COMPUTOLOGY: Journal of Applied Computer Science and Intelligent Technologies
Volume 4, Issue 1, Jan-Jun 2024, pp. 41-54
DOI: 10.17492/computology.v4i1.2403
https://www.journalpressindia.com/cjacsit

Protection of Vehicular AdHoc Networks via Efficient Authentication and Message Encryption

Chindika Mulambia, Sudeep Varshney** and Amrit Suman****

ABSTRACT

Vehicular Networks (VANET) allow vehicles and other infrastructure in the network to communicate with each other about traffic management but also ensure safety on the roads and infotainment as users use roads. The wireless network architecture of a VANET brings about security concerns of security and privacy. This paper proposes a Protection of Vehicular Networks via Authentication Technique to address the issues of security and privacy. The method was implemented in a Linux environment running Ubuntu 20.04 and Python 3.12 was used for the model. The results show efficient vehicle authentication and message encryption with minimal delays as vehicle density increases, the model is compared to other models and displays lower delays. Enabling private and secure vehicular communications by this model facilitates deployment of Vanet applications that enhance road traffic and safety efficiency.

Keywords: *Vanet, Vanet Security, Vanet Authentication, Privacy Preservation, Pseudo Identities.*

1.0 Introduction

Vehicular networks normally called Vanets which stands for Vehicular Ad-Hoc Networks are networks that create links between vehicles and road side units and the main purpose is for communication.(Thamizhmaran, 2020) In a Vanet vehicles and road side units can share information on traffic status whether there’s congestion or road accident.(Choudhary & Pahuja, 2023) This network permits the following type of communications:

**Corresponding author; Student, Department of Computer Science and Engineering, Sharda University, Greater Noida, Uttar Pradesh, India (E-mail: chindikachitalo@gmail.com)*
***Associate Professor, Department of Computer Science and Engineering, Sharda University, Greater Noida, Uttar Pradesh, India (E-mail: sudeep.varshney@sharda.ac.in)*
****Assistant Professor, Department of Computer Science and Engineering, Sharda University, Greater Noida, Uttar Pradesh, India (E-mail: amrit.suman@sharda.ac.in)*

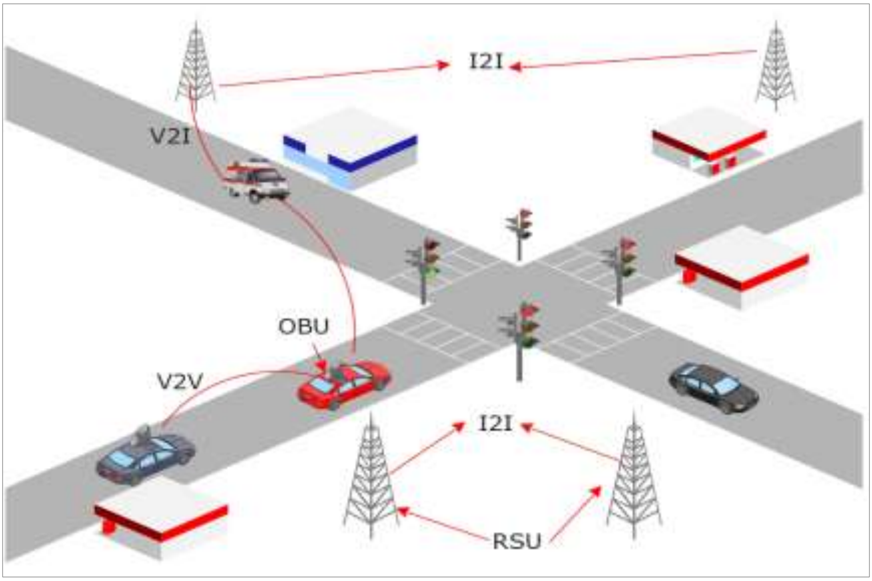
Vehicle to Vehicle(V2V): This is the connection between vehicles. Vehicles can share information like traffic status which are road accidents in that route or if there is congestion in the route. Each vehicle is equipped with an On-Board Unit that has the capacity to send and receive messages. It has limited storage capacity.(Mulambia *et al.*, n.d.)

Vehicle to Infrastructure(V2I): This is communication between vehicles and the Road Side Units. The road side units are usually placed by the road side and have higher computation capacity. They are able to provide connectivity to the vehicles in the network.(Shawky *et al.*, 2023)

Vehicle to Everything(V2X): This is communication of vehicles and everything in the vehicular networks. The vehicle can communicate to all the infrastructure in the network.

Figure 1 shows a simple VANET scenario which shows the different communications that exist in the network.

Figure 1: Simple VANET Scenario



Some of the characteristics of vehicular networks are as follows:

High Mobility: Vehicles in this network move very quickly and the connections made are very short or within a very short period of time and this changes the network dynamics.

Varying Vehicle Density: At a particular route they can be many vehicles or a few vehicles and this variation affects how the network will function. In other words, the network functionality is affected by the number of vehicles in that particular route.(Agrawal *et al.*, 2023)

Wireless Communication: In a vehicular network the vehicles communicate with each other using short range wireless technology which Dedicated Short Range Communication (DSRC) and Wireless Access for Vehicular Environments (WAVE). (Kumar *et al.*, 2022)

Autonomous: As already mentioned the vehicular network is dynamic and this makes the network self-reorganizing. (Kumar *et al.*, 2023)

This is the autonomous nature of the network and it does not rely on a fixed infrastructure.

Time-Sensitive Apps: The vehicular networks allow access to safety apps like collision avoidance. These need that data is sent quickly so that the network functions properly. (Hameed & Mahmoud, 2022)

The main objectives of the vehicular network is to manage traffic, improve road safety and provide infotainment so users are connected to the internet while they are on the move. The objectives of Vehicular Networks explained below:

Traffic Safety: This allows vehicles to share information on traffic status and also information on traffic accidents. This enhances safe driving for users.

Traffic Flow: Vehicles using real time data can plan routes and also traffic systems can be adjusted like traffic lights so that things move and ran smoothly. Infotainment: The users can enjoy access to the internet and also entertainment while they are on the road.

Autonomous Driving: Vehicles that are self-driving can then communicate with each other and also with the road side units and this makes autonomous driving safer.(Kumar & Singh, 2020)

In as much as there are many benefits of vehicular networks there are some attacks that affect them due to the nature of the network and certain requirements have to be met in order to mitigate these attacks. Closer look at some of the attacks that are found in Vehicular Networks:

Denial of Service (DoS): One of the common attacks found in a vehicular network is the DoS attack. In this attack a malicious vehicle can send false information that a particular road has been close due to an accident or congestion. This will make the legitimate vehicles not have access to that route so in other words denial of access to that particular road. The DoS attack can further be extended to Distributed Denial of Service attack (DDoS) in which different malicious vehicles at various locations launch the attacks.(Suman & Kumar, 2019)

Man in the Middle Attack (MITM): This attack involves the malicious user intercepting the vehicle-to-vehicle communication and then impersonates either vehicle in the communication. It does this in order to capture the messages that are being sent by the vehicles and in so doing is able to gather more information on the vehicles communicating and further alter the message that are being transferred by the vehicles.(Mulambia *et al.*, n.d.).

Sybil Attack: The attacker will create an illusion in the network by using multiple identities of the legitimate vehicles. The attacker will do this in order to dominate the whole network and then falsify the messages being sent in the network. This will confuse the legitimate entities in the network. (Kugali, 2020)

Some of the necessary requirements in vehicular networks so as to minimise the security attacks.

Authentication: Vehicles need to authenticate each other so as to avoid a malicious user from gaining access or impersonating a legitimate vehicle. Authentication is process in which a users' identity is verified before permitting that user to access the network resources. It is very necessary that vehicles authenticate each other so that malicious vehicles are identified.(Dong *et al.*, 2023)

Access Control: Access control is a process by which access to Network resources is limited only to the authorised entities. In order to protect the integrity of the network and thwart unwanted access then information should only be accessed by authorised nodes.

Availability: This is when the network resources are available for the users in the network. When the vehicles request safety apps then this are available for them as they request. Availability is one way to ensure that no denial of service is happening to the legitimate users.

Data Trust: Not all data that is being sent in the network is trusted. Data from different vehicles and infrastructure can be actually from malicious entities. The network needs to ensure that it is able to scrutinise the data that is being sent in the network so that it filters out the false information that is being sent from malicious devices.

Privacy: Due to the nature of a vehicular network it is very important to protect the real identities of users and also the whereabouts of these vehicles. This is done so that malicious users are not able to know the real identities of vehicle users and also not able to track the movements of the vehicles. Privacy is essential to so that continuous tracking does not expose sensitive information.(Haydari & Yilmaz, 2022)

Real-Time Restrictions: Some security applications and measures take time to process and this affects safety applications in that they can lag. A vehicular network requires fast responding applications in a scenario where time sensitive apps are being used. In as much as security is need it has to be balanced with response time.(Zhang *et al.*, 2022). These worries highlight how crucial security is for automotive networks. Guidelines for secure messaging and certificate management are provided by standards such as IEEE 1609 WAVE. The goal of ongoing research is to provide trustworthy data verification systems and energy-saving authentication techniques specifically for automotive networks. To get the most out of intelligent transportation networks and linked cars, strong security is essential.

1.1 Objectives of the study

- Propose a method that provides protection through authentication of vehicular network and addresses the issues of privacy and security in VANETs.
- To enable secure and private vehicular communications by the proposed model, facilitating deployment of VANET applications that in turn enhance road traffic efficiency and safety.

2.0 Review of Literature

A comprehensive review was done on different authentication approaches in VANETs. An approach is proposed by Sungjin,Yu et al that uses a vehicle server (VS) for key distribution and authentication(Yu *et al.*, 2020). Pravin et al has a Lattice Based Ring Signature (LRMA) that forms a ring of authenticated vehicles. In the ring each vehicle generates their own key pair and send messages the recipient is able to verify the message from the sender because they are in one ring. Drawback is that as more vehicles join the ring delay also increases. A proxy vehicle is introduced in the approach that is proposed by Liu *et al.* (2020). The proxy vehicle authenticates with certification authority and also authenticates with the RSU after authentication it jointly generates group keys that will be used for message signing and authentication. Vehicles are provided with pseudo IDs that which preserve the privacy but the drawback is that there is decryption overhead. (Chen *et al.*, 2023) Proposes an approach that leverages the use of Blockchain technology to offer tamper resistant and immutable information transactions. Once a transaction has been saved to the blockchain then it makes it harder for malicious users to change the contents in the Blockchain. The drawback with the method is higher computational time.

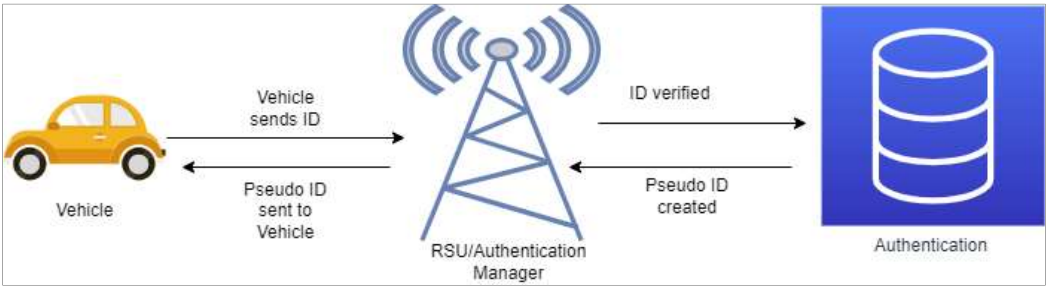
Aghabagherloo *et al.* (2022) uses TA to authenticate vehicles and provides pseudo IDs to the vehicles, it removes continued reliance on RSU and TA. Each message sent is timestamped but this also causes delay. (Luo & Zhou, 2022)Luo et al approach utilizes master keys that are chosen by the TA and computes key pairs and pseudo IDs. When a message is sent the recipient, vehicle checks the timestamp on the message and verifies that message based on that. Approach drawback is computation overhead. The review conducted leads to the proposed approach that preserves the privacy of the vehicles as this is very essential in a VANET. The method is a an Efficient Authentication and Message Encryption Technique that authenticates vehicles before they are given access into the VANET.

3.0 Research Methodology

3.1 Research design

The proposed approach is a Protection of Vehicular Networks via Efficient Authentication and Message Encryption Technique that authenticates vehicles using their vehicle ID. It takes input of the vehicle ID and this is presented to the Authentication Manager which verifies this ID against a list of known IDs as presented in Figure 2. Once authenticated the Vehicle is given access to the VANET and then is permitted to transmit messages in the network. Each of the messages is encrypted with Elliptic Curve Cryptography (ECC).

Figure 2: Proposed Method



3.2 Sources of data

The proposed method takes its real traffic data of India from OSM wizard and the data is simulated in SUMO.

Figure 3 shows the traffic collection and Figure 4 shows the simulation of the traffic. Figure 3 shows the extraction of the Real traffic from the busy streets of India and what is captured is only vehicle traffic. Figure 4 shows the traffic simulation in SUMO and simulated data was then used in the model.

Figure 3: Real traffic extraction

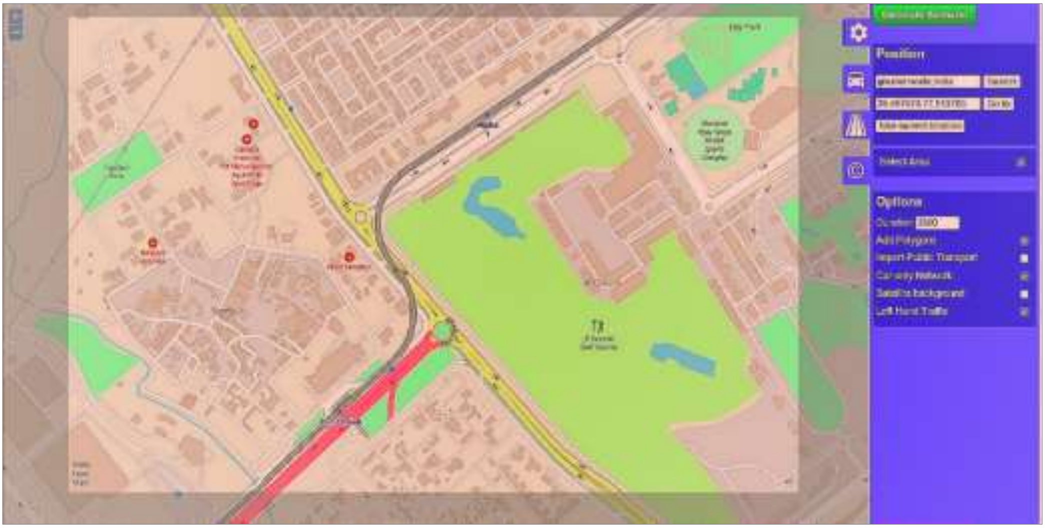
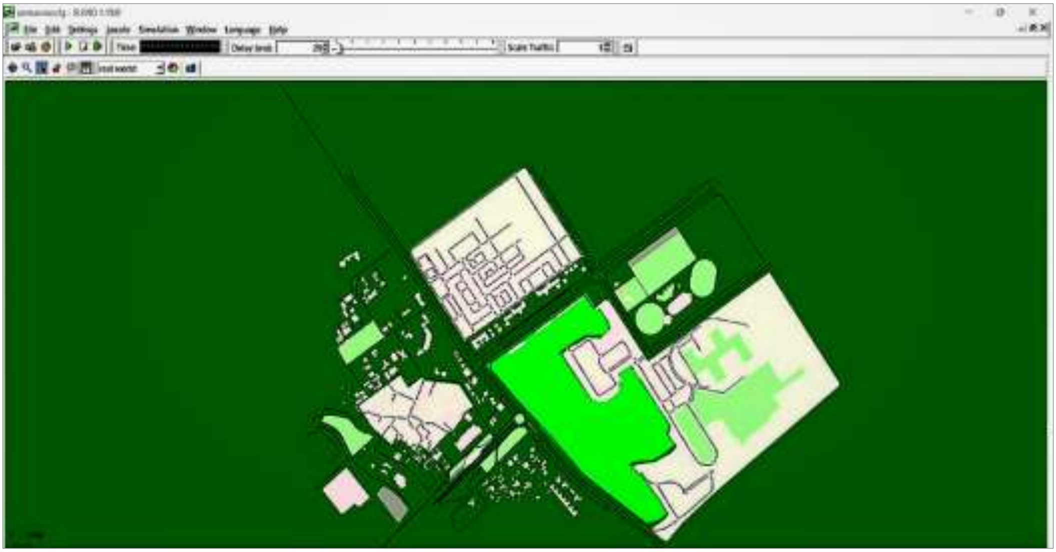


Figure 4: Traffic simulation in SUMO



4.0 Results and Discussion

The method was implemented in a Linux environment running Ubuntu 20.04 and Python 3.12 was used, an Intel core i7 processor 13th Gen. For security analysis the model is able to achieve the following:

Privacy Preservation: The method provides pseudo IDs for each vehicle once it is authenticated. This preserves the privacy of the vehicles in that the pseudo ID cannot be traced to the real identity of the vehicles.

Message Authentication: Each of the messages that are sent within the VANET are signed using the Pseudo ID and encrypted using ECC which is secure. Any message that cannot be verified is discarded.

To verify the performance of the model the following was taken into consideration which is time taken to complete a particular task given. Average delay in completing a task was calculated in milliseconds(ms).

In the vehicle authentication, a vehicle presents its ID and then the authentication manager verifies that ID and authenticates this vehicle. The performance measure looks at the time the vehicle arrives until the time it is verified and given a Pseudo ID. Another thing to the number of vehicles requesting authentication at a given time. Number of vehicles at particular time is calculated using the following formula:

TR_n is for the time received of the nth vehicle. For example if we want to find number of vehicle from a time slot lets say 0-200ms then any vehicle whose TR is within that time slot is counted if it does not satisfy then it is discarded.

$$\begin{cases} 1 \; if \; 0 < x < 200 \\ 0 \; otherwise \end{cases} \qquad \ldots(1)$$

Thereafter the summation is taken and N represents the number of vehicles that have been found as shown in the formula below:

$$N = \sum_1^i I(TR_i) \qquad \ldots(2)$$

Average delay in authentication is calculated using the following parameters:

Time Started = Ts

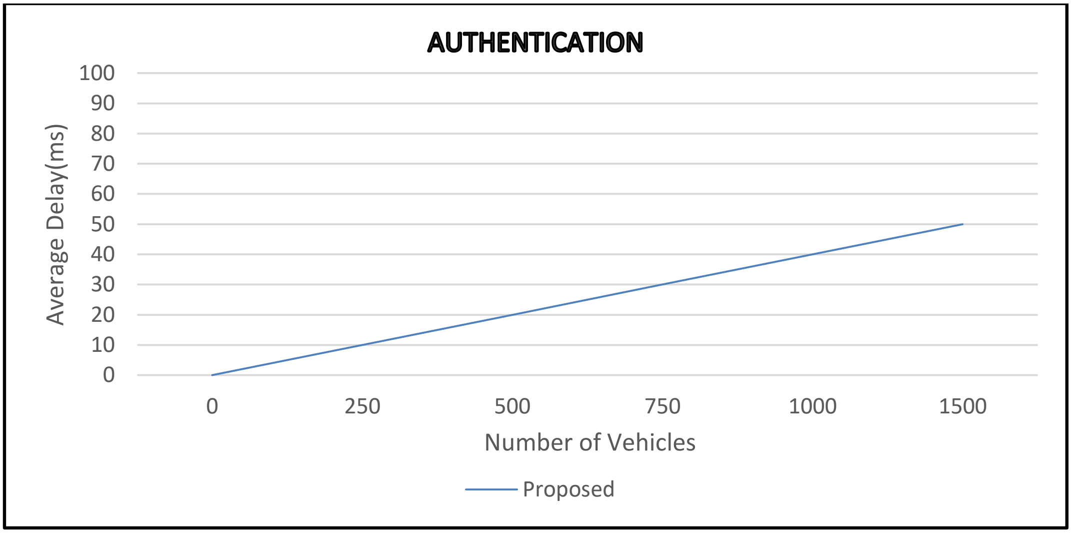
Time Finished = TF

Work Size = WS

$$\frac{TF-TS}{WS} \qquad \ldots(3)$$

The Figure 5 shows the authentication delay as vehicles increase that require authentication. From the results it was observed that the delay increases as the number of vehicles increase and this is expected.

Figure 5: Authentication Delay of Vehicles



The proposed model is compared with the HBPS and CPPA models because they provide pseudo IDs as well and have a similar architecture to the proposed model. When a vehicle is authenticated it is permitted to send messages in the network. The following formula has to be satisfied before the average delay in encryption of messages:

$$\begin{cases} \frac{TF-TS}{WS} & if\ S = 1 \\ 0\ otherwise\ if\ S = 0 \end{cases} \qquad \ldots(4)$$

Status is represented as S. If a vehicle is authenticated it returns 1 and if not then it returns 0.

To calculate time taken to encrypt the following is considered:

Encryption Started = Encry S

Encryption Finished = Encry F

For a given Message C the time taken to encrypt that message will be calculated as follows:

Encry F(C)-Encry S(C) …(5)

Average delay of message encryption is calculated as follows:

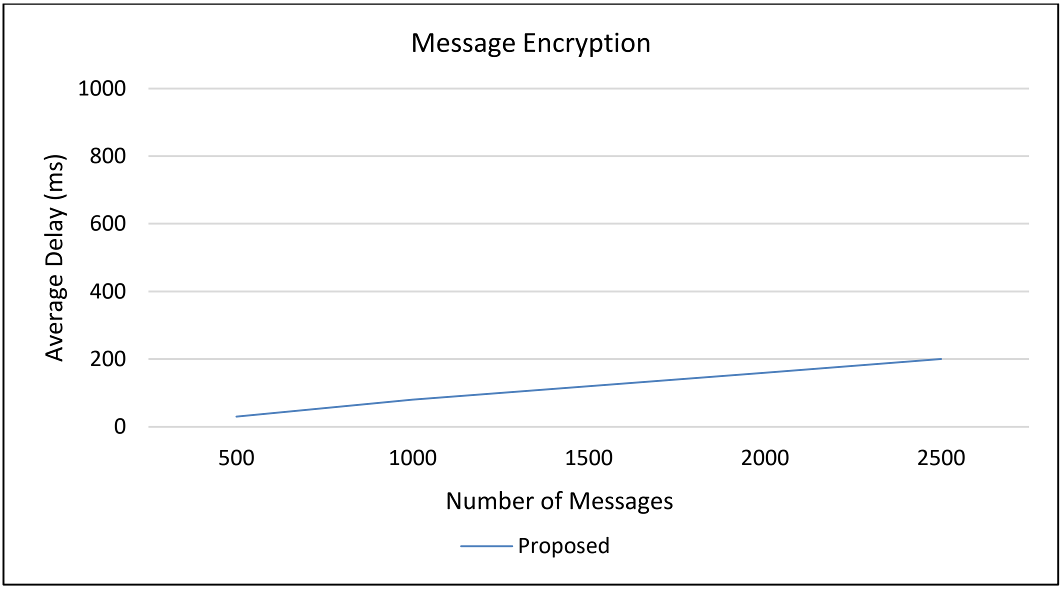
$$\sum_{1}^{c} \frac{Encry\ F(C) - Encry\ S(C)}{WS * N} \qquad \ldots(6)$$

In the formula, N represent the Number of vehicles and WS is the work size.

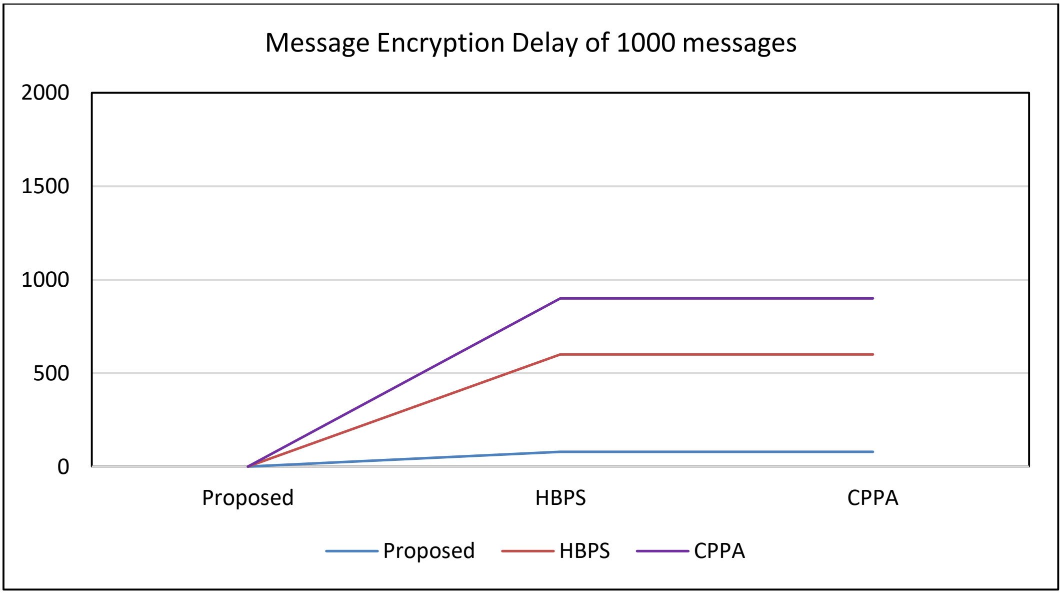
Figure 6 shows the average delay in encrypting messages sent from different vehicles.

Figure 6: Message Encryption Delay

(a)

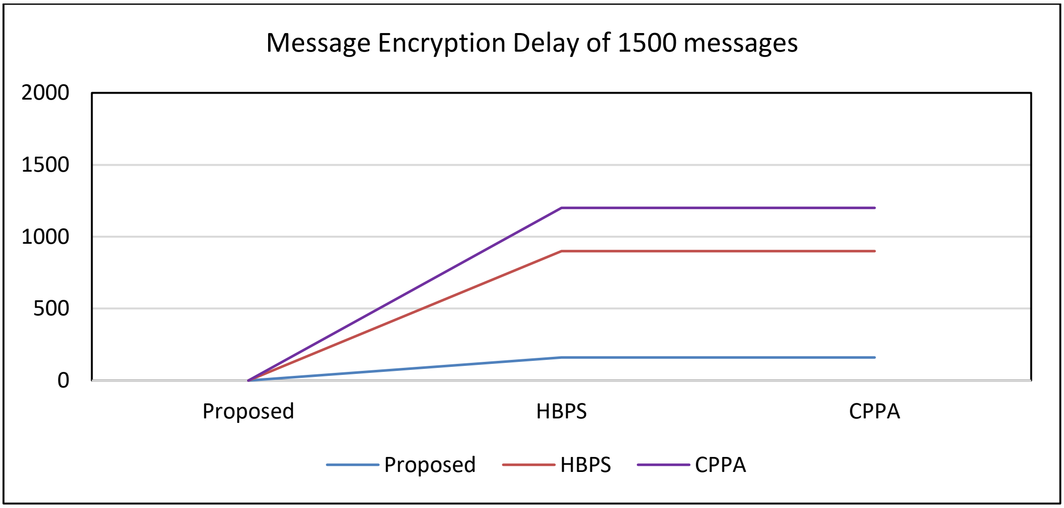


(b)

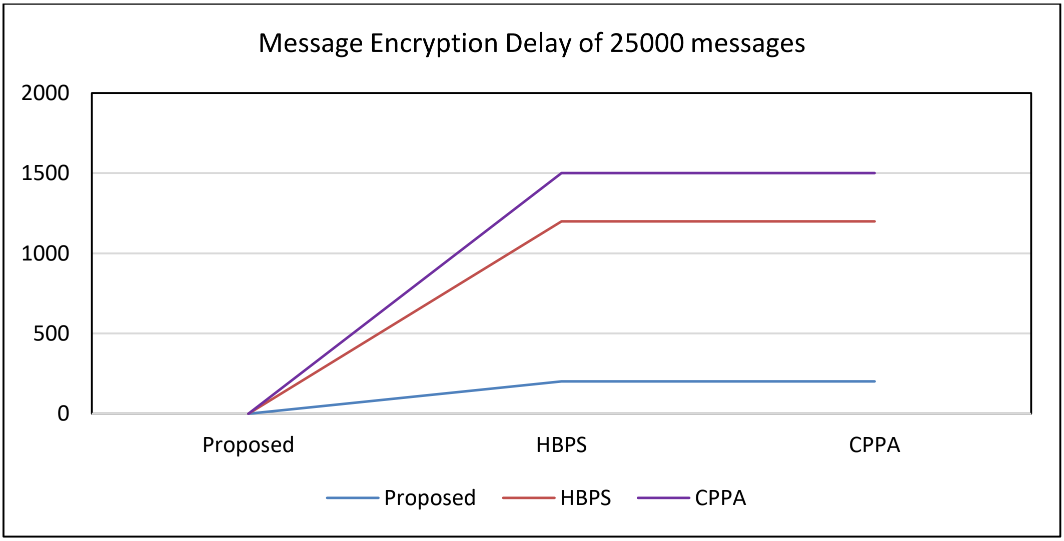


.

(c)



(d)



As vehicles increase then the number of messages that require encryption increase. Figure 6(a) shows the results of message encryption delay of the proposed model and it shows that delay increases as messages increase. Figure 6(b),(c) and (d) show the model being compared to the other models which are HBPS and CPPA. From the results the proposed model encrypts messages faster than the other models.

5.0 Conclusion and Implications

The paper presented a privacy preservation authentication scheme that secures communications in VANETs. The model authenticates vehicles before they are given access to the VANET and then provides them with a pseudo-ID that will be used for communication as they send messages and this enhances authenticity and confidentiality. The performance evaluation shows that unlike other approaches the model displays lower computational delay. Facilitating private and secure communications in VANET enables effective deployment of VANET applications for traffic efficiency and safety. For future work the model will be extended to provide tamper proof key storage and integrate decentralised frameworks to eliminate reliance on authentication manager.

References

Aghabagherloo, A., Delavar, M., Mohajeri, J., Salmasizadeh, M., & Preneel, B. (2022). An efficient and physically secure privacy-preserving authentication scheme for vehicular Ad-hoc NETworks (VANETs). *IEEE Access*, *10*, 93831–93844. Retrieved from https://doi.org/10.1109/ACCESS.2022.3203580

Agrawal, R., Kumar, A., & Singh, S. (2023). Vehicular Ad Hoc betwork: Overview, characteristics, and applications. *AIP Conference Proceedings*, *2721*(1), 070057. Retrieved from https://doi.org/10.1063/5.0154151

Chen, B., Wang, Z., Xiang, T., Yang, J., He, D., & Choo, K.-K. R. (2023). BCGS: Blockchain-assisted privacy-preserving cross-domain authentication for VANETs. *Vehicular Communications*, *41*, 100602. Retrieved from https://doi.org/10.1016/j.vehcom.2023.100602

Choudhary, D., & Pahuja, R. (2023). Awareness routing algorithm in vehicular ad-hoc networks (VANETs). *Journal of Big Data*, *10*(1), 122. Retrieved from https://doi.org/10.1186/s40537-023-00742-3

Dong, S., Su, H., Xia, Y., Zhu, F., Hu, X., & Wang, B. (2023). A comprehensive survey on authentication and attack detection schemes that threaten it in vehicular Ad-Hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, *24*(12), 13573–13602. Retrieved from https://doi.org/10.1109/TITS.2023.3297527

Hameed, A. G., & Mahmoud, M. S. (2022). Vehicular Ad-hoc Network (VANET) – A Review. *2022 Iraqi International Conference on Communication and Information Technologies (IICCIT)*, 367–372. Retrieved from https://doi.org/10.1109/IICCIT55816.2022.10010554

Haydari, A., & Yilmaz, Y. (2022). RSU-based online intrusion detection and mitigation for VANET. *Sensors, 22*(19). Retrieved from https://doi.org/10.3390/s22197612

Kumar, S., Jailia, M., & Varshney, S. (2022). Improved YOLOv4 approach: A real time occluded vehicle detection. *International Journal of Computing and Digital Systems, 11*(1), 489–497. Retrieved from https://doi.org/10.12785/ijcds/120139

Kumar, S., Jailia, M., Varshney, S., Pathak, N., Urooj, S., & Abd Elmunim, N. (2023). Robust vehicle detection based on improved you look only once. *Computers, Materials & Continua*, *74*(2), 3561–3577. Retrieved from https://doi.org/10.32604/cmc.2023.029999

Kumar, S., & Singh, J. (2020). Internet of vehicles over vanets: Smart and secure communication using IoT. *Scalable Computing: Practice and Experience*, *21*(3). Retrieved from https://doi.org/10.12694/scpe.v21i3.1741

Liu, X., Huang, H., Xiao, F. & Ma, Z (2020). A blockchain-based trust management with conditional privacy-preserving announcementscheme for VANETs. *IEEE Internet of Things Journal, 7*(5), 4101-4112.

Luo, M., & Zhou, Y. (2022). An efficient conditional privacy-preserving authentication protocol based on generalized ring signcryption for VANETs. *IEEE Transactions on Vehicular Technology*, *71*(9), 10001–10015. Retrieved from https://doi.org/10.1109/TVT.2022.3179371

Mulambia, C., Varshney, S., & Suman, A. (n.d.). Privacy preserving blockchain based authentication scheme for Vanet. *Engineered Science*. Retrieved from https://doi.org/10.30919/es1073

Kugali, S.N. (2020). Vehicular ADHOC network (VANET): A brief knowledge. *International Journal of Engineering Research and V9*(06), IJERTV9IS060784. Retrieved from https://doi.org/10.17577/IJERTV9IS060784

Shawky, M. A., Usman, M., Imran, M. A., Abbasi, Q. H., Ansari, S., & Taha, A. (2023). Adaptive chaotic map-based key extraction for efficient cross-layer authentication in VANETs. *Vehicular Communications, 39*, 100547. Retrieved from https://doi.org/10.1016/j.vehcom.2022.100547

Suman, A. & Kumar, C. (2019). Implementation of MAC protocol with enhanced security features in VANET. *International Journal of Vehicle Information and Communication Systems*, *4*(1), 78–90. Retrieved from https://doi.org/10.1504/IJVICS.2019.099068

Thamizhmaran, K. (2020). A review of vehicular Ad hoc network broadcasting techniques. *Journal of Sensor Research and Technologies, 2*(3).

Yu, S., Lee, J., Park, K., Das, A. K., & Park, Y. (2020). IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment. *IEEE Access*, *8*, 167875–167886. Retrieved from https://doi.org/10.1109/ACCESS.2020.3022778

Zhang, L., Kang, B., Dai, F., Zhang, Y., & Liu, H. (2022). Hybrid and hierarchical aggregation-verification scheme for VANET. *IEEE Transactions on Vehicular Technology*, *71*(10), 11189–11200. Retrieved from https://doi.org/10.1109/TVT.2022.3189540