IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Journal Européen des Systèmes Automatisés
Vol. 57, No. 3, June, 2024, pp. 861-867
Journal homepage: http://iieta.org/journals/jesa

Secure AODV Routing Strategies in Smart Cities for Vehicular Communication

Ali Muayed Fadhil[1,2*], Norashidah Md Din[3], Norazizah Binti Mohd Aripin[4], Ali Ahmed Abed[2]

[1] College of Graduate Studies, Universiti Tenaga Nasional, Jalan IKRAM- UNITEN, Kajang 43000, Malaysia
[2] Department of Computer Engineering, University of Basrah, Basrah 61001, Iraq
[3] Institute of Energy Infrastructure, Universiti Tenaga Nasional, Jalan IKRAM- UNITEN, Kajang 43000, Malaysia
[4] Institute of Power Engineering, Universiti Tenaga Nasional, Jalan IKRAM- UNITEN, Kajang 43000, Malaysia

Corresponding Author Email: PE21251@student.uniten.edu.my

https://doi.org/10.18280/jesa.570325

Received: 18 April 2024
Revised: 26 May 2024
Accepted: 7 June 2024
Available online: 25 June 2024

Keywords:
AODV, secure routing, VANET, smart city

ABSTRACT

Vehicular Ad hoc Networks (VANETs) have become prominent in the past few years for the transportation sector. Vehicular mobility poses a significant challenge for establishing private communications in VANETs. The classical Ad hoc On-Demand Distance Vector (AODV) routing protocol used in VANET assumes that all nodes are non-malicious. To address this matter, this paper proposes making AODV routing protocols more secure by using a privacy scheme in AODV for vehicle-to-vehicle communication. The AODV privacy scheme tries to keep the automobile network connected reliably and stably during communication with the secured transmission of messages and minimize the risk of unauthorized access to sensitive information from eavesdropper attacks. The proposed privacy secure AODV routing named PSAODV used pseudonym changes in vehicle communication to hide the target vehicle's location. A VANET simulator based on OMNET++ and SUMO are used for evaluating the PSAODV routing protocol. A simulation study was conducted that compared the PSAODV with SE-AOMDV, ECC-AODV, and AODV in fundamentals of efficiency and confidentiality. The analysis results showed that PSAODV routing demonstrates routing efficiency with privacy by diminishing the effect of eavesdropping of vehicles information based on various scenarios in urban cities.

1. INTRODUCTION

Vehicular Ad hoc Networks (VANETs) have become an essential technology in recent years and have far-reaching consequences for the transportation industry [1]. VANETs enable real-time communication for functions like collision prevention and traffic management within smart cities and intelligent transport systems, but their dynamic nature and frequent mobility challenge data protection [2]. VANETs include interchange of data between infrastructure and automobiles, allowing sophisticated functions like collision prevention, traffic management, and infotainment. Nevertheless, VANETs' highly dynamic structure, frequent node mobility, and broadcast wireless communication make them unique properties, make protecting sensitive vehicle and driver data challenging [3]. Secured routing in VANETs uses methods and protocols to ensure the impervious transmission of routing data and communication between vehicles in ever-changing and potentially hostile environments The main features of secure routing are message integrity, authenticity, and privacy while mitigating various attacks that could compromise vehicular communication effectiveness and reliability in the road scenario [4]. VANETs raise privacy concerns because adversaries can track vehicles' movements and behaviors during the road, resulting in a range of hazards, including violations of location privacy and unauthorized entry to confidential data [5].

Privacy strategies in routing ensure message delivery while reducing the exposure of confidential data like the vehicle's identification, geographical coordinates, and travel routes [6]. The existing routing protocols used in VANETs fail to consider the essential aspect of securing the location privacy of vehicles. Consequently, this presents a substantial hazard to individual safety and information security [7]. AODV is a famous and widely utilized routing protocol in VANETs because of its reactive nature, which reduces control overhead and effectively adjusts to the changing vehicular network conditions [8].

In general, implementing a privacy scheme in the VANET routing protocol can ensure location privacy and enhance network security. Enhancing the AODV routing protocol with a privacy layer can conceal vehicle information, protecting against eavesdropping attacks. This approach can significantly improve privacy and network efficiency in VANETs, ensuring safer and more secure vehicular communication in smart urban environments. Providing privacy-based routing protocol in VANET can provide the following potential benefits:

Anonymity: Privacy schemes can provide anonymity to vehicles in vehicular networks, making it difficult for unauthorized entities to track individual vehicles' movements and identify their owners or drivers. By concealing the identity of the vehicles to protect privacy on the road.

Location privacy: With a privacy scheme integrated into the routing protocol, vehicles can transmit and receive messages while keeping their precise location information private. This prevents unauthorized entities from monitoring vehicles' movements and destinations, which enhances location privacy.

Network security: In addition to protecting the identity and location information, privacy schemes can ensure the improvement of the data transmitted over the VANET by employing secure routing protocols, reducing the risk of unauthorized access or eavesdropping.

The objectives of this article are as follows:

• To provide invaluable insights for designing a privacy-respecting vehicular communication system.

• To propose an improved AODV with privacy-enhancing mechanisms in addressing the vulnerabilities associated with information leakage, unauthorized tracking, and location-based attacks which provides protection from network eavesdropper attacks.

The paper is classified into 6 sections. Section 2 presents recent techniques of VANET privacy routing. Section 3 discussed AODV routing and the privacy attack model. Section 4 is the proposed privacy routing scheme whereas Section 5 provides the simulation results analysis. Section 6 is the conclusion.

2. RELATED WORK IN SCURE ROUTING

Traditional routing protocols often neglect security and privacy considerations. While it is essential for establishing efficient communication paths, as a response to these concerns, researchers have been actively investigating innovative approaches that integrate privacy preservation mechanisms into the routing processes of VANETs. This section discusses related work in privacy routing in VANET. They can be grouped into seven categories as follows:

(1) Geographical-based routing protocols

Confidentiality in Secure Geographical Routing: Ensures security by identifying and thwarting harmful nodes using two directional antennas [9].

Location-Based Routing: Manages location information at roadside units to provide location anonymity and prevent unauthorized queries [10, 11]. This is an infrastructure supported route privacy preservation method.

(2) Vehicular social networks secure routing with searchable encryption

Ensures message privacy using a framework that protects keyword confidentiality, resource privacy, demand source verification, and data integrity [12].

(3) Enhanced AODV protocols

Novel AODV with Elliptic Curve Cryptography (ECC) were proposed for key generation and certificate authority for vehicle verification to protect against black hole attacks [13, 14]. This approach achieved good throughput but creates more overhead across the network.

SE-AOMDV Protocol provides safe routing between vehicles using authentication and detection of malicious behavior [15].

(4) Urban peer-to-peer vehicular networks privacy and security certification framework

This framework detects black holes and minimizes transmission delays in urban peer-to-peer vehicular networks [16].

(5) Software-defined networks and blockchain

This leverages on a distributed software-defined network architecture integrated with blockchain for enhanced security in VANET [17].

(6) Hybrid optimization and deep learning hybrid optimization-based deep learning

This technique classifies attacks in VANETs and selects Cluster Heads for routing based on proper feature selection [18].

(7) Trust-based and fuzzy logic authentication and routing

This method restricts the involvement of malicious entities during routing by trust evaluation. A fuzzy logic authentication component was incorporated [19, 20].

This categorization highlights the diversity of privacy-preserving approaches in VANETs, addressing various aspects of security and privacy through different methodologies. So far, there is no privacy scheme being explored with AODV routing using pseudonym change in control messages between vehicle-to-vehicle communication which is the focus of this work.

3. SYSTEM COMPONENTS DESCRIPTION

This section discusses the AODV routing including operation and description also the attack model scenario.

3.1 AODV routing

The AODV protocol is designed to minimize the utilization of bandwidth and computational resources by only transmitting packets when necessary. AODV enables efficient route acquisition for new destinations by mobile nodes, without necessitating the maintenance of routes to targets without active communication [21]. The AODV routing protocol includes the main stages: routing discovery, data forwarding, and maintenance. AODV routing protocol message types include Route Requests (RREQs), Route Replies (RREPs), Route Reply Acknowledgement (RREP-ACK), and Route Errors (RERRs).

AODV includes route table entries like: Destination IP Address, destination sequence number, routing flags, hop count, list of precursors, and lifetime of the route. The AODV creates routes when a vehicle requires transmitting a continuous stream of packets to a destination that lacks a path to it or when its path has expired [22].

The source vehicle transmits an RREQ to navigate to the destination The RREP forwarded directly from target to source or via any subsequent vehicle capable of fulfilling the request that contains a valid route, has a destination sequence number

that is equal to or greater than the one included in the RREQ message [23].

A vehicle generates new entries in the route table once it establishes a path to a new destination. Nodes send RERR messages to precursor nodes about the occurrence of link failure. These messages are illustrated in Figure 1 [24].

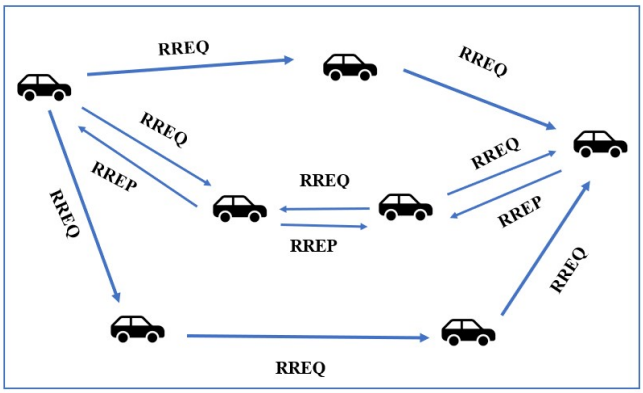

Figure 1. The AODV dissemination of RREQ and RREP

A vehicle in VANET is provided with an On-Board Unit (OBU), a Global Positioning System (GPS), and radar, that establishes communication with other entities within the VANET [25].

3.2 Attack model

VANET is vulnerable to a diverse range of attacks. The primary focus of this study revolves around eavesdropper attacks, in the context of privacy attacks that track various control packets (RREQ, RREP, RERR) in an AODV routing scenario. The privacy scheme technique makes use of a vehicle's pseudonym in response to tracking information from nearby vehicles. Two components are involved in the privacy attack as below.

3.2.1 Eavesdropping stations

The eavesdropper stations are designed to passively monitor the wireless medium to intercept beacon signals transmitted by vehicles. These stations are distributed strategically across an urban area, with their quantity and placement determined by analyzing the typical transmission range of vehicles. By intercepting these beacons, eavesdroppers can gather confidential information such as vehicle positions and velocities. This information is then relayed to the vehicle tracker system [26].

3.2.2 Vehicle tracker system

The vehicle tracker collects beacons from multiple eavesdropping stations. It ensures the elimination of duplicate entries to maintain data integrity. The tracker uses a sophisticated tracking algorithm to reconstruct vehicle trajectories based on the intercepted beacons. This algorithm helps in plotting the movement paths of vehicles accurately. With detailed information about vehicle positions and movements, the system can facilitate various attacks by adversaries, such as inserting or modifying messages within the network to disrupt communication and operations [27]. Figure 2 depicts the attack model.

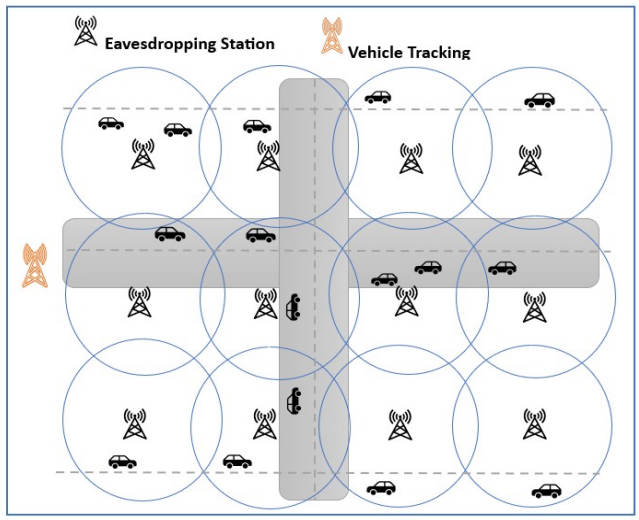

Figure 2. Eavesdropping station and vehicle tracker system

4. THE PROPOSED SECURE ROUTING

The proposed approach uses pseudonyms to protect the node in AODV routing from eavesdropping attacks. The control message in AODV is adapted to become a Pseudonym Route Request (PRREQ), Pseudonym Route Replay (PRREP), Pseudonym Route Error (PRERR) and Pseudonym Route Reply Acknowledgement (PRREP-ACK). The privacy scheme technique makes use of the silent period, where a vehicle's pseudonym will be periodically altered in response to the tracking information from nearby vehicles. The PSAODV algorithm is given below.

The Proposed Secure AODV (PSAODV) Algorithm
Input: All vehicles in the network area Output: Select the route with privacy metrics Step 1: - Creates routes when a vehicle requires - Set up the privacy factors - The vehicle initiates PRREQ for transmission of a data packet - PRREP packet from the neighbor will include a pseudonym - Messages contain the destination ID along with a pseudonym packet - The source chose intermediate PRREP - According to pseudonyms and message quality - Each intermediate node will iterate through the same process. Step 2: - When a route is acquired and activated with a pseudonym packet - The route is established by sending a unicast PRREP back - Vehicle regularly transmits HELLO messages - Monitor the quality of routes and update privacy levels - If a route is compromised (PRERRs), - Start Route Maintenance to discover another -Else - Packet sent to the destination vehicle - Periodically refresh pseudonyms with AODV messages - Repeat steps 1 and 2 - End processing

In the PSAODV simulation scenario, the use of pseudonym aims to provide routing security from any eavesdropping attack whilst not affecting network performance, i.e. quality-of-service parameters from routing inefficiency. The PSAODV protocol works in vehicle-to-vehicle communication without involving roadside units. The simulation scenario is shown in Figure 3.

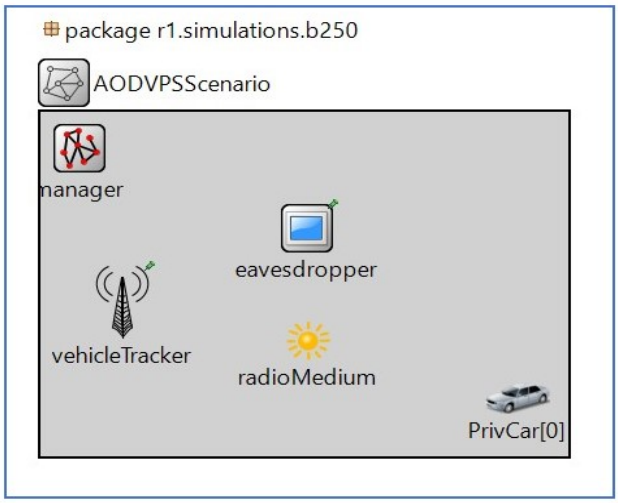

Figure 3. The PSAODV routing scenario with attack model

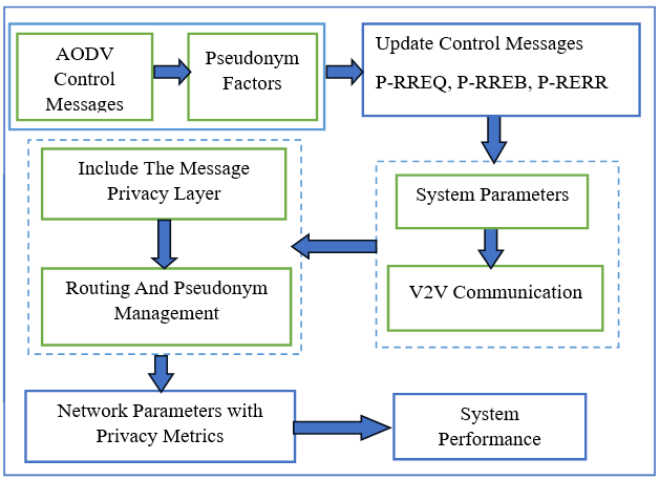

Figure 4. PSAODV protocol flow in vehicle-to-vehicle communication scenario

Several performance parameters must be evaluated when adding a privacy scheme to the AODV routing protocol in VANETs. These parameters assess the effectiveness of the privacy scheme and its impact on the overall network routing performance. Here are the three key performance parameters to consider:

Routing Efficiency: Assess how efficiently the enhanced privacy AODV selects message delivery routes. Efficient routing ensures that messages reach their destinations while minimizing the number of hops and utilizing network resources. Identify scenarios where privacy comes at a cost and scenarios where it provides significant benefits. The QoS parameters are used for assessing this.

Privacy Effectiveness: Measure the degree to which the privacy mechanisms achieve their intended goals. Evaluate parameters like pseudonym change frequency, location accuracy after cloaking, and the anonymity level achieved by anonymous routing. This makes the privacy-enhanced protocol resilient to attacks that aim to bypass or exploit the privacy mechanisms. Consider attacks like location inference, and pseudonym tracking. Location error is used in this work.

Scalability: Analyze how well the privacy enhanced AODV scales as the network size increases. Evaluate how well the protocol supports privacy policies in different scenarios. Consider whether users can customize their privacy settings effectively. Evaluate its performance under various network densities.

Figure 4 shows the PSAODV protocol flow in incorporating the pseudonym in the vehicle-to-vehicle communication scenario.

The PSAODV routing process is depicted in Figure 5.

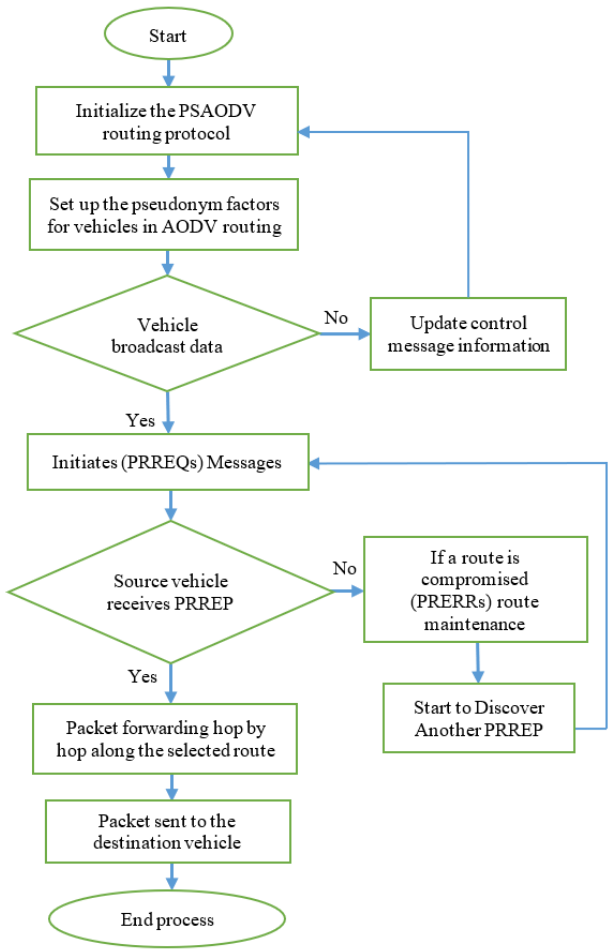

Figure 5. Flow chart of the PSAODV routing process

5. RESULTS AND ANALYSIS

The simulation study was conducted using the road network extracted from Open Street Map database of Basrah, Iraq, in an urban city area. The urban scenarios traffic generation on the road are produced by SUMO [28] with OMNET++ [29], through a traffic Control Interface (TraCI) in VEINS [30] as presented in Figure 6. The network simulation is based on events and a microsimulation model specifically designed for road traffic. The performance of PSAODV was studied under varying numbers of eavesdropping stations with the number of vehicles of 50, 150, and 250 at various speeds in a network coverage area of 2500m×2500m (Figure 7). The simulation parameters are given described in Table 1.

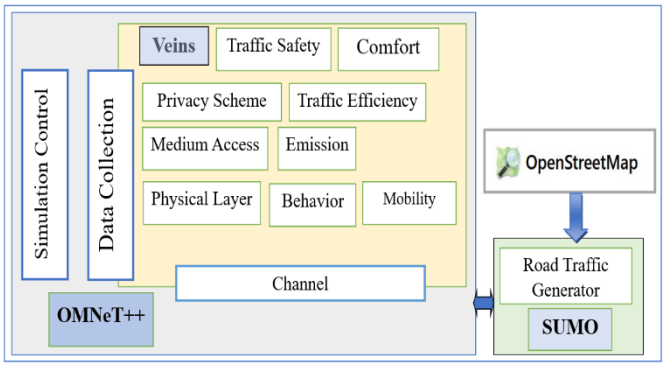

Figure 6. The simulation program framework

Figure 7. Urban map 2500m×2500m simulation scenario

Table 1. Parameters description

Parameters	Value
The urban scenario	2500m×2500m
Vehicles range	50,150,250
Simulation time	1000s
Transmission range	250m
Radio propagation	Two Ray Ground
Packet rate	512 bytes
MAC layer	IEEE 802.11p
Program simulation	Omnet++, Veins, SUMO.
Vehicles speed	40km
Routing protocol	PS-AODV
Eavesdropping station	25
Mobility model	Traffic Control Interface (TraCI)
Traffic type	User Datagram Protocol

The performance parameters used in the study is as follow:

Packet Delivery Ratio (PDR) %: The ratio refers to the total message's destination receives concerning to source-sent packet count. Where v reflects the whole of the network's nodes and represents Kbps.

$$PDR = \left(\frac{\sum_0^V packet\ recived}{\sum_o^r packet\ sent} \times 100\%\right) \quad (1)$$

Network Throughput (NT): The quantity of packets that the destinations have successfully received in the simulation time and is represented in Kbps.

$$NT = \frac{No.of\ packets\ successfully\ recived}{Simulation\ time} \quad (2)$$

The Average Delay: This shows the packet average latency that is successfully received at the destination after being created at the source node across a VANET, and it is represented in milliseconds.

$$AD = \frac{\sum_1^n Recived\ time - Send\ time}{No.of\ packet\ successfully\ sent} \quad (3)$$

In the simulation study, the PSAODV protocol has been compared to three other protocols which are AODV, SE-AOMDV, and ECC-AODV. By changing the number of vehicles within the VANET, the throughput, and routing load were observed. Figures 8 and 9 illustrate the throughput and packet delivery ratio of the compared protocols and various vehicles levels.

In all instances, the throughput and packet delivery ratio of PSAODV showed better performance. This is because the technique introduces pseudonyms at the control messages and does not consume additional overhead. By utilizing this privacy metric in the routing scheme, PSAODV enhances the reliability of data transmission avoiding eavesdropping and any related interference that may cause from it. For throughput, PSAODV produced better performance when compared to ECC-AODV by 9%, SE-AODV by 12%, and AODV by 17%. The results also showed that PSAODV routing protocol improves the packet delivery ratio by approximately 11% compared to ECC-AODV, 14% to SE-AODV, and 21% to AODV.

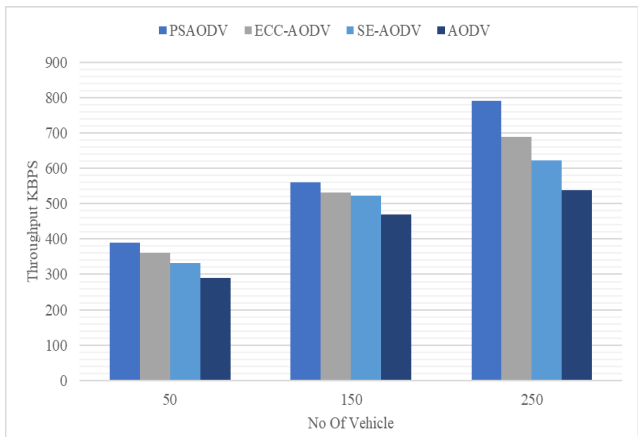

Figure 8. Throughput based on number of vehicles

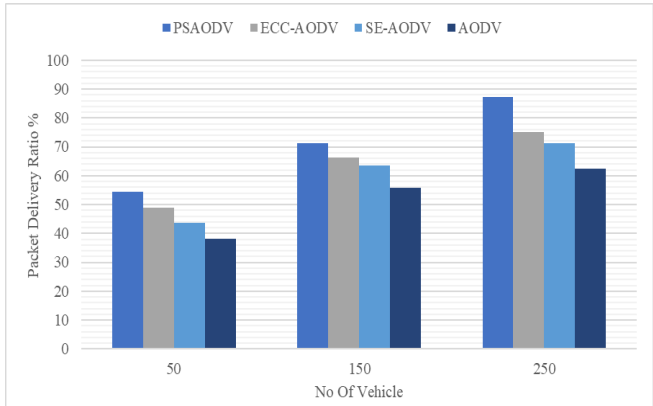

Figure 9. Packet delivery ratio results

Figure 10 displays a graphical depiction of the average delay calculation with different levels of vehicles. Like the earlier results, the suggested protocol is contrasted with ECC-AODV, SE-AODV, and AODV. The eavesdropping attack reduces PRREQ packets, which in turn enhances network performance. The graph demonstrates that the suggested PSAODV protocol's delay is less than other protocols compared. As for the average delay, PSAODV also improved the delay when compared to ECC-AODV by 7%, SE-AODV by 9%, and AODV by 14%.

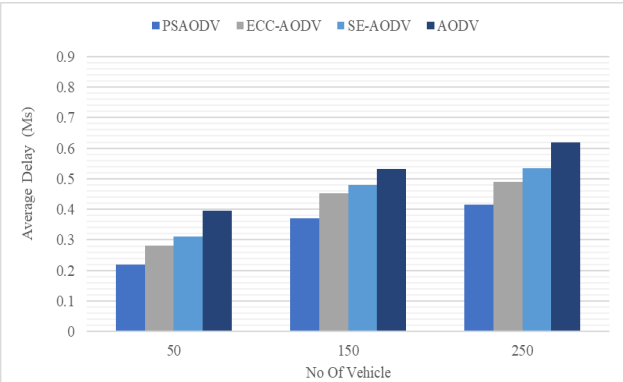

Figure 10. Average delay comparison for vehicles levels

6. CONCLUSIONS

The secure data in VANET can protect vehicles' and occupants' sensitive information, identities, and communication patterns. The fusion of privacy-aware mechanisms with AODV routing presents a promising avenue for addressing the privacy and security concerns accompanying the widespread adoption of VANET technology. To stop eavesdropping activities and disruptive attacks, this proposed solution finds a balance between the privacy of each node and the performance of the network. PSAODV efficiently safeguards location privacy for vehicular transportation during scenario. In this study, the PSAODV protocol enhances AODV control messages with a privacy layer to mitigate eavesdropping attacks.

The PSAODV protocol has been compared to that of other protocols, namely AODV, SE-AOMDV, and ECC-AODV. The simulation results indicate that the PSAODV protocol outperforms the other protocols. PSAODV produced higher packet delivery ratio, throughput, decreased packet loss and average delay, and decreased in location error. These indicates that network performances were not adversely affected by eavesdropping attacks.

This study demonstrates that the use of pseudonym in the proposed PSAODV protocol achieves optimal performance in securing vehicle-to-vehicle communication and can be a good candidate for vehicular communication in our quest for smart transportation systems in smart cities environments. Future works will be looking into testing the algorithm with real world data and investigate further the need for a predictive capability using artificial intelligence and machine learning in terms of pseudonym generation with respect to efficiency and scalability.

ACKNOWLEDGMENT

Thanks to College of Graduate Studies and Institute of Energy Infrastructure, Universiti Tenaga Nasional UNITEN, Malaysia for supporting this project.

REFERENCES

[1] Jurczenia, K., Rak, J. (2022). A survey of vehicular network systems for road traffic management. IEEE Access, 10: 42365-42385. https://doi.org/10.1109/ACCESS.2022.3168354

[2] Lv, Z., Shang, W. (2023). Impacts of intelligent transportation systems on energy conservation and emission reduction of transport systems: A comprehensive review. Green Technologies and Sustainability, 1(1): 100002. https://doi.org/10.1016/j.grets.2022.100002

[3] Kaur, K., Verma, H.K. (2022). An intelligent communication system for collision avoidance on roads: A smart city application. Computers and Electrical Engineering, 103: 108398. https://doi.org/10.1016/j.compeleceng.2022.108398

[4] Rao, B.T., Patibandla, R.L., Narayana, V.L. (2021). Comparative study on security and privacy issues in VANETs. Cloud and IoT-Based Vehicular Ad Hoc Networks, 145-162. https://doi.org/10.1002/9781119761846.ch8

[5] Jan, S.A., Amin, N.U., Othman, M., Ali, M., Umar, A.I., Basir, A. (2021). A survey on privacy-preserving authentication schemes in VANETs: Attacks, challenges and open issues. IEEE Access, 9: 153701-153726. https://doi.org/10.1109/ACCESS.2021.3125521

[6] Soni, G., Chandravanshi, K. (2022). A novel privacy-preserving and denser traffic management system in 6G-VANET routing against black hole attack. In Sustainable Communication Networks and Application: Proceedings of ICSCN 2021. Singapore: Springer Nature Singapore, pp. 649-663. https://doi.org/10.1007/978-981-16-6605-6_49

[7] Liu, J., Bai, F., Weng, H., Li, S., Cui, X., Zhang, Y. (2020). A routing algorithm based on real-time information traffic in sparse environment for VANETs. Sensors, 20(24): 7018. https://doi.org/10.3390/s20247018

[8] Reddy, B., Dhananjaya, B. (2022). The AODV routing protocol with built-in security to counter blackhole attack in MANET. Materials Today: Proceedings, 50: 1152-1158. https://doi.org/10.1016/j.matpr.2021.08.039

[9] Punitha, A., Manickam, J.M.L. (2017). Privacy preservation and authentication on secure geographical routing in VANET. Journal of Experimental & Theoretical Artificial Intelligence, 29(3): 617-628. https://doi.org/10.1080/0952813X.2016.1212103

[10] Rabieh, K., Mahmoud, M.M., Younis, M. (2016). Privacy-preserving route reporting schemes for traffic management systems. IEEE Transactions on Vehicular Technology, 66(3): 2703-2713. https://doi.org/10.1109/TVT.2016.2583466

[11] Wang, Y., Li, X., Zhang, X., Liu, X., Weng, J. (2021). ARPLR: An all-round and highly privacy-preserving location-based routing scheme for VANETs. IEEE Transactions on Intelligent Transportation Systems, 23(9): 16558-16575. https://doi.org/10.1109/TITS.2021.3134686

[12] Ferrag, M.A., Ahmim, A. (2017). ESSPR: An efficient

secure routing scheme based on searchable encryption with vehicle proxy re-encryption for vehicular peer-to-peer social network. Telecommunication Systems, 66(3): 481-503. https://doi.org/10.1007/s11235-017-0299-y

[13] Safavat, S., Rawat, D.B. (2020). On the elliptic curve cryptography for privacy-aware secure ACO-AODV routing in intent-based internet of vehicles for smart cities. IEEE Transactions on Intelligent Transportation Systems, 22(8): 5050-5059. https://doi.org/10.1109/TITS.2020.3008361

[14] Kumar, M., Jain, V., Jain, A., Bisht, U.S., Gupta, N. (2019). Evaluation of black hole attack with avoidance scheme using AODV protocol in VANET. Journal of Discrete Mathematical Sciences and Cryptography, 22(2): 277-291. https://doi.org/10.1080/09720529.2019.1585635

[15] Meddeb Makhlouf, A., Guizani, M. (2019). SE-AOMDV: Secure and efficient AOMDV routing protocol for vehicular communications. International Journal of Information Security, 18(5): 665-676. https://doi.org/10.1007/s10207-019-00436-z

[16] Alaya, B. (2021). Efficient privacy-preservation scheme for securing urban P2P VANET networks. Egyptian Informatics Journal, 22(3): 317-328. https://doi.org/10.1016/j.eij.2020.12.002

[17] Mershad, K. (2020). SURFER: A secure SDN-based routing protocol for internet of vehicles. IEEE Internet of Things Journal, 8(9): 7407-7422. https://doi.org/10.1109/JIOT.2020.3038465

[18] Kaur, G., Kakkar, D. (2022). Hybrid optimization enabled trust-based secure routing with deep learning-based attack detection in VANET. Ad Hoc Networks, 136: 102961. https://doi.org/10.1016/j.adhoc.2022.102961

[19] Azhdari, M.S., Barati, A., Barati, H. (2022). A cluster-based routing method with authentication capability in Vehicular Ad hoc Networks (VANETs). Journal of Parallel and Distributed Computing, 169: 1-23. https://doi.org/10.1016/j.jpdc.2022.06.009

[20] Shokrollahi, S., Dehghan, M. (2023). TGRV: A trust-based geographic routing protocol for VANETs. Ad Hoc Networks, 140: 103062. https://doi.org/10.1016/j.adhoc.2022.103062

[21] Malik, S., Sahu, P.K. (2019). A comparative study on routing protocols for VANETs. Heliyon, 5(8): e02340, https://doi.org/10.1016/j.heliyon.2019.e02340

[22] Shrivastava, P.K., Vishwamitra, L.K. (2021). Comparative analysis of proactive and reactive routing protocols in VANET environment. Measurement: Sensors, 16: 100051. https://doi.org/10.1016/j.measen.2021.100051

[23] Ajjaj, S., El Houssaini, S., Hain, M., El Houssaini, M.A. (2022). Performance assessment and modeling of routing protocol in vehicular ad hoc networks using statistical design of experiments methodology: A comprehensive study. Applied System Innovation, 5(1): 19. https://doi.org/10.3390/asi5010019

[24] Hota, L., Nayak, B.P., Kumar, A., Sahoo, B., Ali, G.M.N. (2022). A performance analysis of VANETs propagation models and routing protocols. Sustainability, 14(3): 1379. https://doi.org/10.3390/su14031379

[25] Sohail, M., Latif, Z., Javed, S., Biswas, S., Ajmal, S., Iqbal, U., Raza, M. (2023). Routing protocols in vehicular adhoc networks (VANETs): A comprehensive survey. Internet of Things, 100837. https://doi.org/10.1016/j.iot.2023.100837

[26] Kerrache, C.A., Calafate, C.T., Cano, J.C., Lagraa, N., Manzoni, P. (2016). Trust management for vehicular networks: An adversary-oriented overview. IEEE Access, 4: 9293-9307. https://doi.org/10.1109/ACCESS.2016.2645452

[27] Emara, K., Woerndl, W., Schlichter, J. (2013). Vehicle tracking using vehicular network beacons. In 2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Madrid, Spain, pp. 1-6. https://doi.org/10.1109/WoWMoM.2013.6583473

[28] Krajzewicz, D., Erdmann, J., Behrisch, M., Bieker, L. (2012). Recent development and applications of SUMO-Simulation of Urban MObility. International Journal on Advances in Systems and Measurements, 5(3&4): 128-138.

[29] Varga, A., Hornig, R. (2010). An overview of the OMNeT++ simulation environment. In 1st International ICST Conference on Simulation Tools and Techniques for Communications, Networks and Systems, Marseille, France, 2008: 1-10. http://doi.org/10.4108/ICST.SIMUTOOLS2008.3027

[30] Sommer, C., Eckhoff, D., Brummer, A., Buse, D.S., Hagenauer, F., Joerer, S., Segata, M. (2019). Veins: The open source vehicular network simulation framework. In Recent Advances in Network Simulation, pp. 215-252. Springer, Cham. https://doi.org/10.1007/978-3-030-12842-5_6