S. Selvaraj, and M. Research, "Overview of various attacks in manet and countermeasures for attacks," vol. 2, no. 1, 2013.

[19] A. Perrig and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks," in IEEE INFOCOM, 2003, pp. 1976-1986

[20] Y.-C. Hu, D. B. Johnson, and A. J. A. h. n. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," vol. 1, no. 1, pp. 175-192, 2003.

[21] K. Saravanan, S. Anthoniraj, S. Kumarganesh, T. S. Kumar, and K. M. Sagayam, "WMLP: Web-based Multi-Layer protocols for Emergency Data Transmission in Mobile Ad Hoc Network," in E3S Web of Conferences, 2021, vol. 297, p. 01065: EDP Sciences

[22] M. A. Hidayat, A. Sofwan, and A. B. Prasetijo, "Gaussian Prediction Method to Enhance Energy Efficient in Energy Aware AODV," in E3S Web of Conferences, 2019, vol. 125, p. 23005: EDP Sciences

[23] I. P. Tummala and S. B. Ramya, "Dynamic Address Routing for Adhoc & Mesh Networks using MANETs," in E3S Web of Conferences, 2021, vol. 309, p. 01188: EDP Sciences