# A Secure, Privacy-Preserving, and Lightweight Authentication Scheme for VANETs

**Article** *in* IEEE Sensors Journal · July 2021

DOI: 10.1109/JSEN.2021.3097172



**7 authors**, including:

Tarak Nandy
UCSI University
**28** PUBLICATIONS **533** CITATIONS
SEE PROFILE

Mohd Yamani Idna Idris
University of Malaya
**208** PUBLICATIONS **6,339** CITATIONS
SEE PROFILE

Rafidah Md. Noor
University of Malaya
**193** PUBLICATIONS **3,434** CITATIONS
SEE PROFILE

Ainuddin Wahid
University of Malaya
**117** PUBLICATIONS **4,185** CITATIONS
SEE PROFILE

# A Secure, Privacy-Preserving, and Lightweight Authentication Scheme for VANETs

Tarak Nandy, *Student Member, IEEE*, Mohd Yamani Idna Idris, *Member, IEEE*, Rafidah Md Noor, Ainuddin Wahid Abdul Wahab, Sananda Bhattacharyya, Raenu Kolandaisamy, Muktar Yahuza, *Student Member, IEEE*.

***Abstract*— The vehicular network is a collection of vehicles and other components facilitated with versatile sensors to communicate, which is backboned by authentication. Present authentication protocols focus on either the lightweight feature or security. On the other hand, privacy during authentication is essential. Moreover, existing schemes are dependent on the trusted authority for checking the legitimacy of a communicating node, which suffers from the infrastructure-less scenario. Alternatively, existing protocols are dependent on a secure communication channel during the registration phase. To address these concerns, an elliptic curve cryptography-based authentication protocol has been designed. Moreover, a secure key establishment is shown in this paper. Pseudo-id-based authentication is used to provide the privacy-preservation on the scheme. On the other hand, symmetric-key cryptography with a session key is used for message encryption during communication. A security analysis on the proposed scheme using the BAN logic and AVISPA shows the protocol's resilience capabilities on various attacks. Alternatively, the mathematical proof of the protocol represents the proof of correctness. Moreover, extensive performance analysis with the existing authentication schemes shows that the proposed algorithm is better in computation cost, communication cost, and energy cost. Lastly, the NS3 simulation shows the packet data transfer among the nodes in the network.**

***Index Terms*— authentication, elliptic curve cryptography (ECC), privacy, security, vehicular ad-hoc network(VANET) ,**

## I. Introduction

THE industries are now investing in the new implementation to make the automation. Automobile industries are also in the same queue. The trends of automation grasp the concept of vehicular communication [1]. Therefore, the vehicular ad-hoc network (VANET) steals substantial attention from both the industry and academia [2]. A VANET contains a set of smart vehicles that can take important decisions based on the send and receive messages on-road. On the other hand, roadside unit (RSU), devices implemented on the street in a specific distance, connects the on-road vehicles to the higher authorities such as trusted authority (TA) or traffic control centre (TMC).

Vehicles send enormous messages to the other vehicles regarding traffic, accident, signal, and many more. However, the legitimation of the vehicles should be identified before processing. VANET is an emerging topic in the current research area. Alternatively, VANET is threatened by a range of attacks [3]. Moreover, securing the VANET is essential for upcoming Intelligent Transport Systems. The major motivation of this research is to study and enhance VANET security. Additionally, the study can solve the problem of balancing the security and lightweight feature in protocol design and improve the security by incorporating the privacy-preserving authentication scheme where not only the safety of the vehicles will improve but also the protection of other components, which are indirectly related to the vehicular network, will increase. Nevertheless, authentication is the best way to validate the legitimate message provider (vehicle) on the road. The traditional authentication protocols are not suitable for a constrained network, with less computation power, less storage capability, less power backup, such as VANET. On the other hand, connecting to the TA during authentication and communication is not suitable for a highly mobile network like VANET. Moreover, the scheme should work on the infrastructure-less environment. On the other hand, a message from a vehicle may have identity value that may reveal some or all private information about a vehicle or the vehicle's driver. Therefore, privacy preservation during the protocol design is essential [4, 5]. Alternatively, existing authentication protocols focused on either lightweight features or security. However, a balance between the lightweight and secure authentication mechanism is needed for the vehicular network with privacy-preservation, motivating the current study.

The core research contributions of the paper are as follows.

1. A lightweight yet highly secure privacy-preserving key establishment in a VANET scenario has been

This study is supported by IIRG008A-19IISS, and FP055-2019A grant`.

Corresponding authors: T. Nandy, M.Y.I. Idris.

T. Nandy, M. Y. I. Idris, R. M. Noor, A. W. A. Wahab, and M. Yahuza are with the Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya, 50603 Kuala Lumpur, Malaysia (e-mail: tarak@um.edu.my; yamani@um.edu.my; fidah@um.edu.my; ainuddin@um.edu.my; mukyahuz@gmail.com).

M. Y. I. Idris, R. M. Noor, and A. W. A. Wahab are with Center for Mobile Cloud Computing Research (C4MCCR), Faculty of Computer Science and Information Technology, Universiti Malaya, 50603 Kuala Lumpur, Malaysia.

S. Bhattacharyya is with the Maldives Business School, Male', 20175, Maldives (e-mail: sananda@businessschool.mv).

R. Kolandaisamy is with Institute of Computer Science and Digital Innovation, UCSI University, 56000 Kuala Lumpur, Malaysia (e-mail: raenu@ucsiuniversity.edu.my)

introduced.

2. The proposed authentication protocol overcomes the existing problems with trusted authority dependency and secure communication channel reliance during the registration.
3. The balance with the lightweight feature, security, and privacy has been established with the help of elliptic curve cryptography.
4. Security resilience has been shown through the elaborative discussion with Burrows–Abadi–Needham (BAN) logic and Automated Validation of Internet Security Protocols and Applications (AVISPA) tools.
5. Mathematical proof for the correctness of the proposed protocol is presented.
6. Extensive performance analysis has been conducted with the prior authentication schemes [6-10], which shows that the proposed scheme has outperformed others in many cases, such as communication cost, computation cost, and power consumption. Additionally, packet transfer during the communication is shown through the NS3 simulation.

The formation of the rest of the paper is as follows. Section II demonstrates the recent related research on vehicle authentication. Section III shows the background and some introductory ideas behind the actual concept. Section IV depicts the proposed authentication scheme elaborately. Section V shows the threats and protection mechanism and mathematical proof of the proposed protocol, followed by the scheme's extensive performance analysis on Section VI. Finally, the conclusion and future scopes are discussed in Section VIII.

## II. Related Work

*VANET* faces a substantial amount of attacks from inside and outside of the network [11]. To address these issues, a slew of VANET authentication research has been conducted in the last decades. Different kinds of authentication mechanisms are introduced in the VANET, including identity-based authentication [7], public-key cryptography, MAC-based, session key-based, and hybrid [12]. On the other hand, emerging technologies such as blockchain, bilinear pairing [13], smartcard [14], and biometric are introduced in that list. Azees, Vijayakumar and Deboarh [15] proposed a bilinear pairing-based conditional privacy-preserving anonymous authentication scheme in *VANET*. In the same year, Liu, Wang and Chang [16] proposed a dual authentication scheme, where vehicles need *RSU* in the first stage and *TA* in the second stage for legitimation; however, *TA* may not be reachable for an infrastructure-less scenario such as rural area. On the other hand, Zhang, Wu, Domingo-Ferrer, Qin and Hu [17] showed the issue with the ideal TPD and proposed a compressed signature technique in the bilinear pairing-based vehicle authentication. However, the *TA* dependency is a problem like others in this work. Asaar, Salmasizadeh, Susilo and Majidi [18] proposed an identity-based message authentication scheme using proxy vehicles. In the next year, Pournaghi, Zahednejad, Bayat and Farjami [19] proposed to put the *TPD* inside the RSU instead of putting them in the OBU. Moreover, they proposed an authentication based on the *RSU* and *TPD*. However, their scheme's primary assumption is that a secure communication channel lies between the RSU and TA, which is non-realistic. Alternatively, Tangade, Manvi and Lorenz [20] proposed a hybrid authentication using asymmetric identity-based cryptography and symmetric hash message authentication code (*HMAC*). However, signature verification during the authentication introduces overhead and extra time complexity. In the same year, Zhong, Huang, Cui, Xu and Liu [21] used the registration list to reduce the computation overhead in their proposed authentication scheme. However, their protocol needs the *RSU* to check other vehicles' legitimacy, which is not possible in all the scenarios. In the following year, Alangudi Balaji, Sukumar and Parvathy [22] employed the ECC and bilinear mapping-based Diffie–Hellman key exchange mechanism in their proposed protocol. Nevertheless, the computation error and average link duration are not considered in the stated scheme. Recently, Cui, Xu, Han, Zhang and Zhong [23] proposed reliable privacy-preserving mutual authentication. In this protocol, a vehicle needs to perform mutual authentication with *TA* before broadcasting any message in the network. Moreover, an update of the *TPD* is performed before a side-channel attack by any adversary. On the other hand, Cui, Zhang, Zhong, Zhang and Liu [24] proposed a multi-cloud environment-based conditional privacy-preserving authentication for VANET where a vehicle needs to register with the *TA* once; however, it needs continuous communication with the cloud. Recently, Vangala, Bera, Saha, Das, Kumar and Park [25] introduced a blockchain-based *VANET* authentication to protect secure transmission. Moreover, the protocol is capable of detecting accidents and notify the danger in vehicular communication. However, two different authentication scenarios, such as vehicle to cluster head and cluster head to RSU, are needed to fulfill the protocol, which is time-consuming and overhead for a high mobility network such as *VANET*.

A set of problems have been identified from the existing authentication protocols for *VANET*; it includes an excessive dependency on *TA* during authentication and communication, imbalance optimization on lightweight and security for designing the protocol, and less concentration on the privacy of a vehicle. An ECC-based mutual key agreement and authentication protocol is designed and shown in this paper to overcome these issues. To ensure the privacy-preservation during insecure communication, a pseudo-identity is introduced. Moreover, the protocol proves the resilience of various attacks and practicality via reliable simulation. Additionally, the performance analysis reserves the lightweight comprehension of the proposed authentication protocol.

## III. Preliminaries

This section of the article describes basic building blocks of the VANET along with threat and system model. Moreover, the assumptions on the proposed protocol are depicted in this part.

### *VANET Architecture*

The VANET is a set of different components and organizational bodies. (See Fig. 1) The explanation of each and every module of VANET are as follows.

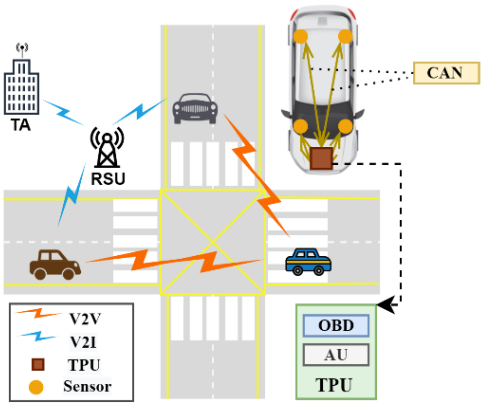



Fig. 1. VANET Scenario; V2V: vehicle-to-vehicle communication; V2I: vehicle to infrastructure communication.

1) *Sensors*

Sensors are the backbone of the whole network, as different kinds of sensors attached to the vehicles make it possible to push vehicular communication in automation. These sensors may include a pressure gauge, speedometer, radar sensors, GPS, and gas sensors. The sensors are directly connected to the OBD via a control access network (CAN) wirelessly. Moreover, sensors sense the environmental actions and send the information to the OBD periodically so that OBD can forward it to the higher authority or decide on an occasion.

2) *Roadside Unit (RSU)*

RSUs are the devices distributed on the roadside, maintaining a specific distance as per the communication range. However, it can be seen in the parking places or in the filling stations. The RSU is a powerful device to help the communications and transfer messages in VANET. Moreover, RSUs are equipped with network devices based on short-range wireless communication standards such as IEEE 802.11p. The core functionality of the RSU are:

- Allowing vehicles to connect to the cloud or trusted authorities.
- Extending the communication range with the different nearby nodes to the other central control systems [26].
- Redistributing the security messages such as basic safety message (BSM), traffic signal information, and accident alert over the network among vehicle [27].

3) *Tamper Proof Unit (TPU)*

All the vehicles are equipped with TPD, secure and detachable from the vehicle without proper authorization. Additionally, TPD consists of two other units called on-board device (OBD) and application unit (AU). The OBU is responsible for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication [28]. Moreover, the transmission on the OBD is based on the dedicated short-range communication (DSRC) [29] supported by 802.11p standardization dedicated to the vehicular network. On the other hand, the AU works based on the application installed in the vehicles, such as warning, network monitoring, or internet-based entertainment.

4) *Trusted Authority (TA)*

TA can be known as the higher authority of the VANETs. TA holds the basic and important information of the network as well as the components of the VANET. Moreover, TA can act like many autonomous or amalgamate super bodies such as communication key generators, vehicle information collectors, authorization providers, component identifiers, and permission grantors. However, the fast and dynamic topological network such as VANET may not connect to the TA in every different scenario, which encourages current research.

## System Model and Assumption

The system architecture of the model is a *VANET* scenario as per [30], where two or more on-road vehicles can authenticate and communicate among themselves without the help of a super body such as a vehicle information server (VIS) of trusted authority (TA). There are two different layers named as 1) server layer and 2) vehicle layer. The server layer consists of a vehicle information server, a powerful high-end system with high storage and computation capabilities. Additionally, the VIS maintains the details and partly credentials of the registering vehicles. Therefore, the registering of a vehicle takes place in this layer. Alternatively, two or more vehicles authenticate and communicate using the registering elements and a few on the spot, supporting the vehicle layer elements. On the other hand, the server layer works under a secure or insecure communication channel, whereas the vehicle layer completely works in an insecure communication channel.

The use of elliptic curve cryptography (ECC) is chosen to protect the communication via helping the registration and the authentication in a VENET scenario. The ECC has powerful features over others to make the model lightweight as well as secure. On the other hand, the traditional cryptographic algorithms (RSA, DSA) are unsuitable for the resource constraint environment such as VANET. The advantages of ECC over RSA or DSA are enormous. A small key size in ECC has more protection against cryptanalysis than a more significant bit size key in others (see Table 1).

TABLE 1
COMPARISON OF KEY SIZE

| ECC (bits) | RSA (bits) | Key Size Ratio (bits) |
|---|---|---|
| 160 | 1024 | 1:6 |
| 224 | 2048 | 1:9 |
| 256 | 3072 | 1:12 |
| 384 | 7680 | 1:20 |
| 512 | 15360 | 1:30 |

## Threat Models

Threat modelling is a method in which it is possible to illustrate capability risks, including technical weaknesses or the lack of adequate security, diagnosed, computed, and justified. The Dolev-Yao (DY) [31] threat model is chosen for the current study as it is best to show the collaborative cryptographic protocol. Furthermore, the model demonstrates the insecure communications among the nodes. On the other hand, the communicating vehicles act as an adversary and as the communication channel is public, the transaction cannot be trusted. Additionally, the DY model considers the scenario where an attacker can receiver, alter, destroy or drop the transmitted packet in the insecure channel. On the other side, the model completely trusts the server. Therefore, in the proposed model, the communication between the vehicles and

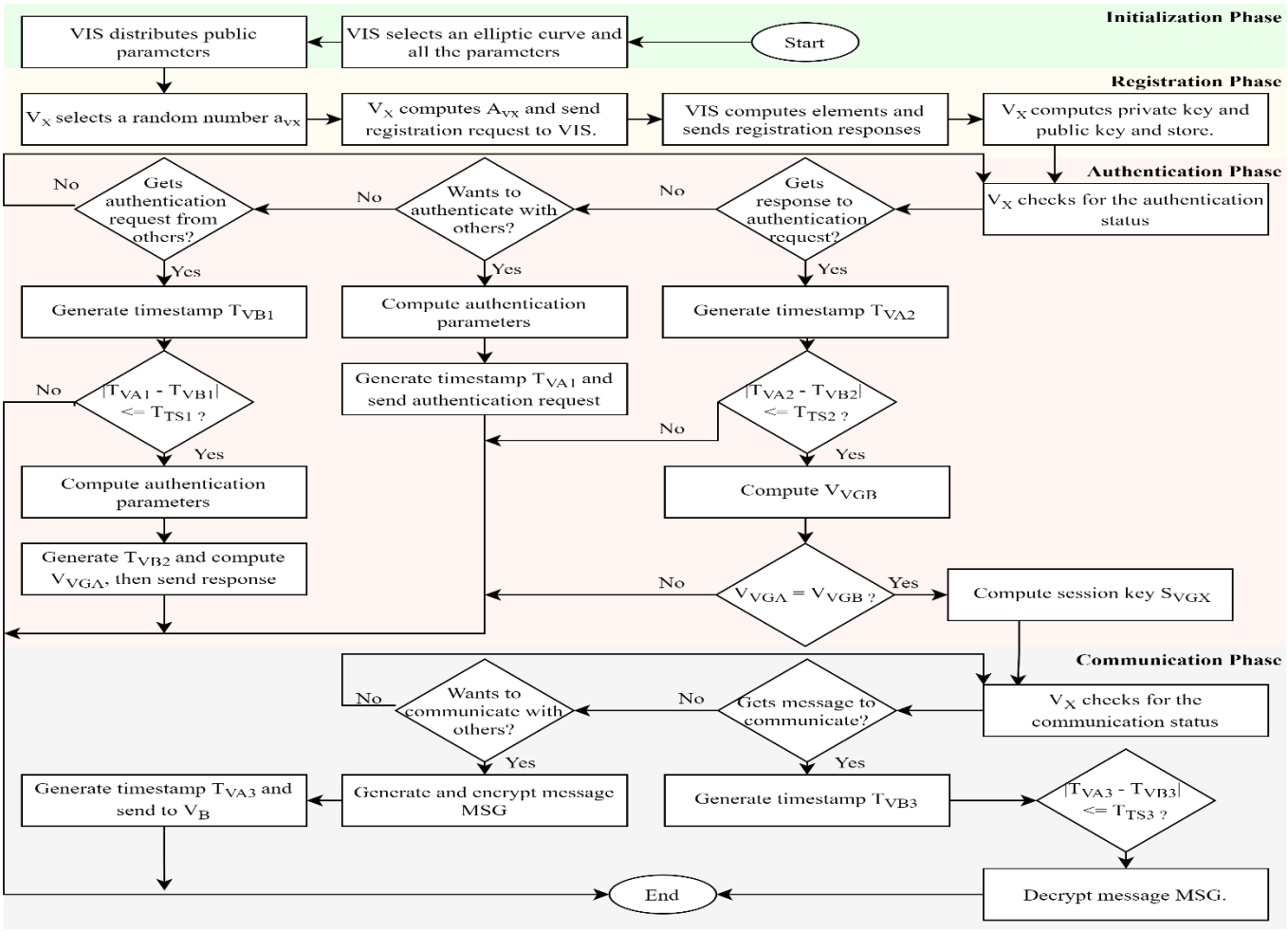



Fig. 2. A complete flowchart of the proposed authentication protocol.

server is trusted and held in a highly secure communication channel without the knowledge of the adversary. However, the adversary has a complete understanding of the transmitted messages between the vehicles over the public network.

On the other hand, the proposed protocol has considered another popular threat model named as Canetti-Krawczyk (CK) adversarial model [32]. This model is represented by a non - deterministic polynomial adversary that can reach and manipulate the complete contact path. As a result, an attacker can alter, delete, sense, edit, replay or discard a message from the communication channel. Alternatively, an adversary has all the knowledge of the public identities of all the participants. The adversary can be a dishonest user of the VANET network. Moreover, any vehicle with or without registration can be an attacker in this present scenario. Therefore, a range of attacks is possible in the network, such as replay, insider, man-in-the-middle, message modification, forward secrecy, privacy protection, and inherited related threats.

### *Elliptic Curve Cryptography (ECC)*

The ECC is a way of achieving the public key cryptography supported by the algebraic elliptic curve $(E)$ over a finite field $(F_p)$ in an exceptional case with a large prime number $p$. ECC provides the same amount of security as other public-key cryptographic algorithms: however, with a much smaller number of key size (see Table 1). The curve $E$ can be shown as $y^2 = x^3 + ax + b$, where $4x^3 + 27b(mod\ P) \neq 0$ and $a, b \in F_P$. Alternatively, a generator point $G$ is chosen in the curve $E$ to generate the cycle group. The popular operations with the ECC are point addition and point multiplication. However, getting the key value from the calculation is hard. Therefore, the operation is known as the elliptic curve discrete logarithm problem (*ECDLP*). On the other hand, an ECC can be used in the encryption conjoining the key management with the symmetric key cryptography.

## IV. Proposed Authentication Protocol

The centralized communication network is common among the message transmission protocols, even in the *VANET*. However, the decentralized communication is challenging, where different dynamic nodes can transfer the massages without the interference of TA or regulatory authority. The decentralized communication supports the proposed protocol. The scheme is further categorized into four phases such as 1) Initialization, 2) Registration, 3) Authentication, and 4) Communication. The details (see Fig. 2) are given in the following sub-sections.

### *Initialization Phase*

The initialization happens in the VIS over a secure or

insecure communication channel. The steps are as follows.

1) VIS selects an elliptic curve $E$ over a finite field $F_p$. Moreover, VIS defines a sizeable prime number $P$ and generator $G$.
2) VIS selects a random value $SK_{VIS}$ from the chosen field $F_p$ such that $SK_{VIS} \in F_p$. Then, VIS set the $SK_{VIS}$ as the private key of the server.
3) VIS then perform a point multiplication on E using $SK_{VIS}$ and $G$ and set the resultant point $PK_{VIS}$ as a public key of the server. $PK_{VIS} = SK_{VIS} * G$.
4) Now, VIS selects two different non-reversible hash functions as $H_i(.)$ where $i = 1, 2$ such as $H_1(x) = \{c\}$ where x is value and $c \in F_P$ and $H_2(.)$ is any one-way hashing mechanism such as Sha2 and Sha3.
5) Finally, VIS stores the public key and private key of itself and distributes $\{E, F_P, H_i(.), PK_{VIS}\}$ to all the registering vehicles.

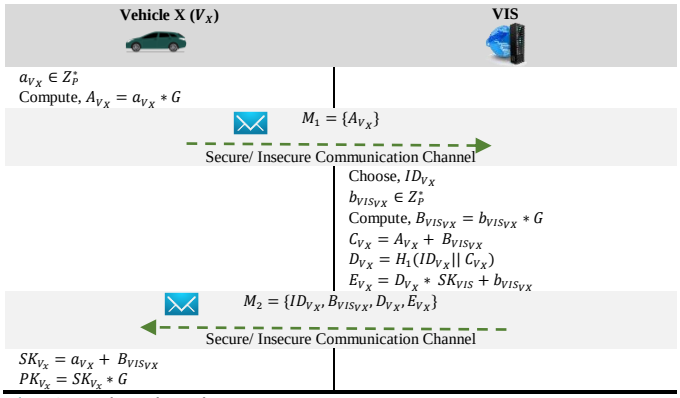



Fig. 3 Registration phase

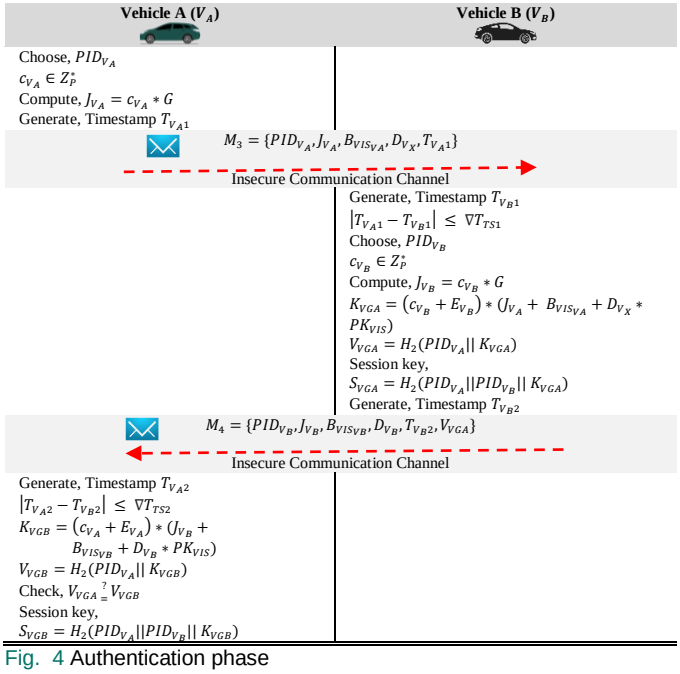



Fig. 4 Authentication phase

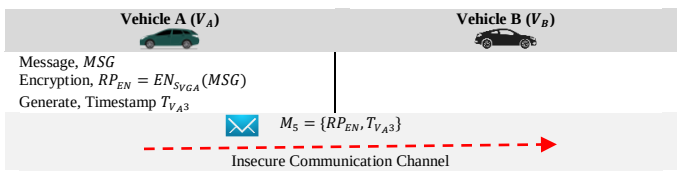



Fig. 5 Communication phase

## Registration Phase

The vehicles ($V_X$) need to register themselves with the VIS, which makes them enable on-road authentication and communication. Vehicles reach the VIS for registration, and the phase operates on a secure or insecure communication channel. The steps (see Fig. 3 ) of the registration phase are shown below.

1) Let a vehicle $V_X$ wants to register with the $VIS$. Therefore, $V_X$ selects a random number $a_{V_X}$ from the finite field $Z_P^*$ where $a_{V_X} \in Z_P^*$ and computes $A_{V_X} = a_{V_X} * G$. Finally, $V_X$ transfer it to $VIS$ as $M_1 = \{A_{V_X}\}$. Here $M_1$ signifies the 1st message transfer between two communicating nodes.
2) After receiving $M_1$ from $V_X$, $VIS$ chooses a unique identification number $ID_{V_X}$ for the vehicle $V_X$. After that, $VIS$ selects another random number $b_{VIS_{VX}}$ from the finite field $Z_P^*$ as the ephemeral secret where $b_{VIS_{VX}} \in Z_P^*$ and performs $B_{VIS_{VX}} = b_{VIS_{VX}} * G$, a parameter to help vehicle for authentication. Then, add the ephemeral secrets of $V_X$ $(A_{V_X})$ and $VIS$ $(B_{VIS_{VX}})$ as $C_{V_X} = A_{V_X} + B_{VIS_{VX}}$. After that, $VIS$ hash the concatenation of $ID_{V_X}$ and $C_{V_X}$ as $D_{V_X} = H_1(ID_{V_X} || C_{V_X})$ and compute $E_{V_X} = D_{V_X} * SK_{VIS} + b_{VIS_{VX}}$ to help $V_X$ to create their public and private key. Finally, VIS sends $M_2 = \{ID_{V_X}, B_{VIS_{VX}}, D_{V_X}, E_{V_X}\}$ to $V_X$.
3) $V_X$ adds its ephemeral secret and $B_{VIS_{VX}}$ to make its secret key $SK_{V_X} = a_{V_X} + B_{VIS_{VX}}$ for future use. Alternatively, $V_X$ calculates the public key $PK_{V_X} = SK_{V_X} * G$ and store all of the receiving elements along with the in the OBD.

## Authentication Phase

The authentication takes place on the road between two or more vehicles. All the vehicles need to authenticate themselves with others to communicate. However, they do not need any authorities to perform this task, making the algorithm more realistic and viable for such a random topological network like VANET. On that same notation, registration serves in insure and public channels; however, the strongly proposed algorithm makes it possible to authenticate different vehicles securely with privacy preservation. Consider $V_A$ wants to communicate with $V_B$; therefore, registers. The steps (see Fig. 4) are shown as follows.

1) Firstly, $V_A$ selects a pseudo identification number $PID_{V_A}$ for preserving privacy over communication. After that, selects a random integer $c_{V_A} \in Z_P^*$ and compute $J_{V_A} = c_{V_A} * G$. Finally, $V_A$ generates the current timestamp $T_{V_A1}$ and sends $M_3 = \{PID_{V_A}, J_{V_A}, B_{VIS_{VA}}, D_{V_X}, T_{V_A1}\}$ to $V_B$.
2) After receiving the $M_3$, $V_B$ generates the current timestamps $T_{V_B1}$ and checks $|T_{V_A1} - T_{V_B1}| \leq \nabla T_{TS1}$ with the previously settle threshold value $\nabla T_{TS1}$ to determine if the message is altered in between the transfer. If the difference of the timestamps are not satisfactory, then $V_B$ terminates the authentication process and quits the communication. However, if it is acceptable, $V_B$ chooses a pseudo

identification $PID_{V_B}$ and compute a random integer $c_{V_B} \in Z_P^*$ to generate $J_{V_B} = c_{V_B} * G$. Ultimately, $V_B$ creates a vehicle group key $K_{VGA} = (c_{V_B} + E_{V_B}) * (J_{V_A} + B_{VIS_{VA}} + D_{V_X} * PK_{VIS})$ to use for future communication. Moreover, to protect and verify the mutual key, $V_B$ computes a verifier $V_{VGA} = H_2(PID_{V_A} || K_{VGA})$. Alternatively, the verifier will be transferred over an insecure network, therefore, $V_B$ creates a secret session key $S_{VGA} = H_2(PID_{V_A} || PID_{V_B} || K_{VGA})$ for ultimate message transfer in the communication phase. Finally, $V_B$ sends $M_4 = \{PID_{V_B}, J_{V_B}, B_{VIS_{VB}}, D_{V_B}, T_{V_B2}, V_{VGA}\}$ to $V_A$.

3) After receiving the $M_4$, $V_A$ generates the current timestamps $T_{V_A2}$ and checks $|T_{V_B2} - T_{V_A2}| \leq \nabla T_{TS2}$ Terminates if it does satisfy. Alternatively, computes vehicle group key $K_{VGB} = (c_{V_A} + E_{V_A}) * (J_{V_B} + B_{VIS_{VB}} + D_{V_B} * PK_{VIS})$ and verifier $V_{VGB} = H_2(PID_{V_A} || K_{VGB})$. Furthermore, $V_A$ compares $V_{VGA} \stackrel{?}{=} V_{VGB}$ and terminates the communication if it does not match. Otherwise, computes the secret session key $S_{VGB} = H_2(PID_{V_A} || PID_{V_B} || K_{VGB})$ and keeps for the communication phase.

The proof of $K_{VGA} \stackrel{?}{=} K_{VGB}$ is shown in Appendix A, $V_{VGA} \stackrel{?}{=} V_{VGB}$ is presented in Appendix B and $S_{VGA} \stackrel{?}{=} S_{VGB}$ is illustrated in Appendix C.

### *Communication Phase*

The communication among the vehicles can take place after the successful authentication. However, authentication happens only for the first time, and communication can ensue again without authentication in every occurrence. Moreover, the communication phase occurs under an insecure channel like authentication. To illustrate further, let $V_A$ and $V_B$ completed the authentication and tries to communicate. The illustration of the different steps (see Fig. 5) of vehicle communications is shown as follows.

1) $V_A$ selects a message $MSG$ to send to $V_B$. Then chooses a common symmetric key cryptography and encrypt $MSG$ with the help of the secret session key $S_{VGA}$ as $RP_{EN} = EN_{S_{VGA}}(MSG)$). Finally, it generates the current timestamp $T_{V_A3}$ and sends $M_5 = \{RP_{EN}, T_{V_A3}\}$ to $V_B$.
2) $V_B$ also generates the current timestamp $T_{V_B3}$ and checks $|T_{V_A3} - T_{V_B3}| \leq \nabla T_{TS3}$ to ensure the legitimacy of the received message $M_5$. If the check shows a positive result, then $V_B$ perform the decryption of $MSG$ with the secret session key $S_{VGB}$ as $RP_{DE} = DE_{S_{VGA}}(RP_{EN})$. As the secret session keys are common, $RP_{DE}$ signifies to $MSG$.

## V. Security Analysis

The section deprecates the security confirmation of the proposed protocol against relevant upgraded cryptographic attacks. However, the security measurements are shown in two formal and informal settings; however, effective security analysis. Finally, the mathematical proof of the protocol is illustrated.

### *Informal Security Analysis*

As the authentication and communication take place on the insecure network, the authentication protocols are vulnerable to get attacked. This section discusses the current and important attacks on the proposed algorithm with resiliency. Let us consider an attacker node $\mathscr{A}$ and a victim vehicle $V_A$.

1) Replay Attack: Vehicles use timestamps for every message passing in an insecure channel such as $T_{V_A1}, T_{V_B1}, T_{V_B2}, T_{V_A2}$ in authentication and $T_{V_A3}, T_{V_B3}$ in communication. Furthermore, if $\mathscr{A}$ tries to sniff and fake any messages, $\mathscr{A}$ will fail due to the checkpoint of every receiving message timing with a predefined threshold as an example $|T_{V_A3} - T_{V_B3}| \leq \nabla T_{TS3}$ in communication.
2) Insider Attack: If a vehicle is legitimate; however, an attacker $\mathscr{A}$ from the network tries to intercept a message, he/she cannot perform cryptanalysis of the message, as the powerful hash function and ECDLP protect it.
3) Man in the Middle Attack: Let $\mathscr{A}$ gets all the transferred messages between $V_A$ and $V_B$. However, $V_A$ and $V_B$ select different ephemeral secrets as $c_{V_A} \in Z_P^*$ and $c_{V_B} \in Z_P^*$ and never share over the network. On the other hand, $V_A$ and $V_B$ calculate the secret key $K_{VGA}$ and send verifier $V_{VGA}$ to others to come into a shared session key $S_{VGA}$. Therefore, $\mathscr{A}$ cannot get the parameters to calculate the session key by a man-in-the-middle attack.
4) Message Modification: In this situation, $\mathscr{A}$ tries to modify a message during communication. However, as an unrevealed session key $S_{VGA}$ protects the scheme, $\mathscr{A}$ cannot decrypt an encrypted message during communication.
5) Mutual Authentication: $V_A$ and $V_B$ use different parameters from the registration phase to calculate the secret key ($K_{VGA}$) between them. On the other hand, $V_A$ and $V_B$ never share the ephemeral secrets to calculate the secret key ($K_{VGA}$). Finally, $V_B$ calculates the verifier $V_{VGA} = H_2(PID_{V_A} || K_{VGA})$ and send it to the $V_A$. On the other hand, $V_A$ also calculates $V_{VGB} = H_2(PID_{V_A} || K_{VGA})$ and checks $V_{VGA} \stackrel{?}{=} V_{VGB}$ to assure mutual authentication.
6) Forward Secrecy: Forward secrecy may happen when $\mathscr{A}$ has full access to the communication messages and have knowledge about the secret key. However, $\mathscr{A}$ is unable to create the secret key ($K_{VGA}$) as the ephemeral secrets of $V_A$ ($c_{V_A}$) and $V_B$ ($c_{V_B}$) are unknown to $\mathscr{A}$.
7) Privacy Protection: $V_A$ generates a pseudo identification $PID_{V_A}$ during authentication. On the other hand, this pseudo identification $PID_{V_A}$ can be different in different instances for the same vehicle $V_A$. Therefore, identity tracing of $V_A$ or its driver is not possible by an attacker from the retrieved message.

### *Formal Security Analysis*

The formal security verification of the proposed authentication scheme is shown in this section with the help of the *ROR* model, *BAN* logic, and the *AVISPA* tool. The details are shown as follows.

#### *1) Formal Security Verification with ROR model*

The formal security analysis of the proposed authentication protocol is shown by the popular *ROR* model [33].

ROR model description

This section shows the entire notations for the *ROR* model. Different terms of this model are shown below.

**Participants:** The proposed protocol uses three independent users, such as $VIS, V_A$ and $V_B$ for vehicle information server, vehicle A, and vehicle B, respectively. Let us assume $\prod_{VIS}^{i}, \prod_{V_A}^{j}$, and $\prod_{V_B}^{k}$ denote instance i, j, k of the participants $VIS, V_A$ and $V_B$, respectively.

**Accepted state:** An instance $\prod^{i}$ is said to be an accepted state if it goes to an accepted mode after receiving the last expected message from the protocol.

**Partnering:** The partnering is based on the session identifier ($sid$) and partner identifier ($pid$), where sid can be identified as a function of all sent and received protocol messages by the instances $\prod^{i_1}$ and $\prod^{i_2}$, and $pid$ is an instance with which a shared secret key is established. Therefore, two instances $\prod^{i_1}$ and $\prod^{i_2}$ are said to be a partner if the following conditions are satisfied, 1) $\prod^{i_1}$ and $\prod^{i_2}$ accept, 2) $\prod^{i_1}$ and $\prod^{i_2}$ share the same $sid$, 3) $pid$ for $\prod^{i_1}$ and $\prod^{i_2}$ are same, 4) no instances other than $\prod^{i_1}$ and $\prod^{i_2}$ accepts with a $pid$ equal to $\prod^{i_1}$ and $\prod^{i_2}$.

**Freshness:** $\prod_{V_A}^{j}$ or $\prod_{V_B}^{k}$ is fresh if the session key $S_{VGX}$ between $V_A$ and $V_B$ are not discovered by the adversary ($\mathcal{A}$) by the reveal $RVL$ ($\prod^{j}$) query.

**Adversary:** An active adversary tries to intercept all the communicating messages among the participants by simulating real attacks using "execute, send, reveal, and test" queries. All the queries are explained as follows.

Execute query $EXC$ ($\prod^{j}, \prod^{k}$): All the messages exchanged by the instances $\prod^{j}$, and $\prod^{k}$ are intercepted (eavesdropped) with the help of this query.

Send query $SND$ ($\prod^{j}$, $m$): $\mathcal{A}$ sends $m$ as a message to an instance $\prod^{j}$ expecting a response to perform an active attack.

Reveal query $RVL$ ($\prod^{j}$): An adversary ($\mathcal{A}$) can get the current session key between the $\prod^{j}$ and its partner by the reveal query.

Test query $TST$ ($\prod^{j}$): $\mathcal{A}$ requests the session key to $\prod^{j}$ and get a reply with an outcome of session key if c=1, or a random number if c=0; otherwise, it is null ($\perp$).

**Semantic security of session key:** $\mathcal{A}$ needs to differentiate between the original session key $S_{VGX}$ and random key in the experiment. Moreover, $\mathcal{A}$ can execute many $TST$ queries to $\prod^{j}$, or $\prod^{k}$. Responses of $c'$ are returned at the end of the experiment; however, the consistency of $c$ is essential. On the other hand, $\mathcal{A}$ can win the game if $c = c'$. Consider $WIN$ as an event where $\mathcal{A}$ wins and $Adv_p^{PLAS}$ is the advantage of A of breaking the semantic security of proposed privacy-preserving lightweight authentication scheme ($PLAS$), say p, then $Adv_p^{PLAS} = [2.P[WIN] - 1]$. On the other hand, it can be said that $p$ is secure if $Adv_p^{PLAS} \leq \eta$ for any small value $\eta > 0$.

**Random oracle:** All the participants ($\prod_{VIS}^{i}, \prod_{V_A}^{j}$, and $\prod_{V_B}^{k}$) and the adversary ($\mathcal{A}$) has access to the one-way hash function $h(.)$, which is further known as a hash oracle.

Formal security proof

The difference lemma has been used for a formal security proof.

**Lemma 1 (Difference Lemma):** Consider $B_1 \wedge \neg B_3 \Leftrightarrow B_2 \wedge \neg B_3$, where $B_1$, $B_2$, and $B_3$ are the events defined in some probability distribution, then,

$$|P[B_1] - P[B_2]| \leq P[B_3] \quad (1)$$

**Theorem 1:** Assume an adversary ($\mathcal{A}$) running in the "polynomial time t," tries to obtain the session key between $\prod_{V_A}^{j}$, and $\prod_{V_B}^{k}$ over the proposed protocol $p$. Then $\mathcal{A}$'s advantage of breaking the semantic security over $p$ is written as,

$$Adv_p^{PLAS}(t) \leq \frac{q_{hash}^2}{|Hash|} + 2.Adv^{ECDLP}(t) \quad (2)$$

Where, $q_{hash}$, $|Hash|$, and $Adv^{ECDLP}(t)$ represent the number of hash queries, the range of one-way hash function $H(.)$ and the advantage of $\mathcal{A}$ in breaking ECDLP.

**Proof:** The proof of this theorem is based on the following four games, say $G_i, i \in [0,3]$. Furthermore, consider $WIN_i, , i \in [0,3]$ as an event where $\mathcal{A}$ guesses the bit $c$ in the game $G_i$ and wins, where $G_0$ represents a real attack on $p$ and $G_3$ shows that $\mathcal{A}$ has the minimal advantage of breaking the $S_{VGX}$ security in $p$.

**Game $G_0$:** A begins with $G_0$ by selecting a bit $c$ and launching a real attack on $p$. Therefore,

$$Adv_p^{PLAS}(t) = |2.P[WIN_0] - 1| \quad (3)$$

**Game $G_1$:** This game corresponds to "an eavesdropping attack" in which $\mathcal{A}$ can have access to all the communicating messages between $\prod_{V_A}^{j}$, and $\prod_{V_B}^{k}$ during authentication and communication phase. A performs $EXC$ ($\prod^{j}, \prod^{k}$) oracle and send a $TST$ ($\prod^{j}$) oracle to determine if the outcome is a session key or random value. The session key is generated by $V_B$ as $S_{VGA} = H_2(PID_{V_A}||PID_{V_B}||K_{VGA})$. On the other hand, $V_A$ generates the same session key as $S_{VGB} = H_2(PID_{V_A}||PID_{V_B}||K_{VGB})$. To determine the $K_{VGA} = K_{VGB} = (c_{V_A} + E_{V_A}) * (J_{V_B} + B_{VIS_{VB}} + D_{V_B} * PK_{VIS})$ needs to know the $PK_{VIS}$ and the random number $C_{V_x}$. Therefore, the chance of winning the game for $\mathcal{A}$ has never increased by eavesdropping, which reflects $G_0$ and $G_1$ are equivalent. Therefore,

$$P[WIN_0] = P[WIN_1] \quad (4)$$

**Game $G_2$:** In this game, the hash query simulation is considered so that the active attack scenario can be tested. $\mathcal{A}$ sends fabricated messages to the participants to perform an active attack. $\mathcal{A}$ needs to undertake the $M_3 = \{PID_{V_A}, J_{V_A}, B_{VIS_{VA}}, D_{V_X}, T_{V_A1}\}$ and $M_4 = \{PID_{V_B}, J_{V_B}, B_{VIS_{VB}}, D_{V_B}, T_{V_B2}, V_{VGA}\}$ to generate an authentication key. On the other hand, $\mathcal{A}$ needs all the secret keys and random numbers to generate $S_{VGX}$, which cannot be obtained through the communicating messages and the queries as the randomness of the message ensures no

collision in the hash digests. Therefore, from the result of the birthday paradox,

$$P[WIN_1] - P[WIN_2] \leq \frac{q_{hash}^2}{|Hash|} \quad (5)$$

**Game $G_3$:** $\mathcal{A}$ tries to get the actual session key $S_{\mathrm{VGx}}$ by attempting eavesdropping. $\mathcal{A}$ does not know the secret key to compute $K_{\mathrm{VGA}}$ or $K_{\mathrm{VGB}}$. On the other hand, retrieving the random number $C_{\mathrm{VX}}$ from $J_{\mathrm{VX}}$ is not feasible as per the computational hardness of $ECDLP$. Hence,

$$P[WIN_2] - P[WIN_3] \leq 2.Adv^{ECDLP}(t) \quad (6)$$

As the session keys are generated independently and randomly by $V_{\mathrm{A}}$ and $V_{\mathrm{B}}$, A does not have any knowledge of the bit $c$. Therefore,

$$P[WIN_3] = \frac{1}{2} \quad (7)$$

From equation (3), (4), and (7),

$$\frac{1}{2}Adv_p^{PLAS} = \left|P[WIN_0] - \frac{1}{2}\right| = \left|P[WIN_1] - \frac{1}{2}\right| \quad (8)$$

By using (5) to (7), lemma 1, and triangular inequality, we get,

$$P[WIN_1] - P[WIN_3] \leq P[WIN_1] - P[WIN_2] + P[WIN_2] - P[WIN_3]$$
$$\leq |P[WIN_1] - P[WIN_2]| + |P[WIN_2] - P[WIN_3]|$$
$$\leq \frac{q_{hash}^2}{|Hash|} + 2.Adv^{ECDLP}(t) \quad (9)$$

Now, from (7), (8), and (9),

$$\left|P[WIN_1] - \frac{1}{2}\right| \leq \frac{q_{hash}^2}{2.|Hash|} + Adv^{ECDLP}(t) \quad (10)$$

So, from (8) and (10), we get the required result as (11).

$$\frac{1}{2}Adv_p^{PLAS} \leq \frac{q_{hash}^2}{2.|Hash|} + Adv^{ECDLP}(t)$$

$$Adv_p^{PLAS} \leq \frac{q_{hash}^2}{|Hash|} + 2.Adv^{ECDLP}(t) \quad (11)$$

### 2) *Formal Security Verification with BAN Logic*

*BAN* logic helps to build the formal validation of an authentication scheme over a shared network. The mentioned logic can determine the data dependency and the protection against the message alteration and sniff. The BAN logic uses a set of rules, assumptions, idealizations, and statements to prove the chosen goals. The interested readers may refer to [34] for a better understanding. The BAN logic ensures that the different vehicles use the shared secret key in the proposed protocol.

The goal of the scheme is to prove the following.

Goal $G_1$ : $V_A \models (V_A \overset{K_{VGX}}{\longleftrightarrow} V_B)$

Goal $G_2$ : $V_B \models (V_A \overset{K_{VGX}}{\longleftrightarrow} V_B)$

Goal $G_3$ : $V_A \models V_B \models (V_A \overset{K_{VGX}}{\longleftrightarrow} V_B)$

Goal $G_4$ : $V_B \models V_A \models (V_A \overset{K_{VGX}}{\longleftrightarrow} V_B)$

The assumptions based on the protocols are as follows.

$Assumption\ A_1$ : $V_A \models \#(\mathrm{T}_{\mathrm{V_A1}})$

$Assumption\ A_2$ : $V_A \models \#(PK_{VIS})$

$Assumption\ A_3$ : $V_A \models \#(\mathrm{T}_{\mathrm{V_A2}})$

$Assumption\ A_4$ : $V_B \models \#(PK_{VIS})$

$Assumption\ A_5$ : $V_B \models \#(\mathrm{T}_{\mathrm{V_A1}})$

$Assumption\ A_6$ : $V_B \models \#(\mathrm{T}_{\mathrm{V_B1}})$

$Assumption\ A_7$ : $V_A \models \#(\mathrm{T}_{\mathrm{V_B1}})$

$Assumption\ A_8$ : $V_A \models V_A \overset{\{K_{VGX}\}_{SK_{VIS}}}{\longleftrightarrow} V_B$

$Assumption\ A_9$ : $V_B \models V_A \overset{\{K_{VGX}\}_{SK_{VIS}}}{\longleftrightarrow} V_B$

$Assumption\ A_{10}$ : $V_A \models V_B \Rightarrow V_A \overset{K_{VGX}}{\longleftrightarrow} V_B$

$Assumption\ A_{11}$ : $V_B \models V_A \Rightarrow V_A \overset{K_{VGX}}{\longleftrightarrow} V_B$

The idealization based on the message passes in the authentication phases are as follows.

- Message 3 ($M_3$): $\{PID_{V_A}, J_{V_A}, B_{VIS_{VA}}, D_{V_X}, T_{V_A1}\}$
  - Idealized for of $M_3 : V_A \longrightarrow V_B : \{T_{V_A1},\ V_A \overset{K_{VGX}}{\longleftrightarrow} V_B\}_{SK_{VIS}}$
- Message 4 ($M_4$): $PID_{V_B}, J_{V_B}, B_{VIS_{VB}}, D_{V_B}, T_{V_B2}, V_{VGA}\}$
  - Idealized for of $M_4 : V_B \longrightarrow V_A : \{T_{V_B2},\ V_A \overset{K_{VGX}}{\longleftrightarrow} V_B\}_{SK_{VIS}}$

Now the goals are needed to be proved based on the rules, idealizations, and assumptions. The proofs are as follows.

From $M_3$,

$S_1$: $V_B \lhd (T_{V_A1},\ V_A \overset{K_{VGX}}{\longleftrightarrow} V_B)_{SK_{VIS}}$

From $S_1, A_9$ and the massage meaning rule,

$S_2$: $V_B \mid \equiv V_A \mid\sim (T_{V_A1},\ V_A \overset{K_{VGX}}{\longleftrightarrow} V_B)$

From $S_2, A_5$ and the freshness rule,

$S_3$: $V_B \models V_A \models (V_A \overset{K_{VGX}}{\longleftrightarrow} V_B)$ **[Proved: G4]**

From $M_4$,

$S_4$: $V_A \lhd (T_{V_B2},\ V_A \overset{K_{VGX}}{\longleftrightarrow} V_B)_{SK_{VIS}}$

From $S_4, A_8$ and the massage meaning rule,

$S_5$: $V_A \mid \equiv V_B \mid\sim (T_{V_B2},\ V_A \overset{K_{VGX}}{\longleftrightarrow} V_B)$

From $S_5, A_7$ and the freshness rule,

$S_6$: $V_A \models V_B \models (V_A \overset{K_{VGX}}{\longleftrightarrow} V_B)$ **[Proved:$G_3$]**

From $S_3, A_{11}$ and the jurisdiction rule,

$S_7$: $V_B \models (V_A \overset{K_{VGX}}{\longleftrightarrow} V_B)$ **[Proved:$G_2$]**

From S6 and A10 and the jurisdiction rule as,

$S_8$: $V_A \models (V_A \overset{K_{VGX}}{\longleftrightarrow} V_B)$ **[Proved: $G_1$]**

The $S_1$ to $S_8$ statements prove the mutual authentication and the key agreement between the communicating vehicles in the proposed protocol.

### 3) *Formal Security Verification using AVISPA: Simulation Study*

The *AVISPA* [35], a well-accepted formal security verification tool, is used to prove the security, such as a replay attack and man-in-the-middle attack against the proposed protocol. *AVISPA* is written in the High-Level Protocols Specification Language (*HLPSL*), and *SPAN* [36] helps to write in the *hlpsl* specification. The *hlpsl* is converted to the machine level language, intermediate format (*IF*), to read by the back-end of the AVISPA such as i) On-the-Fly Model-Checker (*OFMC*), ii) Constraint-Logic-based Attack Searcher (*CL-AtSe*), iii) SAT-based Model-Checker (*SATMC*) and iv) Tree Automata based on Protocol Analyzer (*TA4SP*) to check satisfactory results. The tools specification and results on the proposed protocol are discussed in the following sections.

#### *a) HLPSL specification*

Communication can take place securely if mutual authentication occurs securely. Therefore, the authentication phase is tested under *AVISPA* tools. The basic rolls for the tools are vehicle_a (*VA*), vehicle_b (*VB*), and vehicle_info_server (*VIS*). However, there are two

more roles called environmental roles and session roles.

As the tools work on the authentication phase, the prior specification is assumed to be protected. Accordingly, *VA* changes its state from 0 to 1 and sends an authentication request to the *VB* with secrecy on the ephemeral secret. On the other hand, *VB* receives the message from the *VA* and changes the status to 1. Then *VB* calculate the key and verifier and session key and set two secrecy goals as *secret ({Kvgx^' },s3,{VA,VB})* and *secret( {Ccvb'},s2,{VB}).* On the same note, *VB* sets an authentication goal on the key as *witness(VA,VB,va_vb_kvgx, Kvgx').* *VB* sends the required parameters to *VA* to generate the key and verifies the verifier. Alternatively, *VA* changes the status to 2 and receives the parameters sent by *VB*. Eventually, *VA* calculates the key and check for the authentication goal as *request(VA,VB,va_vb_kvgx, Kvgx')* to make sure about the mutual authentication. *VA* sets two more secrecy goals as *secret({Kvgx},s4,{VA,VB})* and *secret({Ccva},s5,{VA}).*

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/ecc_vanet_auth.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.09s
  visitedNodes: 56 nodes
  depth: 5 plies
```

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/ecc_vanet_auth.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 0 states
  Reachable  : 0 states
  Translation: 0.05 seconds
  Computation: 0.00 seconds
```

Fig. 6. AVISPA results

*b) Result Analysis*

Possible threats to the proposed protocol are measured by the use of *OFMC* and *CL-Atse* back-ends. On the other hand, the proposed scheme uses five different secrecy goals on the local parameters and one authenticity goal on the *VA* and *VB* secret key. Moreover, an intruder with the knowledge of the transfer messages is implemented on the environment role. Additionally, *OFMC* and *CL-Atse* check for the replay attack and the session with the intruder. Moreover, man-in-the-middle-attack is verified by the Delev-Yao (*DY*) against the proposed scheme. As per the simulation results in Fig. 6, the search time in *OFMC* is 0.09 seconds, with 56 visited nodes in 5 piles depth. On the other hand, the translation time for the *CL-Aste* is 0.09 seconds. However, both the back-ends show the summary of the scheme as "SAFE". The simulation result of the *AVISPA* clearly shows that the proposed scheme is safe against replay attack and man-in-the-middle attack.

## Mathematical Proof of Correctness

The proposed scheme is mainly based on authenticity issues. Therefore, proving the mutual authentication between communicating elements should show the correctness of the proposed protocol. Additionally, the values of different parameters are shown in Fig. 7 in a tested environment. It is distinctly visible that two elements are sharing the same values (indicated with different colors) for mutual authentication. The rest of this section will elaborate on the mathematical proof of the proposed authentication protocol's correctness. Our proposed protocol $(S)$ is secure for a given input sample space $i \in F_P$, a transformed output sample space $o \in F_P$ and a random keyspace $K \in F_P$, where $F_P$ is the finite field. The statements and the proofs are given below.

***Statement 1:*** Both the communicating parties compute the common keys for authentication in the scheme $S$.

**Proof 1:** Assume the vehicle $V_A$ wants to communicate to the vehicle $V_B$. $V_A$ sends a registration request to $V_B$. On that same notation, $V_A$ computes $K_{VGB}$ and $V_B$ computes $K_{VGA}$. Therefore, we need to proof $K_{VGA} = K_{VGB}$.

$$K_{VGA} = (c_{V_B} + E_{V_B}) * (J_{V_A} + B_{VIS_{V_A}} + D_{V_A} * PK_{VIS})$$
$$= (c_{V_B} + E_{V_R}) * (c_{V_A} * G + b_{VIS_{V_A}} * G + D_{V_A} * \mathrm{SK_{VIS}} * \mathrm{G})$$
[Substitute $J_{V_A}$ value as $J_{V_A} = c_{V_A} * G, B_{VIS_{V_A}} = b_{VIS_{V_A}} * G, and\ PK_{VIS} = \mathrm{SK_{VIS}} * \mathrm{G}$]
$$= (c_{V_B} + E_{V_B}) * (c_{V_A} + (D_{V_A} * \mathrm{SK_{VIS}} + b_{VIS_{V_A}})) * G$$
$$= (c_{V_B} + E_{V_B}) * (c_{V_A} + E_{V_A}) * G$$ [Substiture $E_{V_A}$ value as ]
$$= (c_{V_A} + E_{V_A}) * (c_{V_B} + E_{V_B}) * G$$
$$= (c_{V_A} + E_{V_A}) * (c_{V_B} + (D_{V_B} * \mathrm{SK_{VIS}} + b_{VIS_{V_B}})) * G$$
[Substiture $E_{V_B}$ value]
$$= (c_{V_A} + E_{V_A}) * (c_{V_B} * G + b_{VIS_{V_B}} * G + D_{V_B} * \mathrm{SK_{VIS}} * \mathrm{G})$$
$$= (c_{V_A} + E_{V_A}) * (J_{V_B} + B_{VIS_{V_B}} + D_{V_A} * PK_{VIS})$$
[Substitute $J_{V_B}$ value as $J_{V_B} = c_{V_B} * G, B_{VIS_{V_B}} = b_{VIS_{V_B}} * G, and\ PK_{VIS} = SK_{VIS} * G$]
$$= K_{VGB}$$

Therefore, we can say that $K_{VGA}$ and $K_{VGB}$ are equivalent and sharing the same values.

| **Parameters of VIS** | Curve =brainpoolP160r1<br>$SK_{VIS}$ = 14581…98098<br>$PK_{VIS}$ = 71294…90911, 64807…41493 |
|---|---|
| **Vehicle $V_A$** | **Vehicle $V_B$** |
| $a_{V_A}$ = 19825…66860 | $a_{V_B}$ = 12658…79033 |
| $A_{V_A}$ = 187115…336174, 78771…793927 | $A_{V_B}$ = 76477…48690, 56541…45940 |
| $ID_{V_A}$ = IDXDV01 | $ID_{V_B}$ = IDXDV02 |
| $b_{VIS_{VA}}$ = 12050…57720 | $b_{VIS_{VB}}$ = 54760…16088 |
| $B_{VIS_{VA}}$ = 53014…27478, 56491…640230 | $B_{VIS_{VB}}$ = 95655…31507, 53450…72921 |
| $C_{V_A}$ = 42657…561944, 28870…73444 | $C_{V_B}$ = 41077…31081, 11296…08750 |
| $D_{V_A}$ = 53502…38143 | $D_{V_B}$ = 50263…95060 |
| $E_{V_A}$ = 78013…09734 | $E_{V_B}$ = 73290…11968 |
| $c_{V_A}$ = 60957…24671 | $c_{V_B}$ = 48132…74768 |
| $J_{V_A}$ = 86419…66709, 10710…30925 | $J_{V_B}$ = 11622…67509, 59308…30183 |
| $K_{VGA}$ = 20753…20195, 11770…17339 | $K_{VGB}$ = 20753…20195, 117706…17339 |
| $V_{VGA}$ = 88e01…568a9 | $V_{VGB}$ = 88e01…568a9 |
| $S_{VGA}$ = 90cd7…c701c | $S_{VGB}$ = 90cd7…c701c |

Fig. 7. Values of all the parameters in a tested scenario.

***Statement 2:*** Both the communicating elements calculate common verifier in the scheme $S$.

**Proof 2:** Computed keys cannot be shared through the public media as it is vulnerable. Therefore, $V_A$ and $V_B$ calculate $V_{VGA}$ and $V_{VGB}$, respectively, as the verifier. Alternatively, it needs to be shown that $V_{VGA}$ and $V_{VGB}$ are the same.

$$V_{VGA} = H_2(PID_{V_A} || K_{VGA})$$
$$= H_2(PID_{V_A} || K_{VGB})$$ [Substitute $K_{VGA}$ value]
$$= V_{VGB}$$

The correctness of the verifiers has been proven.

***Statement 3:*** Both the communicating components share the mutual session key in the scheme $S$.

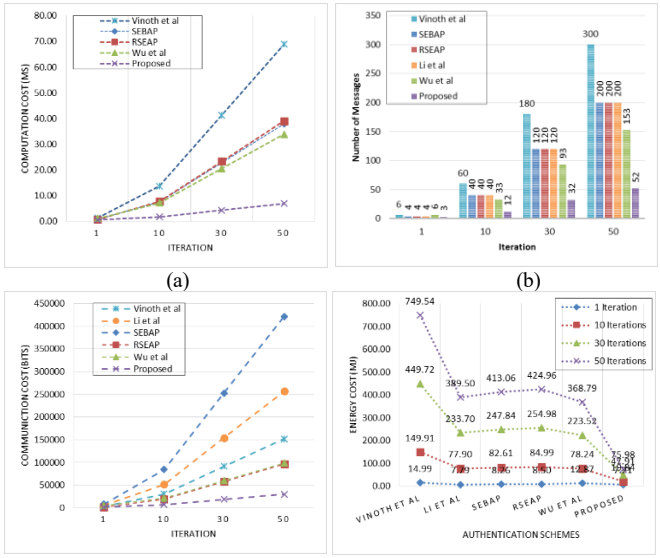
**Proof 3:** As the verifiers are to verify the correctness of the algorithm and are already share in the public network, anyone can get that value. Therefore, a secret session key is required, which needs to transfer over to the other party. $V_A$ and $V_B$ calculate $S_{VGA}$ and $S_{VGB}$, respectively, as the secret session key.

$$S_{VGA} = H_2(PID_{V_A}||PID_{V_B}||K_{VGA})$$
$$= H_2(PID_{V_A}||PID_{V_B}||K_{VGB}) \quad [\text{Substitute } K_{VGA}\text{value}]$$
$$= S_{VGB}$$

It can be said that the communicating couples in scheme $S$ share the equal session key ( $S_{VGX}, X \in \{A, B\}$ ).

## VI. Performance Analysis

The proposed scheme's performance is measured against the recent related authentication protocol [8-10]. The different performance metrics such as functionality features, computation cost, communication cost, and energy cost have been tested on the mentioned schemes. On the other hand, as the initialization and registration phase occurs only once, the performance analysis is done on the authentication and communication phase. The experiments are carried out on an *Ubuntu (18.4.0) based Intel Pentium® CPU 2020M at 240 GHZ* and 64bit system. Moreover, the protocol's functionality is tested and examined on the prevailing programming tool *python 3.8* and the *ECC* and symmetric key cryptography operations are carried out using the *tinyecc* and *crypto* libraries, respectively. The comparison graphs are shown in Fig. 8 and describe as follows.




(a) (b) (c) (d)

Fig. 8. Comparison Analysis, (a) computation cost in milliseconds, (b) message passing count, (c) communication cost in bits, and (d) energy cost in micro joules.

### Security and Functionality Features

All of the protocols have taken some essential protection against common attacks (see Table 2), such as replay attacks and insider attacks. However, the existing protocols keep some loopholes for security breaches. Primarily, existing authentication schemes assume and fully trust the secure communication channel in the registration phase. Due to the fact that they send some information that may reveal the secret key if the network is compromised. These may include $L$ in authentication face as it can be generated from $L = L_1 \oplus S_U$ provided $L_1$ and $S_u$ are received from $M_{R2}$ and $M_{R1}$, respectively in [8]. Similarly, *PWT* in [9] and *h(pwi)* in [10] are vulnerable to key disclosure. On the other hand, all of these protocols have only shown a few attack resilience based on mathematical formation in informal security analysis; however, they have not been proved through any formal security model except [10]. Alternatively, they did not show any mutual authentication using validation tools. Similarly, the protocols have not demonstrated any experiments on the algorithm in any scenario not even in the simulator. Alternatively, the formal security analysis of the proposed protocol is done by the well-known ROR model, which is lack from other existing protocols.

TABLE 2
COMPARISON OF FUNCTIONALITY FEATURES

| Functionality Features | | [8] | [9] | [10] | Proposed |
|---|---|---|---|---|---|
| Resistance of | Masquerade attack | Yes | No | No | Yes |
| | Message modification | N/A | Yes | N/A | Yes |
| | Identity protection | No | Yes | Yes | Yes |
| | Replay attack | Yes | Yes | Yes | Yes |
| | Insider attack | Yes | Yes | Yes | Yes |
| | Mutual authentication | No | Yes | No | Yes |
| Formal verification using AVISPA tool | | No | Yes | No | Yes |
| Formal validation using BAN logic | | No | No | No | Yes |
| Formal verification using ROR model | | No | No | No | Yes |
| Simulation and evaluation | | No | No | No | Yes |
| Based on viable assumptions | | No | No | No | Yes |

### Computation Cost

The cost of the computation of the authentication algorithms depends on the used functionalities. Time consumption for one-way hash ($T_H$), ECC multiplication ($T_{ECM}$), symmetric key encryptions ($T_{EN}$) *and modular multiplication* ($T_{MM}$) are 0.02864ms, 0.064497ms, 0.1046856ms, 0.1717ms respectively. The proposed protocol only needs 0.66ms. for single communication. However, as the design of the scheme, it needs only one authentication to communicate multiple times. Therefore, if a vehicle needs to communicate more than one with the same vehicles, the computation cost is significantly low, reduced by almost 500%. Table 3, Table 4 and Fig. 8(a) shows the computation cost on different iterations.

TABLE 3
COMPUTATION COST IN THE MATHEMATICAL EQUATION

| Scheme | Authentication | Communication | Time cost for a single communication | Time cost for multiple communication (n) |
|---|---|---|---|---|
| [6] | $19T_H + T_{ECM} + 6T_{EN} + 2T_{MM}$ | Combined# | $19T_H + T_{ECM} + 6T_{EN} + 2T_{MM}$ | $(19T_H + T_{ECM} + 6T_{EN} + 2T_{MM})$ * n |
| [7] | $25T_H$ | Combined# | $25T_H$ | $(25T_H)$ * n |
| [8] | $13T_H + 6T_{EN}$ | Combined# | $13T_H + 6T_{EN}$ | $(13T_H + 6T_{EN})$ * n |
| [9] | $9T_H + 5T_{ECM}$ | Combined# | $9T_H + 5T_{ECM}$ | $(9T_H + 5T_{ECM})$ * n |
| [10] | $18T_H$ | $16T_H + 2T_{ECM}$ | $34T_H + 2T_{ECM}$ | $18T_H + (16T_H + 2T_{ECM})$ * n |
| Proposed | $4T_H + 4T_{ECM}$ | $2T_{EN}$ | $4T_H + 4T_{ECM} + 2T_{EN}$ | $4T_H + 4T_{ECM} + (2T_{EN})$ * n |

# Combined with authentication

TABLE 4
COMPUTATION COST IN MILLISECONDS

| Scheme | Computation Cost (ms) | | | |
|---|---|---|---|---|
| | 1 | 10 | 30 | 50 |
| [6] | 1.38 | 13.78 | 41.33 | 68.89 |
| [7] | 0.72 | 7.16 | 21.48 | 35.80 |
| [8] | 0.76 | 7.59 | 22.78 | 37.97 |
| [9] | 0.78 | 7.81 | 23.44 | 39.06 |
| [10] | 1.18 | 7.19 | 20.54 | 33.90 |
| Proposed | 0.66 | 1.82 | 4.40 | 6.98 |

### Communication Cost

The message transfers between the vehicles during the stipulated phases are responsible for the communication cost. Therefore, the number of message pass and the size of each message is taken for consideration. Fig. 8(b, c) shows that the communication cost and message passing increases with the

communication iterations. Previous schemes are dependent on the *TA* during authentication and communication; however, the proposed scheme does not need that. The proposed protocol's communication cost (see Table 5) is significantly low than other previous schemes.

TABLE 5
COMMUNICATION COST AND TA DEPENDENCY

| Scheme | TA Dependency | Message Passing | Communication (bits) | | | |
|---|---|---|---|---|---|---|
| | | | 1 | 10 | 30 | 50 |
| [6] | Yes | 6 | 3040 | 30400 | 91200 | 152000 |
| [7] | Yes | 4 | 5132 | 51320 | 153960 | 256600 |
| [8] | Yes | 4 | 8432 | 84320 | 252960 | 421600 |
| [9] | Yes | 4 | 1920 | 19200 | 57600 | 96000 |
| [10] | Yes | 6 | 4384 | 21664 | 60064 | 98464 |
| Proposed | No | 3 | 1824 | 7008 | 18528 | 30048 |

### Energy Cost

The OBU needs a significant amount of energy consumption to perform the authentication. On the other hand, the major power source of a vehicle is the battery. Therefore, reducing the consumption of the battery over time is essential. The energy consumption is directly proportionate to the execution complexity of an algorithm. Consequently, energy cost is calculated based on Vasudev and Das [37] scheme and can be measured as $EN_C = T_E * C$, where $T_E$ is the segment's execution time, and $c$ signifies the maximum power of the *CPU* [38] in wireless communication. Alternatively, all the vehicles need to register once with the *VIS* and authenticate and communicate without *VIS*. Therefore, the energy cost is also calculated on the authentication and communication phases. As per the proposed protocol structure, the energy cost of authentication and communications are 5.35mJ and 1.38mJ, respectively. Therefore, the total cost for a single communication is 6.73mj. However, authentication is not needed to further communication as per the proposed scheme. Therefore, the cost for 10, 30, and 50 iterations are 19.13mJ, 45.69mJ, 74.25mJ, respectively. On the other hand, the iterative communication cost in the same set of vehicles is much higher than the proposed algorithm (see Fig. 8(d)). The extensive comparison of the energy cost on recent related works shows that the proposed scheme is better in single communication as well as iterative message transfer with identical vehicles, which confirms the lightweight feature.

It has been seen that the performance of the proposed protocol outperformed other existing related authentication schemes in every sector, not only in comparison with the single communication but also in the multi-communication environment.

## VII. Simulation and Evaluation

The practicality and the viability of the proposed protocol are tested on the popular network simulator NS-3. Moreover, the simulation for urban mobility (*SUMO*) is used to create the vehicular environment's mobility. On the other hand, the message passing during the authentication and communication among the vehicles are used for the environment and compared with the existing prior model [8-10]. Furthermore, NetAnim, a useful animation model, is used to capture the animation (see Fig. 9) of the message transfer during the simulation. The specification of the experimental environments is shown in Table 6.

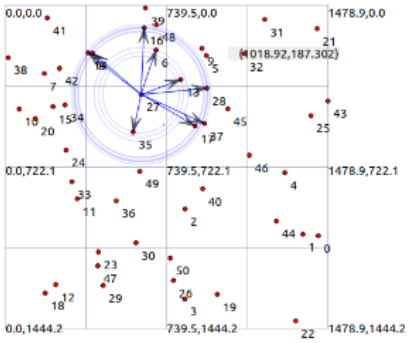



Fig. 9. A glimpse of message transfer in NetAnim tool.

TABLE 6
SIMULATION PARAMETERS

| Parameters | Value |
|---|---|
| Simulation Area | 1500 x 1500 (m2) |
| Routing Protocol | AODV |
| Communication Protocol | IEEE 802.11p |
| Mobility Model | Random Way Point |
| Speed of the vehicles | 50 Km/h to 80 Km/h |
| Channel Bandwidth | 5.9 GHz |
| Simulation Time | 70 s |

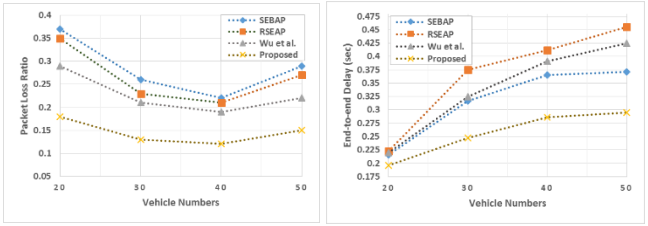
### Average Packet Loss Ratio (PLR)

Packet loss of a network can be measured using parameters of total send packets and complete received packets. PLR is happed due to various reasons such as bandwidth, distance, loss model, mobility model, and execution. We have calculated the PLR as per the following equation.

$$PLR = \frac{\sum N_{tx} - \sum N_{rx}}{\sum N_{tx}} \; x \; 100\% \tag{12}$$

Where, $\sum N_{tx}$ and $\sum N_{rx}$ are the number of transfer packets and received packets, respectively.

The experiment is done on the different densities of the on-road vehicles, such as 20, 30, 40, and 50. Average packet loss of the authentication schemes decreases as the vehicle density increase. (See Fig. 10) However, slight changes in the pattern in PLR have been noticed from the scenario of vehicles 40 to 50. The proposed protocol has shown a significant result among others as 0.18, 0.13, 0.12, and 0.15 in 20 vehicles, 30 vehicles, 40 vehicles, and 50 vehicles scenario, respectively.




*(a)* *(b)*

Fig. 10. NS3 simulation result. (a) the packet loss ratio vs. the vehicle density, and (b) the end-to-end delay vs. vehicle density.

### Average End-to-End Delay (E2ED)

The end-to-end delay is measured based on the difference between the send packets' timing and the received packet's timing, which is represented in (2).

$$E2ED = \frac{1}{N_{rx}} \left( \sum T_{rx} - \sum T_{rx} \right) \tag{13}$$

Where $N_{rx}, N_{rx},$ and $N_{rx}$ are the total number of sent packets, timestamp of the received packet, and timestamp of the transmitted packet, respectively.

The experiment is done based on the same scenario as described in *PLR* section. Fig. 10(b) shows the E2ED comparison of the proposed protocol with existing authentication schemes. Results deprecate that the message receiving delay increases with the number of vehicles increment. On the other hand, the proposed technique has a low delay compared to others as 0.196s, .0247s, 0.286s, 0.295s for 20 vehicles, 30 vehicles, 40 vehicles, 50 vehicles environment, respectively.

The implementation and simulation are the added advantages to understand the completeness of the proposed scheme. Moreover, the result clearly shows the significant benefits of the proposed protocol over the prior existing authentication schemes for VANET.

## VIII. Conclusion And Future Work

In this paper, an ECC-based secure and pseudo-identity-based privacy-preserving authentication protocol for VANET is proposed, which can solve the issue of *TA* dependency during the authentication and communication of a vehicle. Moreover, the proposed protocol creates an efficient balance between security and lightweight features. Alternatively, the message encapsulation during the transmission enhances the ability to transfer messages irrespective of secure and insecure channels. The experimental analysis showed that the proposed scheme outperforms the existing related models. On the other hand, the simulation of the proposed scheme proves reliability as well as acceptability. The mathematical proof of the protocol determines the correctness with real-world settings. The future scope of the research can be extended to the testbed experiment as well as the amalgamation with collaborative learning. Furthermore, the intrusion detection system can be implemented with the proposed protocol to develop network security.

## Acknowledgment

This work was supported in part by the University of Malaya Impact Oriented Interdisciplinary Research Grant under Grant IIRG008A-19IISS, and in part by the Ministry of Higher Education Malaysia Fundamental Research Grant Scheme (FRGS) under Grant FP055-2019A respectively. Authors thanks all the anonymous reviewers for making the manuscript powerful.

## References

[1] S. K. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. G. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Generation Computer Systems-the International Journal of Escience*, vol. 84, pp. 216-227, Jul, 2018.

[2] F. Qu, Z. Wu, F. Wang, and W. Cho, "A Security and Privacy Review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985-2996, 2015.

[3] T. Nandy, M. Y. I. B. Idris, R. M. Noor, M. L. M. Kiah, L. S. Lun, N. B. A. Juma'at, I. Ahmedy, N. A. Ghani, and S. Bhattacharyya, "Review on Security of Internet of Things Authentication Mechanism," *IEEE Access*, vol. 7, pp. 151054-151089, 2019.

[4] P. Vijayakumar, V. Chang, L. Jegatha Deborah, B. Balusamy, and P. G. Shynu, "Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks," *Future Generation Computer Systems*, vol. 78, pp. 943-955, 2018/01/01/, 2018.

[5] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, and B. Balusamy, "Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks," *Cluster Computing*, vol. 20, no. 3, pp. 2439-2450, 2017/09/01, 2017.

[6] R. Vinoth, L. J. Deborah, P. Vijayakumar, and N. Kumar, "Secure Multifactor Authenticated Key Agreement Scheme for Industrial IoT," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3801-3811, 2021.

[7] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, "A Lightweight Privacy-Preserving Authentication Protocol for VANETs," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3547-3557, 2020.

[8] V. Kumar, M. Ahmad, A. Kumari, S. Kumari, and M. Khan, "SEBAP: A secure and efficient biometric-assisted authentication protocol using ECC for vehicular cloud computing," *International Journal of Communication Systems*, pp. e4103, 2019.

[9] V. Kumar, M. Ahmad, D. Mishra, S. Kumari, and M. K. Khan, "RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing," *Vehicular Communications*, vol. 22, pp. 100213, 2020/04/01/, 2020.

[10] L. Wu, Q. Sun, X. Wang, J. Wang, S. Yu, Y. Zou, B. Liu, and Z. Zhu, "An Efficient Privacy-Preserving Mutual Authentication Scheme for Secure V2V Communication in Vehicular Ad Hoc Network," *IEEE Access*, vol. 7, pp. 55050-55063, 2019.

[11] R. Kolandaisamy, R. M. Noor, I. Kolandaisamy, I. Ahmedy, M. L. M. Kiah, M. E. M. Tamil, and T. Nandy, "A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET," *Journal of Ambient Intelligence and Humanized Computing*, 2020/07/03, 2020.

[12] U. Rajput, F. Abbas, H. Eun, and H. Oh, "A Hybrid Approach for Efficient Privacy-Preserving Authentication in VANET," *IEEE Access*, vol. 5, pp. 12014-12030, 2017.

[13] I. Ali, and F. Li, "An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs," *Vehicular Communications*, vol. 22, pp. 100228, 2020/04/01/, 2020.

[14] B. Ying, and A. Nayak, "Anonymous and Lightweight Authentication for Secure Vehicular Networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 10626-10636, 2017.

[15] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467-2476, 2017.

[16] Y. Liu, Y. Wang, and G. Chang, "Efficient Privacy-Preserving Dual Authentication and Key Agreement Scheme for Secure V2V Communications in an IoV Paradigm," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2740-2749, 2017.

[17] L. Zhang, Q. H. Wu, J. Domingo-Ferrer, B. Qin, and C. Y. Hu, "Distributed Aggregate Privacy-Preserving Authentication in VANETs," *Ieee Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516-526, Mar, 2017.

[18] M. R. Asaar, M. Salmasizadeh, W. Susilo, and A. Majidi, "A Secure and Efficient Authentication Technique for Vehicular Ad-Hoc Networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 5409-5423, 2018.

[19] S. M. Pournaghi, B. Zahednejad, M. Bayat, and Y. Farjami, "NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET," *Computer Networks*, vol. 134, pp. 78-92, 2018/04/07/, 2018.

[20] S. Tangade, S. S. Manvi, and P. Lorenz, "Decentralized and Scalable Privacy-Preserving Authentication Scheme in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8647-8655, 2018.

[21] H. Zhong, B. Huang, J. Cui, Y. Xu, and L. Liu, "Conditional Privacy-Preserving Authentication Using Registration List in Vehicular Ad Hoc Networks," *IEEE Access*, vol. 6, pp. 2241-2250, 2018.

[22] N. Alangudi Balaji, R. Sukumar, and M. Parvathy, "Enhanced dual authentication and key management scheme for data authentication in vehicular ad hoc network," *Computers & Electrical Engineering*, vol. 76, pp. 94-110, 2019/06/01/, 2019.

[23] J. Cui, W. Xu, Y. Han, J. Zhang, and H. Zhong, "Secure mutual authentication with privacy preservation in vehicular ad hoc networks," *Vehicular Communications*, vol. 21, pp. 100200, 2020/01/01/, 2020.

[24] J. Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, "Extensible Conditional Privacy Protection Authentication Scheme for Secure Vehicular Networks in a Multi-Cloud Environment," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1654-1667, 2020.

[25] A. Vangala, B. Bera, S. Saha, A. K. Das, N. Kumar, and Y. H. Park, "Blockchain-Enabled Certificate-Based Authentication for Vehicle Accident Detection and Notification in Intelligent Transportation Systems," *IEEE Sensors Journal*, pp. 1-1, 2020.

[26] T. Nandy, R. M. Noor, M. Y. I. Idris, and S. Bhattacharyya, "T-BCIDS: Trust-Based Collaborative Intrusion Detection System for VANET." pp. 1-5.

[27] T. Zhang, and Q. Zhu, "Distributed Privacy-Preserving Collaborative Intrusion Detection Systems for VANETs," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 148-161, 2018.

[28] M. A. Al-shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of Authentication and Privacy Schemes in Vehicular ad hoc Networks," *IEEE Sensors Journal*, pp. 1-1, 2020.

[29] J. B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162-1182, 2011.

[30] T. Nandy, M. Y. I. B. Idris, R. M. Noor, I. Ahmedy, and S. Bhattacharyya, "An Enhanced Two-factor Authentication Protocol for V2V Communication in VANETs." pp. 171–176.

[31] D. Dolev, and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198-208, 1983.

[32] R. Canetti, and H. Krawczyk, "Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels." pp. 453-474.

[33] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-Based Authenticated Key Exchange in the Three-Party Setting." pp. 65-84.

[34] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.

[35] "AVISPA," 11 April 2020, 2020; http://www.avispa-project.org/.

[36] "SPAN," 11 April 2020, 2020; http://people.irisa.fr/Thomas.Genet/span/.

[37] H. Vasudev, and D. Das, "A Lightweight Authentication Protocol for V2V Communication in VANETs." pp. 1237-1242.

[38] D. He, C. Chen, S. Chan, and J. Bu, "Secure and Efficient Handover Authentication Based on Bilinear Pairing Functions," *IEEE Transactions on Wireless Communications*, vol. 11, no. 1, pp. 48-53, 2012.

**Tarak Nandy** (S'19) is currently pursuing a Ph.D. and serving as a Graduate Research Assistant in Computer System and Technology from the University of Malaya, Malaysia. His interest includes vehicular communication, IoT, cyber-physical security, ML, DL.

**Mohd Yamani Idna Idris** (M'19) received the Ph.D. degree in electrical engineering. He is currently an Associate Professor with the FCSIT, University of Malaya. His expertise is in the area of IoT, security systems, sensor, and signal/image processing

**Rafidah Md Noor** received the Ph.D. degree in computing from Lancaster University, U.K., in 2010. She is currently an Associate Professor with the FCSIT, University of Malaya. Her research interests are transportation systems, vehicular networks, wireless networks, QoS, and the IoT.

**Ainuddin Wahid Abdul Wahab** Received the PhD degree from Surrey University, UK. He is currently as an Associate Professor, and the Deputy Dean (Undergraduate) in FCSIT, University of Malaya, Malaysia. His research interests are Information Security, Network Security, Steganography, and Sensor.

**Sananda Bhattacharyya** received her M. Tech from India. She is an ad-hoc faculty in the IT in Maldives Business School, Maldives. Her area of interest is in network security, cryptography, data security, steganography.

**Raenu Kolandaisamy** received his his PhD degree at the University of Malaya, Malaysia. He is an assistant professor at the UCSI University, Malaysia. His research interest includes IoT, VANET, ITS, security and privacy.

**Muktar Yahuza** (S, 19) is currently pursuing a PhD degree in Computer Science from the University of Malaya, Malaysia. His area of research includes Information Security, Internet of Drones, and, Image processing.