

Privacy-preserving authentication approach for vehicular networks

Chindika Mulambia, Sudeep Varshney, Amrit Suman

Department of Computer Science and Engineering, Sharda University, Greater Noida, India

Article Info

Article history:

Received Oct 21, 2023

Revised Feb 25, 2024

Accepted Mar 16, 2024

Keywords:

Authentication manger

Message authentication

Privacy

Road side unit

Vehicular networks

ABSTRACT

Vehicle AdHoc networks have an important role in intelligent transport systems that enhance safety in road usage by transmitting real traffic updates in terms of congestion and road accidents. The dynamic nature of the vehicular AdHoc networks make them susceptible to attacks because once malicious users gain access to the network they can transform traffic data. It is essential to protect the vehicular ad hoc network because any attack can cause unwanted harm, to solve this it is important to have an approach that detects malicious vehicles and not give them access to the network. The proposed approach is a privacy preserving authentication approach that authenticates vehicles before they have access to the vehicular network thereby identifying malicious vehicles. The model was executed in docker container that simulates the network in a Linux environment running Ubuntu 20.04. The model enhances privacy by assigning Pseudo IDs to authenticated vehicles and the results demonstrate effectiveness of the solution in that unlike other models it boasts faster authentication and lower computational overhead which is necessary in a vehicular network scenario.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Chindika Mulambia

Department of Computer Science and Engineering, Sharda University

Greater Noida, India

Email: chindikachitalo@gmail.com

1. INTRODUCTION

Transportation is key in improving the social and economic development of people because it serve as a means of movement from one point to another on daily basis [1]. The increase in usage of transportation has now causes many accidents so to improve safety and efficiency in transportation intelligent transport systems (ITS) was developed to achieve the aim [2]. One key element in ITS is vehicular ad-hoc network (VANET), a VANET is a network of vehicles that are continuously mobile and it enhances safety in transportation by sending messages about the current traffic conditions, the conditions can be whether a particular route has traffic congestion or an accident has taken place [3], [4]. Once the other vehicles receive these messages, they can decide to avoid that route and use another route. The main components in a VANET are on board unit (OBU) which is found in a vehicle, it has the capacity to send and receive messages. Another component is road side unit (RSU) which has high computational capacity and provides connectivity to the vehicles in the network [5]. The VANET can also have a certification authority (CA) and trusted authority (TA) which highly trusted government agencies that have real information of the vehicles and also provide certificates to the OBUs and RSUs. The main types of communication in a VANET are:

- Vehicle to vehicle (V2V): In this communication vehicles transmit messages to each other on the traffic status like congestion or road accidents [6].

- Vehicle to infrastructure (V2I): This communication involves vehicle to RSU or other infrastructure in the VANET.
- Vehicle to everything (V2X): Vehicle communicates with everything in the VANET [7].

Figure 1 shows a scenario whereby a road accident had occurred and a vehicle reports to the other vehicle in the network of the accident. The other vehicle receives the messages and decides whether to stop or change route.



Figure 1. Accident announcement in a VANET scenario

A VANET structure is a wireless network in which all vehicles within the proximity of the network can connect as such this raises some security concerns because malicious vehicles can join the network and transmit false messages about traffic conditions and also alter the messages that are being sent in the network which in turn can cause a denial of service attack because the legitimate vehicles can be denied access to a certain route [8]–[10]. The malicious vehicles can also find out the real identities of the vehicles and create an illusion of those identities causing a sybil attack [11], [12]. Malicious vehicles can also trace the location of vehicles as they move around in the network and this poses as a security threat to the legitimate vehicles.

That being said securing the VANET is very essential through authentication and privacy schemes; authentication is a process that verifies an entity before they are permitted to access a particular network's or system's resources [13]. In this case the identity of the vehicles will be verified and once authenticated that particular vehicle will be given access to the network resources [14], [15]. Authentication will be the initial step to prevent malicious vehicles from accessing the VANET and this will prevent the malicious vehicles from transmitting messages because they have not been given access to the network [16], [17]. Messages are always transmitted in a VANET as mentioned earlier so it is important that these messages are verified and authentication helps in verifying the source of the messages and also confirms the integrity of these messages [18], [19]. Privacy in a VANET also promotes security, it provides anonymity by concealing the real identity of the vehicles so that malicious users don't track these legitimate vehicles or create an illusion of these vehicles [20].

Extensive research was conducted on existing authentication schemes in VANETs. Mundhe *et al.* [21] proposes an approach called lattice-based ring signature (LRMA) which forms a ring of authenticated vehicles that generate their own key pair. The sending vehicle will produce a signature that it will use on the message and the recipient vehicles verify the signature when they receive this message. Once verified the vehicles accept the message if not verified, they reject the message. Approach drawback is that since each vehicle creates its own signature it is unclear if all the vehicles use the same parameters making some signatures to be intercepted. Hybrid proxy based scheme (HPBS) an approach by Liu *et al.* [22] that uses a proxy vehicle which is verified by the RSU; the main duty of the proxy vehicle is to manage the messages that are being transmitted in its group. Every message transmitted in the group goes through the proxy vehicle for authentication, once authenticated the proxy transmits the message to the intended recipient. Drawback is computation cost on the proxy vehicle. Ullah *et al.* [23] discusses extensively on elliptic curve and how it enhances security. This is applied in VANETs by Rajkumar and Kumar [24] elliptic curve public key cryptography approach uses which provides vehicles with primary and secondary Pseudo IDs (PPID/SPID). When a sender vehicle sends a message it calculates a signature with their primary and secondary Pseudo ID. The other vehicles in the VANET have a copy of the sender's SPID so they use it to verify the signature if they can verify the signature then the message is accepted otherwise message is rejected. The drawback of the approach is that the SPID is only used once when a vehicle sends a message for them to send another message, they have to request a new SPID which increases computational cost.

Feng *et al.* [25] divides the VANET into domains that are managed by the RSUs and does this using the law enforcement authority (LEA). The RSUs distribute vehicle certificates they are authorised to do this

by the LEA. The RSU's periodically updates the certificate database and messages sent in the domain are verified by it. Messages in the domain are signed using an algorithm that uses a Pseudo certificate that cannot be traced to the original certificate. Drawback of the approach is that the certificate management. Real or random model (ROR) by Lee *et al.* [26] uses a TA that authenticates and RSUs and generates session keys that are used by domain in the VANET. Each domain is managed by the RSU and vehicles in the same domain use a shared session key. Drawback is verification of individual vehicle since they are all using same session key. From the review conducted most of the schemes are complex and they increase the computation cost while also causing delay in the authentication process and some of the schemes do not preserve user privacy which is key in a VANET. These reasons lead to the proposed approach which is a privacy preserving authentication approach; vehicles present the vehicle ID to the authentication manager and this is verified against the list of known Vehicle IDs. Once a vehicle is verified it is provided with Pseudo ID that will be used for communication in the VANET. The Pseudo ID preserves the privacy of the vehicles as this Pseudo ID is not linked to the real identity of the vehicle.

2. METHOD

The proposed method is a non-complex architecture that has an RSU which is an authentication manager and vehicles present their IDs and the authentication manager verifies that vehicle. Once the vehicle is verified, it is provided with a Pseudo ID that the vehicle now uses to send a message. Any vehicle not verified is not permitted to transmit messages in the network. Real traffic is collected from India using OSM wizard and this is simulated using simulation of urban mobility SUMO. The extracted data is implemented in the model so as number of vehicles requiring authentication at a particular instance is verified with real data. The parameters used to verify performance are time taken to complete a task at a given instance; focus is time vehicle arrives for authentication, time the vehicle is authenticated, start time of encryption and end time of encryption. The results are observed in docker container. Figure 2 shows the proposed method that has a vehicle that sends its ID to the authentication manager which authenticates the vehicle and once authenticated supplies it with a Pseudo ID. Figure 3 shows the flow of data in the proposed method; a vehicle will submit its ID to the RSU which also acts as the authentication manager and if that particular ID is verified it will be given a Pseudo ID then the particular vehicle is permitted to transmit messages.

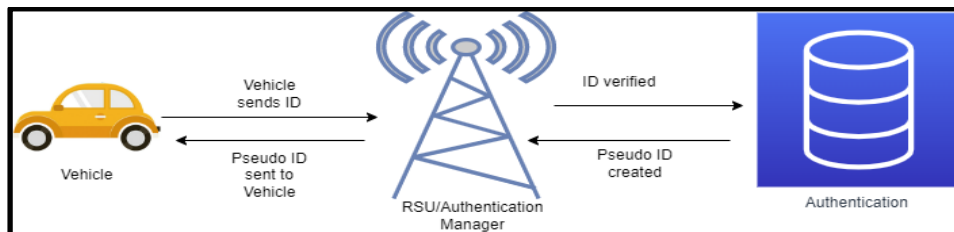


Figure 2. Proposed method system model

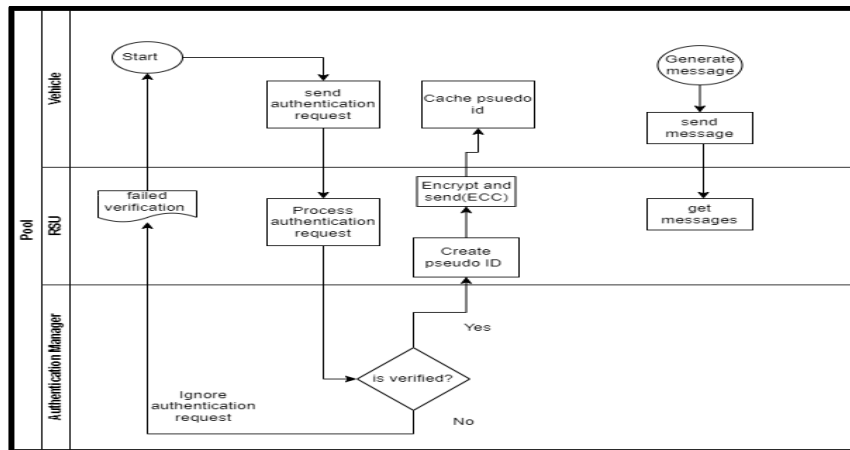


Figure 3. Proposed method data flow

Figure 4 shows the extraction of real time data from busy streets in India. OSM wizard was used as shown in the figure and after the data was extracted it was run in SUMO shown in Figure 5. Sumo simulated the traffic and the data was then used in the model. Table 1 shows the steps in the vehicle authentication process until the vehicle is authenticated and later on given a Pseudo ID.



Figure 4. Real traffic extraction

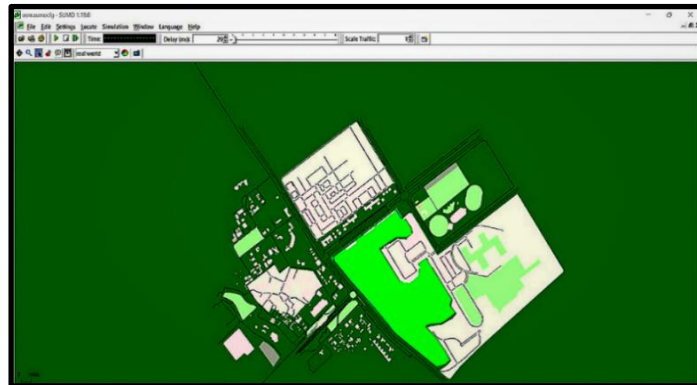


Figure 5. Real traffic simulation run in SUMO

Table 1. Vehicle authentication process steps

No	Entity	Authentication Process
1	Vehicle	Authentication manager:<ViD >
2	Authentication Manager ^{verf}	ViD:<Verify (ViD)
3	Authentication Manager ^{cal}	Pseudo iD:< (PiD ViD)
4	Authentication Manager	Vehicle:<PiD >

The connection of a vehicle has the following steps: Step 1: authentication manager receives Vid from the vehicle. Step 2: the authentication manager then verifies the id of the vehicle. Step 3: a Pseudo ID is generated for the vehicle. Step 4: the Pseudo ID is transmitted to the vehicle. Once the vehicle is authenticated it will then be permitted to send a message M about traffic conditions. The steps are shown in Table 2. Step 1: a message M is generated by the vehicle and transmitted to the RSU. Step 2: RSU verifies the Pseudo ID that has signed the message. Step 3: once Pseudo ID is verified then the message is accepted and stored.

Table 2. Steps for sending messages

No	Entity	Message sending process
1	Vehicle (Pseudo ID)	RSU:<(M Pseudo ID >
2	RSU ^{verify}	Pseudo ID:< (M Pseudo ID)>
3	RSU ^{store}	< (M Pseudo ID)>

3. RESULTS AND DISCUSSION

The proposed model, implemented in Python 3.12, ran on Ubuntu 20.04 within a Linux environment. It utilized a Docker container to simulate the network, ensuring reproducible simulations and enhancing portability across systems.

3.1. Security analysis

Preservation of Privacy: vehicles once authenticated are given a Pseudo ID which cannot be traced to the real ID of the vehicles. As vehicles send messages in the network, they use this Pseudo ID and this prevents malicious users from tracing the real ID of the vehicle. Message authentication: each message transmitted is encrypted and also the message is signed with the Pseudo ID of the user. Any message signed with an ID that is not known in the VANET will be rejected. Messages are authenticated due to encryption and the Pseudo ID signature.

3.2. Performance analysis

Performance is measured in milliseconds (ms) by calculating the average delay that it takes to authenticate a vehicle and provide it with a Pseudo ID. Number of vehicles requesting authentication in an instance for example 100ms. TR_i is for the time received of the i^{th} vehicle. Number of vehicles requesting authentication is calculated as follows:

$$\begin{cases} 1 & \text{if } 0 < x < 100 \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

$$N = \sum_1^i I(TR_i) \tag{2}$$

N represents the Number of vehicles requesting authentication at a particular time. For each vehicle in the network the time received is checked to be within that instance. If $0 < TR_i < 100$ then 1 is returned as a count to the number of vehicles if it does not satisfy the function then 0 is returned. To calculate how long it takes to authenticate a vehicle the following parameters; time started (T_s), time finished (T_F), and work size (WS) were used (3).

$$\frac{T_F - T_S}{WS} \tag{3}$$

Figure 6 shows the authentication process of the model with Figure 6(a) showing the simulation of the system status before authentication starts and after it has started. From the simulation in Figure 6(a) it shows the time is 0ms when authentication process has not yet started, and the starts to increase from 1 ms as more vehicles are authenticated. Similarly, the line graph in Figure 6(b) displays when the number of vehicles increase then the average delay also increases which is expected.

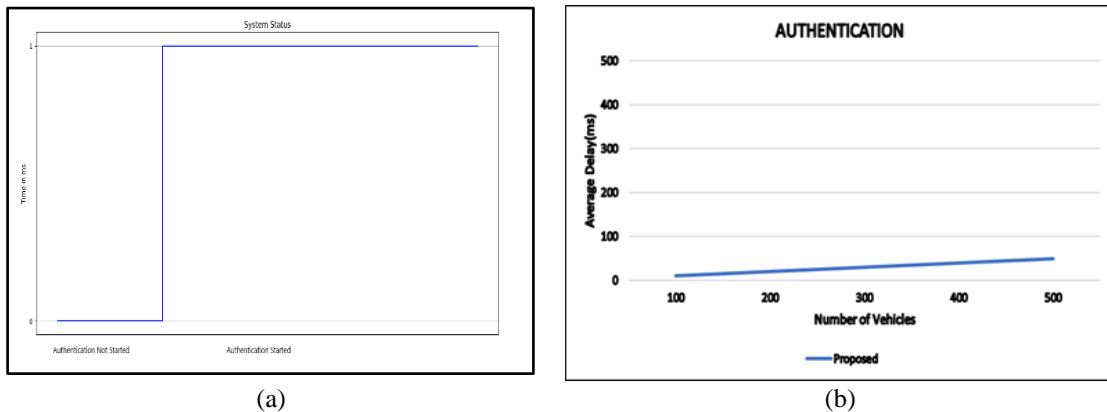


Figure 6. Depiction of simulation process and line graph illustration the authentication delay of model (a) simulation of system before and after started and (b) authentication the average delay

The proposed model is compared to HPBS and SEPPA because the schemes are similar to the proposed scheme in terms of encryption and that they all provide Pseudo IDs to the vehicles once authenticated. After a vehicle is authenticated, it will be given a Pseudo ID and then the vehicle can send a message that will be encrypted. The function to calculate how long it takes to encrypt is described as follows: Status=S. The following function has to be satisfied before the encryption time is calculated.

$$\begin{cases} \frac{TF-TS}{WS} & \text{if } S = 1 \\ 0 & \text{otherwise if } S = 0 \end{cases} \tag{4}$$

Once a vehicle is authenticated it S returns a value of 1. Similarly, if a vehicle is not authenticated S returns 0. If S returns 1 then the formula to calculate how long it takes to encrypt has to take the following into consideration. The time the encryption started and the time it ended. Encryption Started=Enc S. Encryption. Finished=Enc F. For a given Message M the time taken to encrypt that message will be calculated as follows:

$$Enc F(M)-Enc S(M) \tag{5}$$

to calculate the average time of encryption for multiple messages then we use the following formula:

$$\sum_{1}^m \frac{Enc F(M)-Enc S(M)}{WS*N} \tag{6}$$

where WS is the work size as mentioned above and N is the number of vehicles sending messages.

Figure 7 shows the delay of message encryption of the proposed scheme after vehicles have been authenticated. Number of messages is increased as vehicles increase in the VANET; in Figure 7(a) shows the proposed model’s results as the messages increase due to number of vehicles. Figure 7(b) compares the model with HBPS and SEPPA over 1,000 messages, Figures 7(c) and 7(d) shows comparison over 1500 and 2500 messages respectively. From the results the proposed scheme is faster because it does not provide a new Pseudo ID for each sent message while the other schemes provide a new Pseudo ID for each sent message increasing the computational overhead. In Table 3, the comparison of the proposed method with the existing methods in term of authentication methods, computational overhead, message authentication, privacy preservation, authentication speed, and complexity of the authenticity architecture.

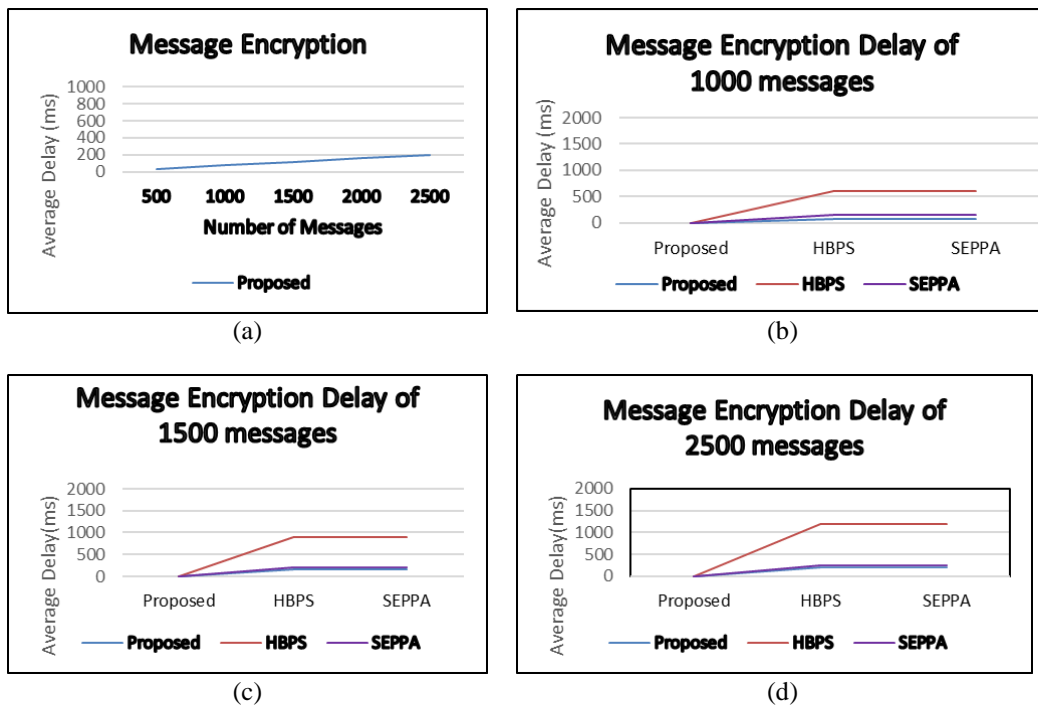


Figure 7. Illustrates the encryption delay of messages comparing the delay for varying message quantities in different models

Table 3. Comparison of methodology with existing methods

Criteria	Proposed approach	HPBS	SEPPA
Authentication method	Pseudo ID assignment by authentication manager	Proxy vehicle verification by RSU	Primary and secondary Pseudo IDs by EC PKC
Computational overhead	Lower than alternative methods	Higher due to proxy vehicle computation	Higher due to frequent SPID requests
Message authentication	Pseudo ID signature	Proxy-based verification of Pseudo ID	EC PKC Signature with primary and secondary IDs
Privacy preservation	Assigns pseudo-IDs to vehicles	Limited privacy as proxy vehicles manages groups	Uses primary and secondary Pseudo IDs
Authentication speed	Faster due to single pseudo-ID assignment	Slower due to proxy vehicle verification	Slower due to frequent SPID requests
Complexity of the authentication architecture	Non-complex	Complex due to proxy vehicle involvement	Complex due to EC PKC and SPID management

4. CONCLUSION

Authentication plays a pivotal role in network security by thwarting unauthorized access attempts. Once a malevolent vehicle is identified, it mitigates the issue of malevolent nodes disseminating harmful messages. In the unlikely event that a malicious vehicle manages to send messages in the VANET, the implemented model promptly rejects it because every message received is also authenticated using the Pseudo ID; As such the message will not be accepted. The model demonstrates faster authentication in comparison to other models because it only uses one Pseudo ID for a vehicle at a particular time. Future research will focus on renewal of Pseudo ID after a particular period of time while ensuring faster computation time. Pseudo ID renewal is necessary as prolonged usage of the ID can lead to tracking by Malicious users.




REFERENCES

- [1] M. Tantaoui, M. Moukhafi, and I. Chana, "Big data vehicle density management in vehicular ad-hoc network," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 33, no. 1, p. 314, Jan. 2024, doi: 10.11591/ijeecs.v33.i1.pp314-323.
- [2] A. A. Ganin, A. C. Mersky, A. S. Jin, M. Kitsak, J. M. Keisler, and I. Linkov, "Resilience in intelligent transportation systems (ITS)," *Transportation Research Part C: Emerging Technologies*, vol. 100, pp. 318–329, 2019, doi: 10.1016/j.trc.2019.01.014.
- [3] M. Ali Zuhdi Rosli, S. F. A. Razak, and S. Yogarayan, "5G handover issues and techniques for vehicular communications," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 32, no. 3, p. 1442, Dec. 2023, doi: 10.11591/ijeecs.v32.i3.pp1442-1450.
- [4] T. Chatterjee, R. Karmakar, G. Kaddoum, S. Chattopadhyay, and S. Chakraborty, "A survey of VANET/V2X routing from the perspective of non-learning- and learning-based approaches," *IEEE Access*, vol. 10, pp. 23022–23050, 2022, doi: 10.1109/ACCESS.2022.3152767.
- [5] M. R. Ali, M. F. A. Kadir, A. F. A. Abidin, A. R. Mamat, and M. A. Mohamed, "Review of random early detection optimization for congestion control in vehicular ad hoc networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 32, no. 1, pp. 449–457, 2023, doi: 10.11591/ijeecs.v32.i1.pp449-457.
- [6] R. Kalkundri, R. Khanai, and P. Kalkundri, "Enhancing safety communication in autonomous vehicles with hybrid elliptic curve digital signatures," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 32, no. 2, p. 1177, Nov. 2023, doi: 10.11591/ijeecs.v32.i2.pp1177-1186.
- [7] E. Farsimadan, F. Palmieri, L. Moradi, D. Conte, and B. Paternoster, "Vehicle-to-everything (V2X) communication scenarios for vehicular ad-hoc networking (VANET): an overview," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12956 LNCS, 2021, pp. 15–30. doi: 10.1007/978-3-030-87010-2_2.
- [8] M. A. R. Bae, L. Simpson, E. Foo, and J. Pieprzyk, "The security of '2FLIP' authentication scheme for VANETs: attacks and rectifications," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 101–113, 2023, doi: 10.1109/OJVT.2022.3217552.
- [9] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: communication, applications and challenges," *Vehicular Communications*, vol. 19, p. 100179, Oct. 2019, doi: 10.1016/j.vehcom.2019.100179.
- [10] L. Kim, "Cybersecurity: ensuring confidentiality, integrity, and availability of information," 2022, pp. 391–410. doi: 10.1007/978-3-030-91237-6_26.
- [11] X. Feng, C. yan Li, D. xin Chen, and J. Tang, "A method for defending against multi-source sybil attacks in VANET," *Peer-to-Peer Networking and Applications*, vol. 10, no. 2, pp. 305–314, 2017, doi: 10.1007/s12083-016-0431-x.
- [12] S. Masood *et al.*, "Detecting and preventing false nodes and messages in vehicular ad-hoc networking (VANET)," *IEEE Access*, vol. 11, pp. 93920–93934, 2023, doi: 10.1109/ACCESS.2023.3308035.
- [13] C. Mulambia, S. Varshney, and A. Suman, "Privacy preserving blockchain based authentication scheme for vanet," *Engineered Science*, 2023, doi: 10.30919/es1073.
- [14] M. Houser and M. L. Hasnaoui, "A risk and security assessment of VANET availability using attack tree concept," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 6, p. 6039, Dec. 2020, doi: 10.11591/ijece.v10i6.pp6039-6044.
- [15] B. T. Rao, R. S. M. L. Patibandla, and V. L. Narayana, "Comparative study on security and privacy issues in VANETs," in *Cloud and IoT-Based Vehicular Ad Hoc Networks*, Wiley, 2021, pp. 145–162. doi: 10.1002/9781119761846.ch8.
- [16] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey," *Vehicular Communications*, vol. 16, pp. 45–61, Apr. 2019, doi: 10.1016/j.vehcom.2019.02.002.




- [17] D. Hahn, A. Munir, and V. Behzadan, "Security and privacy issues in intelligent transportation systems: classification and challenges," *IEEE Intelligent Transportation Systems Magazine*, vol. 13, no. 1, pp. 181–196, 2021, doi: 10.1109/MITS.2019.2898973.
- [18] S. Gaba, M. Gupta, and H. Singh, "A comprehensive survey on VANET security attacks," in *AIP Conference Proceedings*, 2023, p. 020029. doi: 10.1063/5.0145236.
- [19] J. Mahmood *et al.*, "Secure message transmission for V2V based on mutual authentication for VANETs," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–16, Nov. 2021, doi: 10.1155/2021/3400558.
- [20] M. Hataba, A. Sherif, M. Mahmoud, M. Abdallah, and W. Alasmary, "Security and privacy issues in autonomous vehicles: a layer-based survey," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 811–829, 2022, doi: 10.1109/OJCOMS.2022.3169500.
- [21] P. Mundhe, V. K. Yadav, S. Verma, and S. Venkatesan, "Efficient lattice-based ring signature for message authentication in VANETs," *IEEE Systems Journal*, vol. 14, no. 4, pp. 5463–5474, Dec. 2020, doi: 10.1109/JSYST.2020.2980297.
- [22] H. Liu, H. Wang, and H. Gu, "HPBS: A hybrid proxy based authentication scheme in VANETs," *IEEE Access*, vol. 8, pp. 161655–161667, 2020, doi: 10.1109/ACCESS.2020.3021408.
- [23] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf, "Elliptic curve cryptography; applications, challenges, recent advances, and future trends: A comprehensive survey," *Computer Science Review*, vol. 47, p. 100530, Feb. 2023, doi: 10.1016/j.cosrev.2022.100530.
- [24] Y. Rajkumar and S. V. N. S. Kumar, "An elliptic curve cryptography based certificate-less signature aggregation scheme for efficient authentication in vehicular ad hoc networks," *Wireless Networks*, vol. 30, no. 1, pp. 335–362, 2024, doi: 10.1007/s11276-023-03473-8.
- [25] X. Feng, Q. Shi, Q. Xie, and L. Wang, "P2BA: a privacy-preserving protocol with batch authentication against semi-trusted RSUs in vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3888–3899, 2021, doi: 10.1109/TIFS.2021.3098971.
- [26] J. Lee, G. Kim, A. K. Das, and Y. Park, "Secure and efficient honey list-based authentication protocol for vehicular ad hoc networks," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2412–2425, Jul. 2021, doi: 10.1109/TNSE.2021.3093435.

BIOGRAPHIES OF AUTHORS






Chindika Mulambia    holds a B.Sc in Information and Communication Technology from Mzuzu University and currently pursuing a Master's Degree in Technology specializing in Networking and Cybersecurity at Sharda University. Currently working as Principal IT Officer for the Government of Malawi. Previous post was Principal Lecturer and has 10 years experiencing in lecturing. She used to be projects coordinator and has supervised more than 20 students pursuing their bachelors degree in Technology. Main areas of interest is vehicular networks and cybersecurity. She can be contacted at email: chindikachitalo@gmail.com.



Dr. Sudeep Varshney    is an Associate Professor and obtained his doctorate in CSE from IIT(ISM), Dhanbad. With over 19 years of experience in academics and vast research experience he has notable publications in national and international conferences including journal publications. His area of expertise is wireless sensor networks. He has also achieved senior membership in IEEE and life membership in CSI, IACSIT, and ISTE. He can be contacted at email: sudeep149@gmail.com.



Dr. Amrit Suman    is an Assitant Professor who obtained his doctorate from IIT(ISM) Dhanbad speacializing in Network Protocol Development. Areas of expertise are Software Engineering, AI/ML and sensor netowrks. He has vast experience in research with publications and presentations in several SCI/Scopus Journals and International Conferences. Before joining the academic field, he poses experience of over 11 years as an IT professional with expertise in software development and testing. He can be contacted at email: amrit.suman@sharda.ac.in.