Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 1, No.1, January : 2025

AVOIDANCE AND DISCOVERY OF MITM ATTACKS ON AOMDV ROUTING PROTOCOLS

Dr.V. B. Kute, Professor, Department of Computer Science & Engineering, P R Pote Patil College of Engineering & Management, Amravati, Maharashtra, India
Prof. M. K. Nichat, Assistant Professor, Department of Computer Science & Engineering, P R Pote Patil College of Engineering & Management, Amravati, Maharashtra, India
Prof. S. S. Sagane, Assistant Professor, Department of Computer Science & Engineering, P R Pote Patil College of Engineering & Management, Amravati, Maharashtra, India
Prof. P. G. Nemade, Assistant Professor, Department of Computer Science & Engineering, P R Pote Patil College of Engineering & Management, Amravati, Maharashtra, India

ABSTRACT:
The Ad Hoc On-Demand Multipath Distance Vector (AOMDV) routing protocol, which is crucial for the effective functioning of various mobile ad hoc networks (MANETs), encounters significant security challenges, particularly from Man-in-the-Middle (MitM) attacks. This article presents a comprehensive examination and innovative approaches for the prevention and identification of MitM attacks within AOMDV-enabled networks. Initially, the article explores the operational principles of AOMDV, highlighting its susceptibility to MitM attacks as a result of the absence of an inherent security framework. The proposition of utilizing threshold calculations for the detection of malicious nodes during Route discovery phases of AOMDV is put forth.
We assess the efficacy of our proposed solutions by conducting extensive simulations, wherein AOMDV's Performance is compared under attack scenarios with and without the inclusion of our security enhancements. The outcomes of these simulations indicate a significant enhancement in the resilience of AOMDV against MitM attacks, as demonstrated by metrics such as throughput, packet delivery ratio, average delay, and packet delivery ratio. Furthermore, our methodology ensures that the efficiency and scalability of the protocol are maintained, which is of utmost importance in the context of MANET applications.
This research makes a valuable contribution to the field by addressing a crucial security gap that exists in the AOMDV protocol.
Keywords: MANET, Ad-Hoc Networks, AOMDV, MitM attack, Security in MANET, MANET Security

INTRODUCTION:

The wireless Mobile Ad Hoc Networks (MANETs) have gained widespread adoption in various applications, such as military communications, disaster management, and day-to-day use [1][2]. Unlike wired networks, MANETs present additional challenges due to their on-the-fly network formation, which enables communication between heterogeneous nodes without fixed infrastructures and centralized control [3]. Reactive routing protocols are used to discover routes when needed, and multi-path routing protocols in MANETs significantly reduce the frequency of route discovery than single path routing protocols. AOMDV is a reactive and multi-path routing protocol specifically designed for MANETs, aiming to establish and maintain efficient communication paths between nodes [4][5]. However, the decentralized and dynamic nature of ad hoc networks makes them vulnerable to various security threats, with MitM (MitM) attacks being particularly concerning [4][5].
MitM attacks disrupt communication in MANETs by intercepting and potentially manipulating communication between two parties, compromising data integrity, allowing unauthorized access to the network, and causing disruptions in network functionality. The use of AOMDV, which discovers

multiple routes between source and destination, further exacerbates the potential impact of MitM attacks on the route discovery process, posing a severe threat to communication integrity and reliability. Unauthorized entities can exploit these vulnerabilities to inject themselves into the route discovery and maintenance processes, disrupting communication between legitimate nodes [5][6]

MOTIVATION:

The need for robust security mechanisms becomes of utmost importance as the reliance on wireless ad hoc networks continues to grow in various sectors. The consequences of a compromised AOMDV routing protocol can be severe, including data diversion, unauthorized access, and network degradation. Therefore, it is crucial to address the vulnerabilities in AOMDV and develop effective prevention and detection mechanisms to safeguard against MitM attacks.

The key objectives in this work are as follows:

To examine and investigate the vulnerabilities of the AOMDV routing protocol that render it susceptible to MitM attacks.

- To suggest avoidance strategies that can strengthen AOMDV against potential threats, ensuring the secure establishment and maintenance of communication paths.
- To develop and evaluate detection mechanisms capable of identifying and mitigating MitM attacks in real-time within the AOMDV framework.

This research paper is structured into several sections to comprehensively address the prevention and detection of MitM attacks on the AOMDV routing protocol. The subsequent sections will thoroughly review the existing literature on AOMDV and MitM attacks. The paper will then propose prevention strategies, discuss the vulnerabilities in AOMDV, and examine the development and evaluation of detection mechanisms. Finally, the research findings will be summarized, and potential avenues for future work in securing AOMDV against evolving security threats will be outlined.

LITERATURE REVIEW :

In [7] Sadoon Hussain et al. presented a solution for ensuring end-to-end security in flying ad hoc networks using a column mobility model, inspired by ant behavior. To achieve this, they employed an ant colony optimization-based routing technique to establish secure communication standards within the network. The authors evaluated the performance of their approach, AntHocNet, by analyzing parameters such as throughput, network utilization, and packet drop. Jia, X., Huang, D., & Qin, N. (2024) in [8], proposed a machine learning model for security and routing management in MANETs. Here the network security has been monitored. The authors apply trust-based multi-tier honey pot analysis. The analysis has been with stacked reinforcement learning.

In their paper Khalfaoui, H., Farchane, A., & Safi, S. (2022, May) [5] assessed the security challenges in MANETs and offered AI-based security solutions. Bondada, P., Samanta, et. al. in [9] suggested a secure and energy-efficient routing protocol that utilizes group key management. This protocol incorporates two specialized nodes that employ Asymmetric Key cryptography and are selected based on energy consumption and trust values. Danilchenko, K., Azoulay, et. al. proposed a method for minimizing delays in MANETs in [10]. The authors focused on minimization of end-to-end packet delay by assigning weights based on request priorities.

In [11], Vargheese, M., Vanithamani, et. al. introduced a methodology that utilizes Fuzzy Logic Control (FLC) to establish a probabilistic QoS guarantee in MANETs. This approach leverages the mobility of network nodes to determine the probabilistic QoS. Furthermore, the methodology conservatively manages bandwidth by refraining from sending packets from the source network in the absence of efficient routes. Marandi, A. K., Dogra, R., Bhatt, R., Gupta, R., Reddy, S., &Barve, A. (2022) in [12], utilized a weighted graph to assess network performance in MANETs, aiding in the calculation of routes and identification of viable paths for routing metrics. The effectiveness of

the GBNWG model was compared to that of the traditional QOD technique.
The research paper authored by Rahamat Basha, & et. al. [13] centers on the implementation of a reliability forerunner advancing technique that employs the concept of straddling path recovery in MANET. The projected technique, referred to as Reliability Antecedent Packet Forwarding (RAF), ensures a dependable routing process between the source node and the destination node. This method effectively avoids the flooding of nodes, preserves previous routing information, and retrieves backup information in the event of communication interference.
In [14], Yamini, K. A. P., Stephy, J., Suthendran, K., and Ravi, V. (2022) introduced an innovative trust-based routing evidence scheme ETERE to enhance the detection of routing disruption attacks in MANETs. The author's approach comprises the development and manipulation of mental representations of information. Central to this proposal is I-Trust, a probabilistic approach designed to detect node misbehavior and secure the routing process in MANETs as part of the ETERE scheme. This paper evaluates the performance of the ETERE scheme against various routing disruption attacks, effectively demonstrating its efficacy in maintaining routing efficiency.
Abdan, M., and Seno, S. A. H. (2022) presented a study in [15] that focuses on machine learning techniques for wormhole attack detection in MANET. The authors utilize various machine learning methods, including Classic and Modern ML Algorithms for the purpose of classification. Notably, the study emphasizes the utilization of nodes' properties, particularly their speed, for feature extraction in MANETs.
In [16], Teli, T. A., et. al. conducted an extensive review of MANET Routing Protocols, their vulnerabilities to attacks, and strategies for mitigating such attacks. This study delves into different routing protocols employed in MANETs, explores various potential attacks on these protocols, and discusses methods to counter these threats. Additionally, the research presents a comparative analysis of the different routing protocols based on several criteria, including Route Structure, existence of Multiple Routes, Route Maintenance, Loop Freedom, Number of Required Tables, and usage of Hello Messages.
In [17], Al-Shareeda MA and Manickam S. delve into the increasing utilization of MANETs across various sectors such as environmental monitoring, efficient energy utilization, smart way of transportation, intelligence in agriculture, and ecosystem for the IoT ecosystems. The rapid advancement of wireless technology positions MANETs as significant players in the future of the Internet. However, the seamless inter-node communication that is integral to MANETs faces a critical challenge in the form of security threats, particularly MitM attacks that have taken center stage. MitM attacks happen if a malicious node captures and intercept data exchanged among legitimate nodes, posing a significant risk to the integrity of MANETs. This research targets examination of attackers' strategies in executing MitM assaults in MANETs, with a specific focus on delayed and dropped messages. Severe impact observed in the findings on authentic entities within MANETs, resulting in a substantial increase in compromised messages, elevated Delay, and Packet Loss.
In their work [18], Joardar S. et. al address the challenge of mitigating Denial of Service (DoS) attacks in MANETs by enhancing their resilience through AI-Integrated Node Reputation. The study highlights a potential limitation of general classification models, which may struggle to accurately identify DoS attacks. Such models often fail to distinguish between network errors and actual malicious attacks. This research contributes to the ongoing efforts to reinforce The MANET's security, ensuring their robustness in the face of evolving threats.
Saxena, M., Dutta, S., Singh, B. K., &Neogy, S. (2023) in [19] introduce a new routing algorithm, MO-AOMDV (Multi-objective-AOMDV). The algorithm selects routes as per node quality and links. The work used graph for representations of nodes and connections between nodes. The node keeps track of its own and neighboring nodes' residual energy.

In [2] Dabideen, S., Smith, B. R., & Garcia-Luna-Aceves, J. J. (2009, October) introduces a novel approach to enhance security in MANETs and contribute to dependable routing in the presence of node and/or link failures. Traditional network security solutions are not directly applicable to MANETs due to the unique challenges posed by node mobility and limited bandwidth. Furthermore, the mere discovery of a path does not guarantee successful data transmission. The authors focus on secure routing in MANETs, which requires the end-to-end verification of the physical attributes of paths and leverages the diversity of paths to identify secure routes. They incorporate this methodology into SRDV protocol. The paper demonstrates that this protocol exhibits comparable efficiency to existing secure and non-secure on-demand or proactive routing methods under normal conditions and provides robust defense against various types of attacks.

The comprehensive survey [21] conducted by VK Quy, VH Nam, DM Linh, and LA Ngoc in Wireless Personal Communications (2022) explores the rapidly evolving realm of MANETs and their increasing integration in various domains such as monitoring the environment, efficacy of energy, etc. The authors emphasize the growing significance of MANETs in the future landscape of the Internet. A crucial observation in this paper is that the performance of MANETs is primarily influenced by the routing protocols utilized, given the inherent characteristics of the mobile ad hoc environment. However, these protocols often encounter performance challenges. Therefore, the survey highlights the necessity for routing protocols that possess not only flexibility but also intelligence to enhance the overall network performance. The authors have extensively analyzed a range of proposed protocols designed for MANET-IoT networks and their classifications with regards to improvement in performance, QoS-awareness, energy-saving, and security-aware protocols. It is worth noting that most of these protocols have evolved from traditional routing protocols.

A noteworthy aspect of the study involves the evaluation of the traditional routing protocols with different speed of node movement. This comparison specifically aims to determine stable routing protocol for smart city environments. The findings from these experiments reveal that proactive protocols exhibit better results when the node movement is low. In contrast, reactive protocols demonstrate greater stability and higher performance in scenarios with high movement speeds.

The survey concludes by affirming the increasing importance of customizing routing protocols for MANETs, particularly through the enhancement of the AOMDV protocol. This enhancement is viewed as a crucial step towards developing more effective MANET systems for IoT ecosystems.

The study conducted by Ramalingam et al. (2022) in [22] delves into the challenges associated with providing QoS-aware service composition in MANETs through the utilization of a dynamic selection of secured broker mechanism. This work in MANETs aims to fulfill user requirements by considering different atomic services while considering non-functional QoS parameters. The authors utilize the AODV protocol and subject it QoS analysis on MANET's. The study proposes a novel architecture for QoSDSBS in service composition for MANETs. This architecture involves dynamic brokers that act as composers within the MANET network and facilitate Secure path selection.

Wireless ad hoc networks have become an integral part of various applications due to flexible nature, deployment’s ease, and operations in non-fixed infrastructure. The AOMDV routing protocol is commonly used in these networks to establish dynamic and efficient communication paths. However, the decentralized nature of ad hoc networks exposes them to security threats, with particular concern for MitM (MitM) attacks. This literature review examines existing research on preventing and detecting MitM attacks on the AOMDV routing protocol.

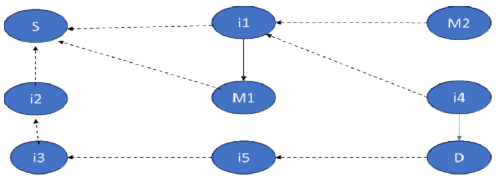
AOMDV establish and maintain multiple paths in-between source and destination nodes to ensure reliable communication. Research in this area often emphasizes the efficacy of AOMDV in managing dynamic network conditions, making it a suitable choice for ad hoc networks [2] [3]

MitM attacks are well-documented security threats where an adversary intercepts and potentially alters communication between two parties. In the context of AOMDV, MitM attacks exploit vulnerabilities in the route discovery and maintenance processes, compromising data integrity and confidentiality [17].
Studies have identified specific vulnerabilities in AOMDV that make it susceptible to MitM attacks. The on-demand nature of AOMDV enables attackers to inject themselves into the route discovery process, leading to the establishment of malicious communication paths. Additionally, the absence of robust authentication mechanisms in AOMDV contributes to its vulnerability.
Several proposed prevention strategies aim to enhance the security of AOMDV against MitM attacks. Cryptographic techniques, such as digital signatures and encryption, are suggested to secure the route discovery process and prevent unauthorized nodes from participating. Node authentication mechanisms are also proposed. This guarantee contributions on only trusted nodes in the routing, mitigating the risk of malicious entities disrupting communication.
Real-time detection of MitM attacks is crucial for maintaining the integrity of AOMDV-based networks. Research suggests integrating monitoring techniques to continuously observe network behavior. Anomaly detection methods are explored to identify deviations that may indicate a potential MitM attack. Trust-based systems, which evaluate the behavior of nodes within the network, are also considered for their effectiveness in detecting abnormal or malicious activities.
Existing research often evaluates proposed prevention and detection mechanisms through simulation and experimentation. These evaluations aim to assess the effectiveness of the strategies in securing AOMDV against potential security threats, particularly MitM attacks.
While significant progress has been made in understanding and addressing the security challenges of AOMDV, there are still gaps in the literature. Future research directions may include developing more advanced security mechanisms, exploring machine learning techniques for real-time detection, and considering emerging technologies to enhance the overall security of AOMDV-based ad hoc networks.
In conclusion, the literature review emphasizes the importance of securing AOMDV against MitM attacks and provides insights into existing research efforts focused on prevention and detection. The following segments of this research work will get deeper into specific vulnerabilities, prevention strategies, detection mechanisms, and the evaluation of proposed solutions.

VULNERABILITIES IN AOMDV :
The AOMDV (AOMDV) routing protocol, although efficient for dynamic ad hoc networks, is not impervious to security vulnerabilities. In the context of preventing and detecting MitM (MitM) attacks, it is imperative to comprehend these vulnerabilities. This section explores specific weaknesses in AOMDV that render it susceptible to MitM attacks. AOMDV operates as an on-demand routing protocol, wherein routes are established solely when required. This on-demand nature can be exploited by an attacker during the route discovery phase [2]. Malicious nodes have the capability to participate in the route establishment process, resulting in the creation of compromised communication paths. MitM attackers may intercept, modify, or selectively forward packets along these paths, compromising the integrity and confidentiality of the communication [17].
AOMDV lacks robust authentication mechanisms, posing a challenge to ensuring the legitimacy of participating nodes. In the absence of proper authentication, malicious nodes can inject themselves into the routing process, impersonate legitimate nodes, and potentially disrupt the routing paths [19]. This absence of node authentication opens the door for MitM attackers to compromise the integrity of the network. Once a route is established, AOMDV relies on periodic route maintenance to adapt to changing network conditions [3]. However, the lack of secure mechanisms for route maintenance introduces vulnerabilities. An attacker may exploit these vulnerabilities by injecting false route

updates, leading to the diversion of data through malicious nodes. This manipulation can result in MitM attacks as the compromised routes are utilized for communication.
While AOMDV is designed to adapt to the dynamic and frequent topology changes these changes, the network can be exploited by MitM attackers. Fluctuations in the network topology may be utilized by attackers to inject themselves into the routing process during periods of topology changes, further compromising the integrity of communication paths. AOMDV does not inherently incorporate encryption mechanisms to secure the exchanged routing information. The absence of encryption makes the protocol susceptible to eavesdropping by potential MitM attackers. Unauthorized access to routing information allows attackers to gain insights into the network's topology, facilitating the identification of potential targets and the injection of malicious nodes into the routing paths [2] [3].
Addressing these vulnerabilities is crucial to enhancing the security of AOMDV against MitM attacks. Next we present prevention strategies and detection mechanisms aimed at mitigating these vulnerabilities and ensuring the secure operation of the AOMDV routing protocol in ad hoc networks [2] [17] [19][23].

THE METHODOLOGY:
The AOMDV node employs a method of discovering multiple routes for a single destination on demand. In this process, the RREQ packets are broadcasted and an RREP is expected in response. AOMDV adopts a hop by hop routing approach. In contrast to AODV, the parent protocol of AOMDV, the AOMDV node does not discard duplicate RREP messages. Instead, it recognizes the potential for multiple routes in the duplicate RREP messages. This approach effectively reduces the frequency of route discovery. The fundamental principles of AOMDV are loop-free and disjoint route discovery.
In an active MitM attack, the attacker exploits the same idea used in AOMDV. The malicious nodes, m1 and m2, generate fake and illegitimate RREP messages in response to the RREQ messages. These fake RREP messages pretend to offer the shortest path to the destinations. As part of its normal routine algorithm, the AOMDV source node may consider these fake RREP messages as legitimate and initiate communication. This compromise on security greatly affects the confidentiality of the data. This attack is depicted in Figure 1 and Figure 2, which illustrate the presence of a MitM in AOMDV. In Figure 1, the broadcast of the RREQ message from the source node (S) is shown, along with the broadcast of the RREQ message by the neighboring intermediate node, along with the malicious nodes M1 and M2. Figure 2 displays the behavior of the malicious nodes (M1 and M2) when responding to the RREQ message. In this scenario, M1 and M2 do not broadcast the RREQ message but instead pretend to have a route to the destination.



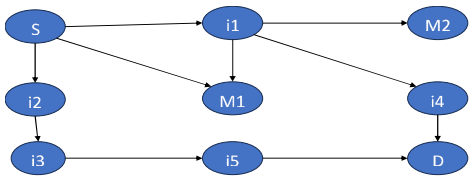


Fig. 1. Broadcast RREQ for route discovery. Fig. 2. RREP forwarded from the Destination(D)
As seen from the figures 1 & 2 node M1 & M2 provides shortest routes as it does not forward the RREQ to the intended destinations. Instead, they send RREP pretending that they have shortest route to destination. This paper is an attempt to address this issue. The proposed approach calculates the average of number of hopes needed by each received route. Since AOMDV does not discard duplicate routes in intent to discover multiple routes. Hope count and round trip delay between

source and destinations is considered and standard deviation of it considered for calculations of threshold. All routes having hope count and round trip time above threshold will be considered as legitimate and others below the threshold to be discarded considering illegitimate routs. Following protocol considered for evaluation

```
function calculateThreshold (routes):
        sumHops = 0
        sumRoundTripDelay = 0

   for each route in routes:
   sumHops += route.hopCount
        sumRoundTripDelay += route.roundTripDelay
   averageHops = sumHops / number_of_routes
   averageRoundTripDelay = sumRoundTripDelay / number_of_routes
   sumSquaredDifferences = 0

    for each route in routes:
   differenceHops = route.hopCount - averageHops
   differenceDelay = route.roundTripDelay - averageRoundTripDelay
   sumSquaredDifferences += differenceHops^2 + differenceDelay^2
   variance = sumSquaredDifferences / number_of_routes
        standardDeviation = sqrt(variance)
   threshold = averageHops + averageRoundTripDelay + standardDeviation
   return threshold

function filterLegitimateRoutes(routes, threshold):
   legitimateRoutes = []

for each route in routes:
   if route.hopCount + route.roundTripDelay> threshold:
        legitimateRoutes.append(route)
   return legitimateRoutes

function main():
   routes = AOMDV.discoverRoutes() // Assuming AOMDV is a function to discover routes
   threshold = calculateThreshold(routes)
   legitimateRoutes = filterLegitimateRoutes(routes, threshold)
   // Use legitimateRoutes for further processing or forwarding RREQs
   // Discard routes below the threshold as illegitimate routes
```

EVALUATION AND DISCUSSION:

The assessment of the proposed preventive and detection mechanisms for MitM (MitM) attacks on the AOMDV routing protocol is of utmost importance in determining their efficacy. In this section, the methodologies employed for evaluation, the experimental setup utilized, and the results obtained are discussed, shedding light on the effectiveness of the various strategies implemented. For simulation purposes, we utilized network simulator-2 (ns-2) version 2.34 [26] and employed the 802.11 MAC protocol to facilitate shared access to wireless channels. The simulation of the AOMDV protocol entailed the incorporation of both CBR and TCP traffic. To account for the mobility of nodes, the average node speed ranged from 5 to 50 ms. To test the resilience of the

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 1, No.1, January : 2025

AOMDV protocol during route discovery phases, various scenarios of MitM attacks were simulated. These scenarios encompassed different conditions such as varying numbers of nodes, mobility patterns, and traffic loads. The MitM attacks were carried out by attackers employing diverse strategies aimed at intercepting or manipulating data packets. Moreover, preventive strategies to ensure secure route discovery were implemented. The subsequent graphs present the findings pertaining to the AOMDV protocol, showcasing the impact of MitM attacks with threshold considerations. An analysis of throughput, routing overheads, end-to-end delay, and packet delivery ratio is presented for both the schemes.

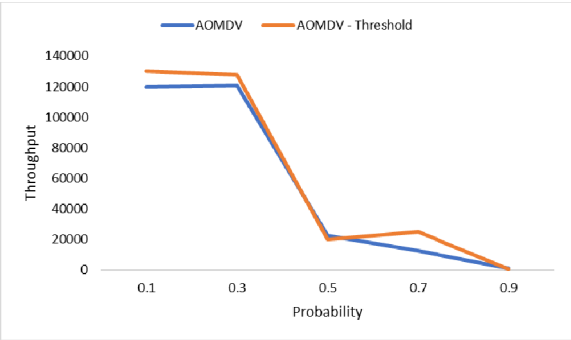


Fig. 3. Throughput

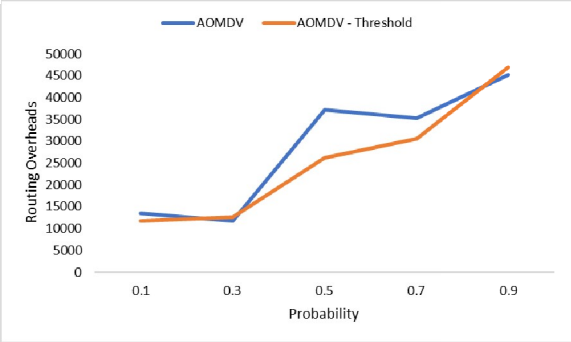


Fig. 4. Routing Overheads

When considered the throughput of AOMDV without threshold and proposed threshold mechanism the performance of two schemes presented in the graph shown above. It is evident from the graph in Figure 3 that the throughput improves when the threshold mechanism applied as the routes shown by malicious nodes are discarded. The simulation was run for 200s and mean node speed is varied. As the term overhead indicates it makes some impact on the processing. The routing overheads in terms of the threshold calculations increases on each node, this can be depicted by the graph in Figure 4. The routing overheads of the AOMDV without threshold are better. Focusing the detection and prevention of the malicious node the increase in routing heads looks advisable. The calculations of threshold include calculations of average hop count and round-trip delays at each node may it be source or intermediate. This calculation is definitely not at malicious nodes at first place.

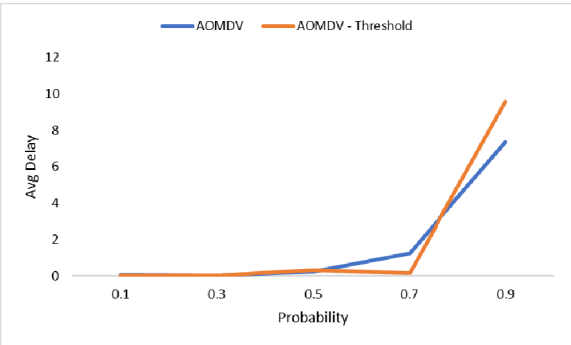


Fig. 5. End to End Delay

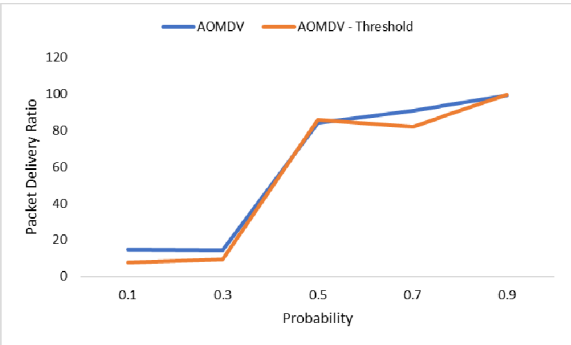


Fig. 6. Packet Delivery Ratio

Graph in Figure 5 show the end to end delay in packet deliveries when considered normal AOMDV and AOMDV with threshold calculations. It can be seen that the delay increases as the node mean speed increases. This may be as the threshold calculations procedures may be required to do frequently and more and more routes may get discarded in the process. Figure 6 shows a graph for Packet delivery ratio. The packet delivery ratio does not look to be affected more even if the

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 1, No.1, January : 2025

threshold mechanism is included in the processing.

The Graphs if Figure 3, Figure 4, Figure 5, and Figure 6 used to depict the performance of the AOMDV – Threshold against orthodox AOMDV with Random Waypoint mobility Model. The Graphs in Figure 7, Figure 8, Figure9 and Figure 10 presents the performance of AOMDV – Threshold against AOMDV with Random Walk Mobility Model.

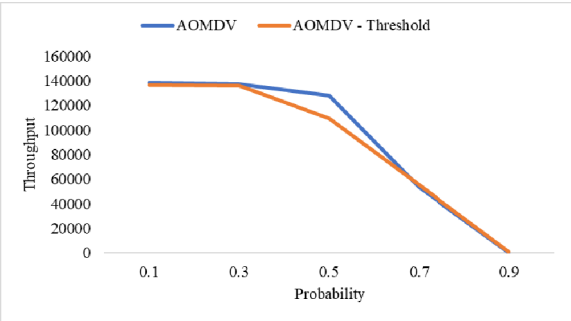


Fig. 7. Throughput

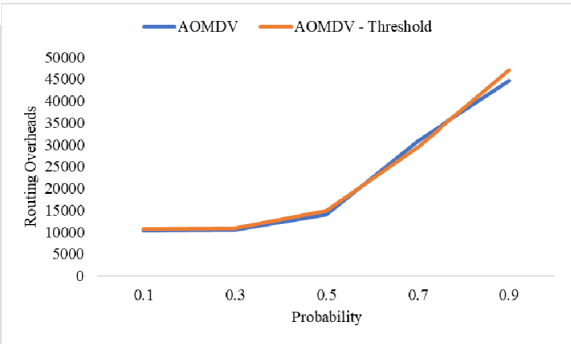


Fig. 8. Routing Overheads

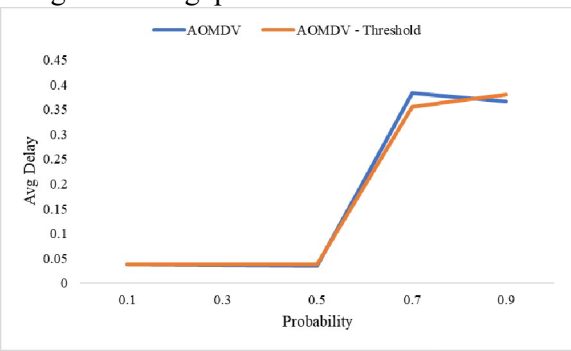


Fig. 9. End to End Delay

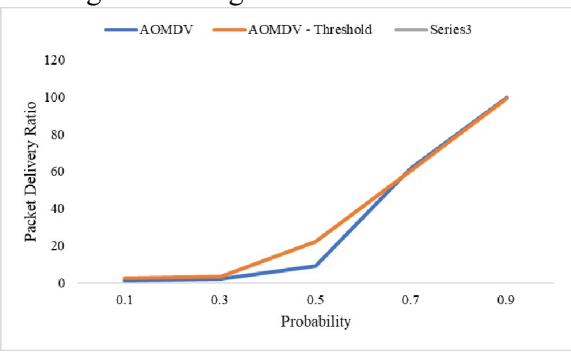


Fig. 10. Packet Delivery Ratio

The evaluation of the AOMDV routing protocol with respect to the MitM attack while considering the Random Walk mobility model can be seen through the Figures 7 to Figure 10. The graphs evidently present the performance of AOMDV- Threshold against traditional AOMDV. The novice protocol with addition of threshold aspects significantly shows similar performance for throughput (Fig. 7), Routing Overheads (Fig. 8), Average Delay (Fig. 9) and Packet delivery ratio (Fig. 10) in Random Walk Mobility Model.

The AOMDV performance with Random Waypoint and Random Walk Mobility models with and without threshold mechanism looks mostly alike, this proves to be a better addition to prevent the MitM attack. The integration of prevention and detection mechanisms generally resulted in a slight increase in end-to-end delay, attributable to the additional processing required for security checks. Despite this, the overall network performance, in terms of packet delivery ratio and throughput, remained robust under attack scenarios, indicating the effectiveness of the implemented security measures.

CONCLUSION :

The evaluation findings illustrate that the proposed methods of prevention and detection significantly augment the resilience of the AOMDV routing protocol against MitM attacks. While there exists an inherent trade-off between security and network performance, the equilibrium attained in these

experiments suggests that the security enhancements bring about advantages in upholding the integrity and dependability of ad hoc networks that employ the AOMDV protocol. Further research and enhancement of these methods might result in more optimized solutions that reduce the performance overhead while preserving high security standards.

REFERENCES :

[1] Sivapriya, N., & Mohandas, R. (2022). Analysis on Essential Challenges and Attacks on MANET Security Appraisal. *Journal of Algebraic Statistics*, 13(3), 2578-2589.
[2] Dr. Vivek Kute, Ad Hoc and Wireless Networks, *Notion Press Platform*, 2023
[3] Kute, Vivek B., and M. U. Kharat. "Analysis of quality of service for the AOMDV routing protocol." *Engineering, Technology & Applied Science Research* 3.1 (2013): 359-362.
[4] M. K. Marina, S. R. Das, "AOMDV routing", *Wirel. Commun. Mob. Comput*., Vol. 6, pp. 969-988, 2006
[5] Khalfaoui, H., Farchane, A., & Safi, S. (2022, May). An Overview of the Security Improvements of Artificial Intelligence in MANET. In *International Conference on Cybersecurity, Cybercrimes, and Smart Emerging Technologies* (pp. 135-146). Cham: Springer International Publishing.
[6] Lv, X., & Li, H. (2013). Secure group communication with both confidentiality and non-repudiation for mobile ad-hoc networks. *IET Information Security, 7(2), 61-66.*
[7] Hussain, S., Ahmed, S., Thasin, A., & Saad, R. M. (2022). AI-Enabled Ant-Routing Protocol to Secure Communication in Flying Networks. *Applied Computational Intelligence and Soft Computing*, 2022.
[8] Jia, X., Huang, D., & Qin, N. (2024). AI-enhanced security demand and routing management for MANETs with optical technologies. *Optical and Quantum Electronics*, 56(2), 229.
[9] Bondada, P., Samanta, D., Kaur, M., & Lee, H. N. (2022). Data security-based routing in MANETs using key management mechanism. *Applied Sciences*, 12(3), 1041.
[10] Danilchenko, K., Azoulay, R., Reches, S., & Haddad, Y. (2022). Deep learning method for delay minimization in MANET. *ICT Express*, 8(1), 7-10.
[11] Vargheese, M., Vanithamani, S., David, D. S., & Rao, G. R. K. (2023). Design of fuzzy logic control framework for qos routing in manet. *Intelligent Automation & Soft Computing*, 35(3), 3479-3499.
[12] Marandi, A. K., Dogra, R., Bhatt, R., Gupta, R., Reddy, S., &Barve, A. (2022). Generative Boltzmann Adversarial Network in Manet Attack Detection and QOS Enhancement with Latency. *International Journal of Communication Networks and Information Security*, 14(3), 199-213.
[13] Rahamat Basha, S., Sharma, C., Sayeed, F., Arularasan, A. N., Pramila, P. V., Shinde, S. K., ... &Yeshitla, A. (2022). Implementation of reliability antecedent forwarding technique using straddling path recovery in manet. *Wireless Communications and Mobile Computing*, 2022, 1-9.
[14] Yamini, K. A. P., Stephy, J., Suthendran, K., & Ravi, V. (2022). Improving routing disruption attack detection in MANETs using efficient trust establishment. *Transactions on Emerging Telecommunications Technologies*, 33(5), e4446.
[15] Abdan, M., & Seno, S. A. H. (2022). Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (MANET). *Wireless Communications and Mobile Computing*, 2022, 1-12.
[16] Teli, T. A., Yousuf, R., & Khan, D. A. (2022). MANET Routing Protocols Attacks and Mitigation Techniques: A Review. *International Journal of Mechanical Engineering*, 7(2), 1468-1478.
[17] Al-Shareeda MA, Manickam S. MitM Attacks in Mobile Ad Hoc Networks (MANETs): *Analysis and Evaluation. Symmetry*. 2022; 14(8):1543. https://doi.org/10.3390/sym14081543.
[18] Joardar, S., Sinhababu, N., Dey, S., & Choudhury, P. (2023). Mitigating DoS attack in MANETs considering node reputation with AI. *Journal of Network and Systems Management*, 31(3), 1-34.
[19] Saxena, M., Dutta, S., K. Singh, B., &Neogy, S. (2023). Multi-objective based route selection approach using AOMDV in MANET. *SN Computer Science*, 4(5), 581.
[20] Dabideen, S., Smith, B. R., & Garcia-Luna-Aceves, J. J. (2009, October). An end-to-end solution for secure and survivable routing in manets. In *2009 7th International Workshop on Design of Reliable Communication Networks* (pp. 183-190). IEEE.
[21] Quy, V. K., Nam, V. H., Linh, D. M., & Ngoc, L. A. (2022). Routing algorithms for MANET-IoT networks: a comprehensive survey. *Wireless Personal Communications*, 125(4), 3501-3525.

[22] Ramalingam, R., Muniyan, R., Dumka, A., Singh, D. P., Mohamed, H. G., Singh, R., ... &Noya, I. D. (2022). Routing protocol for MANET based on QoS-aware service composition with dynamic secured broker selection. *Electronics*, 11(17), 2637.

[23] Ahmad F, Adnane A, Franqueira VNL, Kurugollu F, Liu L. MitM Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers' Strategies. *Sensors. 2018; 18(11):4040. https://doi.org/10.3390/s18114040*

[24] V. C. Patil, R. V. Biradar, R. R. Mudholkar, S. R. Sawant, "On-demand multipath routing protocols for mobile ad hoc networks issues and comparison", *International Journal of Wireless Communication and Simulation, Vol. 2, No 1, pp. 21-38, 2010.*

[25] V. B. Kute, M. U. Kharat, "Survey on QoS for multi-path routing protocols in MANET", *3rd International Conference on Machine Learning and Computing (ICMLC 2011),* Vol. 4, pp. 524-528, 2011

[26] K. Fall, K. Varadhan, The Ns Manual, *http://www.isi.edu/nsnam/ns/nsdocumentation.html*, last accessed: Jan 6, 2009