Alkadhim Journal for Computer Science, Vol. 3, No. 2 (2025)

Open Access ISSN: 3007-1437 (Online), ISSN: 3007-1429 (Print)

IRAQI Academic Scientific Journals

Alkadhim Journal for Computer Science (KJCS)

Journal Homepage: https://alkadhum-col.edu.iq/JKCEAS

KJCS ALKADHIM JOURNAL FOR COMPUTER SCIENCE

LV2PA: A Lightweight Verification with Privacy-Preserving Authentication for Vehicular Communications

[1]Murtadha A. Alazzawi*, [1]Aqeel Luaibi Challoob, [2]Kai Chen, [2]Hongwei Lu

[1] Department of Computer Techniques Engineering, Imam Alkadhim University College, 10001, Baghdad, Iraq

[2] School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, 430074, China

Article information

Article history:

Received: November,22 2024

Accepted: June,22, 2025

Available online: June,25, 2025

Keywords:

Vehicular adhoc network (VANET), Chinese remainder theorem (CRT), Mutual authentication, Bloom filter

Corresponding Author:

Murtadha A. Alazzawi

murtadhaali@iku.edu.iq

DOI:

https://doi.org/10.53523/ijoirVolxIxIDxx

Abstract

Security and privacy must be taken into account for vehicular ad-hoc networks (VANETs) due to the fact that broadcasting occurs through an open communication channel. This work offers a Lightweight Verification with Privacy-Preserving Authentication (LV2PA) approach for vehicular communications to overcome these challenges. To satisfy security and privacy requirements, the proposed LV2PA approach employs not only the cryptographic hash function, but also a Bloom filter and the Chinese remainder theorem. During the mutual authentication of the LV2PA scheme, only the first roadside unit (RSU) and on-board unit are required to communicate with a trusted authority (TA) due to the changeover use, however the other RSUs in vehicular communications do not require TA communication. Consequently, bottleneck problems for the TA are avoided. In addition, the RSU updates the shared group key whenever a vehicle joins or departs the group; hence, the proposed LV2PA provides complete forward secrecy and backward secrecy for vehicular communications. The formal (Burrows–Abadi–Needham (BAN) logic) and informal security analyses demonstrate that the proposed LV2PA scheme is legitimate and meets the security and privacy requirements, respectively. In terms of computing and communication expenses, the performance evaluation of the proposed LV2PA scheme has advantageously low overhead and low latency compared to state-of-the-art schemes

1. Introduction

One subset of Mobile Ad-hoc Network (MANETs), vehicular ad hoc networks (VANETs) are enabled by mobile nodes, or automobiles equipped with wireless networking capabilities. [1]. Vehicular communications not only enhance reliability for intelligent transportation system development but also provides traffic and safety information exchange to vehicle drivers [2], [3]. Figure 1 shows how the major entities of vehicular communications. Many onboard units (OBUs), some roadside units (RSUs), and a trusted authority (TA), communicate with one another using the dedicated short-range communication (DSRC) protocol. The OBU is a

vehicle-mounted unit, the RSU is a node in the roadside infrastructure, and the TA is in charge of overseeing the entire system [4].

To improve traffic roadways and reduce traffic jams and road accidents, the vehicle exchanges safety-related-message with other vehicles via vehicle-to-vehicle (V2V) communication or with adjacent RSUs via vehicle-to-infrastructure (V2I) communication. Still, before using the received information to make a decision, the receiving entities (vehicle or RSU) should validate the correctness and authenticity of these signals. Moreover, private details like the car's name and where it is parked need to be protected from any unauthorized nodes. Forged messages and unlawful nodes that seek to prevent them from traveling via vehicular communications raise serious security and privacy concerns. Moreover, the private data stored in a car needs to be safeguarded. Disrupting vehicle communications due to forged messages and unlawful nodes can lead to traffic congestion and accidents. However, in a heavy-traffic location with a high population density, automobiles or RSUs may receive safety-related messages from up to 180 vehicles within a 300 ms, necessitating the recipient to examine about 600-2000 messages each second [5]. Therefore, the performance overheads in terms of computing and communication costs are also key difficulties that should be addressed as soon as possible, in addition to the security and privacy concerns in vehicle communications. Before expanding the use of vehicle communications, it's important to solve these problems.

To address these issues, this paper proposes a lightweight verification with privacy-preserving authentication (LV2PA) scheme that is both efficient in terms of computational and communication costs and yet robust enough to address the study's stated security and privacy goals. By employing a Bloom filter, Chicness remainder theorem techniques, and a cryptographic hash function, the proposed LV2PA scheme satisfies the design goals in terms of security and privacy without necessitating preloading the master private key of the system onto the TPD (tamper-proof device) of the vehicle. Moreover, the proposed LV2PA approach makes use of V2V and V2I communications within vehicular communications; a registered vehicle first executes authentication of V2I with a nearby RSU and can then occur in the communication of V2V. As a result, the vehicle is unable to communicate mandatory safety-related communications without first executing V2I authentication, which ensures that only registered vehicles can share messages.

The main contributions of this paper are as follows:

1) Proposed LV2PA Scheme: A lightweight and privacy-preserving authentication protocol that significantly reduces computational and communication overhead by minimizing message size during generation and verification.
2) Conditional Anonymity: Vehicles remain anonymous unless suspicious behavior is detected, preserving privacy while allowing for accountability.
3) Scalable Authentication: Mutual authentication requires communication with the TA only during initial registration and handover; subsequent RSU interactions occur locally, avoiding TA bottlenecks.
4) Formal Security Verification Using BAN Logic: The proposed LV2PA scheme has been formally analyzed using the Burrows–Abadi–Needham (BAN) logic to verify its security properties, ensuring that critical authentication goals—such as message integrity, entity authentication, and key freshness—are correctly achieved.

The remaining sections of this work are laid out as follows. In Part II, we will look at the various authentication methods used in vehicle-to-vehicle communications. The preliminaries can be found in Section III, while the stages of the proposed LV2PA concept are outlined in Section IV. Sections V and VI introduce security analyses and performance evaluation, respectively. The final part of this paper offers a summary of the work done.

2. Related Work

For several vehicular communication methods, researchers have examined and discussed security and privacy concerns. Existing security and privacy schemes can be broadly grouped into two broad categories, as follows:

2.1 Public key infrastructure-based schemes

Public key infrastructure (PKI) was used by Raya and Hubaux [6] as the foundation for their protection model, and PKI was modified to meet the authentication and integrity needs of vehicle-to-vehicle communication. Nonetheless, the attacker can sow confusion in the system because in their scheme TA preloads a huge number of certificates and public-private pairs to each vehicle, and these certificates are updated at the beginning of each period. To protect the anonymity of the vehicle's identity in vehicular communications, Rajput et al. [7] suggested a privacy-preserving pseudonymous authentication technique. The vehicle's onboard memory is insufficient for storing crucial data like certificates and public-private keys for their system. The TA also creates a certification revocation list (CRL) to eliminate invalid nodes, but this CRL will be so extensive that it will be of little use. Using the concept of a group of cars as an ID, Lin et al. [8] developed a GSIS system that combines ID-based signatures with group signatures. To provide conditional privacy, their plan conceals the individual identities of its participants. The fundamental drawback of this approach, however, is the identity escrows problem, and selecting a group manager is a difficult task. [9].

2.2 Identity-based schemes

Several researchers [10]– [13] have proposed identity-based schemes as a way to address problems with PKI-based schemes. In these schemes, the verifier utilizes the sender's public key, which contains identifying information, to verify the sender's identity and the message's authenticity. There is no need for extra computational overhead or memory space because this technique does not preload a large number of certificates and public-private pairs to each vehicle. These schemes are adjusted without the use of a CRL as well. However, their technique involves bilinear pairing procedures, which introduce a huge computational burden into the process of verifying signatures. More importantly, their schemes are vulnerable to valuable insider assaults since they do not meet the vehicle's privacy-preserving and revocation requirements. Several studies have employed elliptic curve cryptography (ECC) procedures in place of bilinear pair operations to deal with the enormous calculations overhead load of these methods [14–18]. Though these techniques can lessen computational burden, they are still susceptible to insider assaults and revocation processes. Alazzawi et al. [19] developed a method for signing and confirming communications' authenticity and integrity using ECC. In developing a VANET based Privacy-Preserving Communication Scheme, Al-shareeda at el., [20] referenced the work of Alazzawi et al., [19]. (VPPCS). The technique presented in [19] and [20] still has substantial communication and calculation costs during broadcasting, but this is a significant improvement. Ming et al. [22], Kamil and Ogundoyin [23], and Ming et al. [24] all use ECC with uncertificated cryptography, which was first developed by Al-Riyami and Patersos [21]. The KGC generates a partially secret key so that the car can generate a fully secret key without the KGC's knowledge. As a result, their protocols account for identity escrow issues.

Identity-based systems were developed by Cui et al. [25], Zhong et al. [26], Cui et al. [27], [28], and Zhang et al. [29] to protect RSU-based vehicle communications. For the purpose of protecting communications between vehicles, Cui et al. [25] proposed an ECC-based authentication technique that makes use of a cuckoo filter to ensure confidentiality. Under their plan, the cuckoo filter keeps the received safety-related messages in two distinct piles, one for messages whose authentication was successful and another for those whose authentication was not. Additionally, filters accompanying each alert message are dispersed according to a predetermined plan. Receivers will use cuckoo filters to determine the legitimacy of the safety-related communications after they have been received. Similarly, Zhong et al. [26] devised authentication techniques with a lower performance overhead by replacing the cuckoo filter and the ECC with the Bloom Filter (BF) and a cryptographic hash function. An authentication approach based on privacy-preserving cuckoo filter notifications was presented by Cui et al., [27], wherein RSUs rely on neighboring vehicles to efficiently validate received messages and subsequently deliver the notification outcomes within their covered region.

Using the conditional random token (CRT) and a cryptographic hash function, Cui et al. [28] offer the conditional privacy-preserving authentication and group-key agreement (HCPA-GKA) technique for exchanging the group key between vehicles inside the RSU's coverage area. Each vehicle has its own key to decipher the encrypted messages sent to it via the HCPA-symmetric GKA's AES and group key. However, they are vulnerable to insider attacks since they do not satisfy the non-repudiation and revocation requirements in their work. By segmenting the system into many domains, Zhang et al. [29] proposed an authentication strategy using ECC instead of the AES algorithm. Their plan, however, may lead to TA bottleneck issues due to inefficient latency and processing cost, as well as repetitive handovers.

2.3 Limitations in Prior Work and LV2PA Contributions

While existing solutions have advanced the field, many suffer from at least one of the following:

1) High computational or communication overhead,
2) Centralized dependence on the TA,
3) Inefficient revocation or group management,
4) Lack of formal verification of security claims.

To address these limitations, we propose the LV2PA (Lightweight Verification with Privacy-Preserving Authentication) scheme. Unlike prior works:

1) LV2PA avoids preloading master keys or excessive certificate management.
2) It employs Bloom filters, Chinese Remainder Theorem, and cryptographic hash functions to ensure efficient and secure authentication without incurring high computational loads.
3) Unlike Cui et al. [28] and Zhong et al. [26], LV2PA provides formal security validation using BAN logic, strengthening the credibility of its privacy and authentication claims.
4) The scheme minimizes reliance on TA after initial registration, thus ensuring scalability in high-density vehicular networks.
5) Finally, LV2PA significantly reduces communication and computation costs, as shown in our performance evaluation, while satisfying conditional anonymity and resistance to insider threats.

3. Preliminaries

In this section, we introduce the network model along with the concepts of the cryptographic hash function. The Chinese remainder theorem, and the Bloom filter as they pertain to the need for privacy and security in vehicular communications. The proposed LV2PA scheme's notations and their definitions are presented in Table 1.

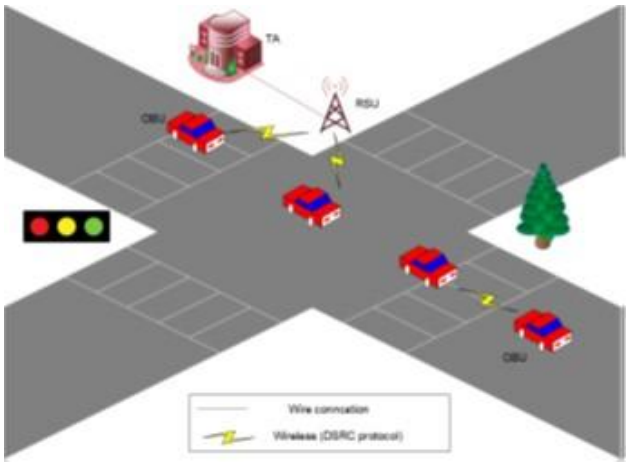


Figure. (1). Network model of vehicular communications

3.1 Network model

As seen in Fig. 1, the system model for the proposed LV2PA concept consists of three parts.

OBU: Vehicles equipped with this portable device can communicate with other OBUs or adjacent RSUs using the DSRC protocol to relay important safety information. A tamper-proof device (TPD) is included into every OBU to safeguard the confidential data it stores.

RSU: This is a piece of roadside infrastructure. RSU's primary function is to handle traffic-related notification messages and manage safety-related messages received between cars within its range. For the proposed LV2PA method to work, each incoming notification message must first be checked for legitimacy by the RSU, and only then will the results be transmitted. In addition, it transmits information on the outgoing vehicle to the receiving RSU as part of the handover procedure.

TA: This is a reliable organization that must register all other entities involved in car-to-car communication. It is also responsible for communicating with all RSUs through wire-channel technology and setting up the system's initial parameters.

3.2 Requirements of Privacy and Security

The proposed LV2PA scheme should be satisfied the security and privacy requirements in vehicular communications.

- Authentication and privacy-preserving: This guarantees the sender's authenticity without disclosing the true identity of the vehicle.
- Message integrity: This guarantees the validity of messages without changing.
- Unlikability: The adversary is not able to map two or more messages from the same signer.
- Traceability and revocation: The TA can trace and revoke any illegal vehicle in vehicular communications during a suspicious scenario.
- Non-repudiation: The signer cannot deny messages sent at another time.
- Security attack resistance: The proposed scheme can withstand attacks such as location tracking, Sybil, replay, bogus information, modification, Man-In-The-Middle (MITM), and impersonation.
- Forward secrecy and backward secrecy: After the vehicle leaves the group, it cannot get any data. In addition, before a joining vehicle joined the group, it cannot access previous data.
- Low overhead: The robust security and privacy scheme should be satisfied with a low overhead in terms of computation and communication costs.

3.3 Cryptographic hash function

The main work of the cryptographic hash function is to take arbitrary length data as input and computes a uniform, hash value of fixed length. It is a one-way function, in which tiny alters in the original data can lead to important alters resulting. Besides, for x and y, it is a hardness to compute f(x) = f(y) [30].

In the proposed LV2PA scheme, the cryptographic hash function is employed to ensure message integrity and to generate compact authentication tokens that help reduce computational overhead during message verification.

3.4 Chinese remainder theorem

The main idea of the Chinese remainder theorem is that the Euclidean division of an integer value n is known by anyone by various integer values [31]. He/she could matchlessly identify the division remainder of n by these integer values products under the situation that pairwise coprime divisors. Suppose that $\{x1; x2; \dots xn\}$ are pairwise prime relatively positive integers, where $n \geq 2$ and the set $X = x_1x_2 \dots x_n = x_1X_1 = x_2X_2 = \dots = x_nX_n$, where, $X_i = {}^{X}/_{x_i}$, $i = 1,2,3 \dots n$. The positive integer number of congruence Eq (1) is $k \equiv \sum_{i=1}^{n} y_iX_iX_i^{'} \equiv y_1X_1X_1^{'} + y_2X_2X_2^{'} + \dots + y_nX_nX_n^{'}(mod\ X)$, where $X_i^{'}$ is a positive integer number and meets the congruence equation $X_iX_i^{'} \equiv 1(mod\ x_i), i = 1,2,3 \dots n.$

$$\begin{cases} k \equiv y_1(mod\ x_1) \\ k \equiv y_2(mod\ x_2) \\ \quad \dots\dots. \\ k \equiv y_i(mod\ x_i) \end{cases} \qquad (1)$$

In LV2PA, the CRT technique is utilized to efficiently handle cryptographic computations by breaking down complex operations into smaller modular computations, which significantly improves processing speed without sacrificing security.

3.4 Bloom Filter (BF)

BF is a modern probabilistic data structure form that is utilized to store a pool of n items and verify whether an item is a member of this pool [32]. The main fundamental is to construct an array of m bits and firstly pool bits to zero. To add an item to the bloom filter, we calculate k times the hash function for this item, and then each value from this k hash function's results will map to a bit in the bloom filter. Lastly, all maps are set from bits to one, as pretested in Fig. 2. We execute the same k hash function to check whether or not an item is in the bloom filter. When all the included bits are mapped by the k hash function output in one, then the item is a member of the bloom filter; otherwise, it is not a member.

The LV2PA scheme leverages Bloom filters to rapidly and efficiently verify safety-related messages, drastically reducing memory usage and computational cost during message authentication in high-density vehicular networks.

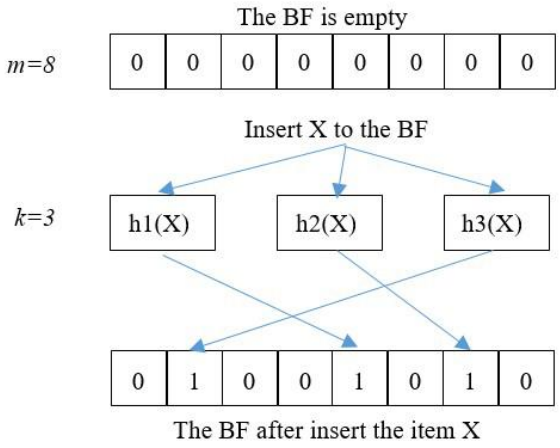


Figure. (2). The bloom filter (BF) Insertion

4. The LV2PA Scheme

A lightweight verification with privacy-preserving authentication scheme, that can effectively cope with the relevant security and privacy concerns with lightweight and efficient performance relying on computation and communication costs for vehicular communications is proposed. The six phases included in the LV2PA scheme are presented as follows. The phase of initialization, phase of registration, phase of shared group key generation, phase of mutual authentication, phase of handover, and phase of broadcasting and verifying. After the TA initializes the parameter of the system, the rest entities are registered in vehicular communications. The RSU then computes a shared group key based on the Chinese remainder theorem in the phase of shared group key generation, which will be renewed when a registered vehicle is revoked by TA or joins or leaves the group.

The vehicle and RSU will be able to send and receive safety-related messages after completing a mutual authentication process. The vehicle communicates with the RSU-protected area using a lightweight authentication mechanism. In vehicular communications, the vehicle authenticates itself with the TA via the first RSU; subsequent RSUs do not require the TA's participation in this initial authentication. The RSU will change the group key after the registered vehicle has left the group. An illustration of the vehicle's operation under the proposed LV2PA concept is provided in Fig. 3.

Table (1) : Definition Of Notations In This Paper

Notation	Descriptions
p, q	substantial prime numbers
h	Hashing function for encryption
TID_v, TID_r	Real identities of the Vehicle and RSU
T_V^{Reg}, T_R^{Reg}	Time of vehicle registration and that of the RSU
$PID_v\ PID_r$	Vehicle's and ASU's fictitious names
M	A message relating to traffic
Sk	The collective group key
$Alist$	All vehicle information is contained in the list on the RSU
RL_v, RL_r	Vehicle registration list
$TList$	Permanent handshake list
$T,\ \triangle T, Tr, T_{1-4}$	Timestamps

This example illustrate the processing stages. In stage (A), TA is responsible to authenticate vehicles during mutual authentication. In stage (B), the vehicle sends safety-related messages. Stage (C), explains how the LV2PA scheme addresses the problem of handover, which does not cause TA bottlenecks. Nevertheless, once the vehicle moves from the current RSU to the next one, the current RSU will send the information of the vehicle to the next via a secure channel. In this stage, the information of the vehicle is known by the new RSU which can determine whether it is authentic or unauthentic without supporting the TA. In the last stage, the safety-related messages are again started to be broadcast by the vehicle within the newly covered area by RSU.

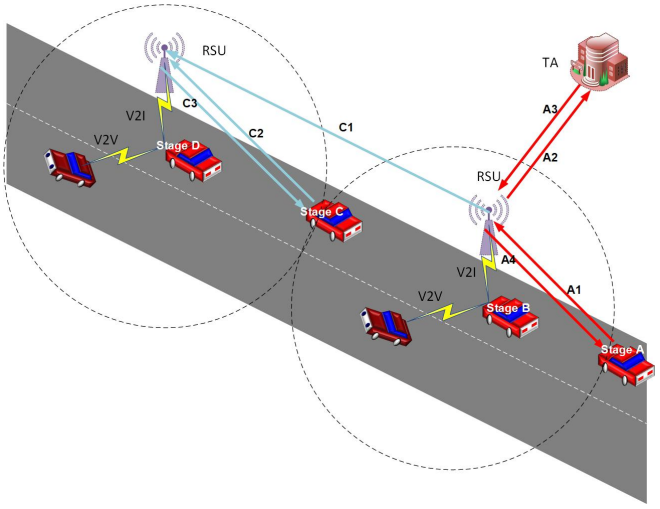


Figure. (3). The proposed LV2PA scheme works.

4.1 Phase of initialization

This phase initializes the parameters of the system by TA as below,

1) To choose the necessary random numbers and the shared group key, the TA first produces two huge prime numbers, p, and q, where $p > q$ and $q \leq [p/4\ ]$.
2) TA selects a cryptography hash function h.
3) The TA propagate and update $\{p, q\ , h\}$ parameters periodically.

4.2 Phase of registration

The TA registers the RSU and OBU as follows:

RSU registration:

The TA registers RSU to obtain the relevant parameters as follows:

1) TA obtains the true identity TID_r from the RSU.
2) TA produces a random integer (INT) number $m_r \in Z_q^*$.
3) TA gets the registering time T_R^{Reg}
4) TA stores $\{TID_r, m_r, T_R^{Reg}\}$ to the registration list RL_r
5) TA preloads $\{TID_r, m_r, T_R^{Reg}\}$ to the RSU.

OBU registration

The TA registers OBU to obtain the relevant parameters as follows:

1) True identity (TID_v) and password (PWD) for the vehicle is selected by TA.
2) TA produces a random INT number $m_v \in Z_q^*$.
3) TA gets the registration time T_V^{Reg}
4) TA stores $\{TID_v, m_v, PWD, T_V^{Reg}\}$ to the registration list RL_v
5) TA preloads $\{TID_v, m_v, PWD, T_V^{Reg}\}$ into each TPD on the OBU of the vehicle.

4.3 The phase of shared group key generation

Each RSU creates and publishes a shared group key reling on the Chinese theorem:

1) Following the mutual authentication step, RSU re-numbers the random INT number x_i that was given to each vehicle at random. The matched random INT numbers are numbered as $x_1, x_2, x_3, \ldots x_n$ if there are n authentic automobiles.
2) The RSU chooses a random number (integer) Sk less than q.
3) The RSU computes $(\omega = \prod_{i=1}^{100} x_i)$, $(\alpha_i = {}^{\omega}/_{x_i})$, $(\beta_i$ such that $\alpha_i.\beta_i \equiv 1(mod\, x_i))$, $(\lambda_i = \alpha_i.\beta_i)$, $(\varphi = \sum_{i=1}^{100} \lambda_i)$ and $(\gamma = \varphi.Sk)$.
4) The RSU broadcasts $\{T, \gamma, \sigma_{Sk}\}$, where $\sigma_{Sk} = h(T \parallel Sk)$.
5) Once the OBU has received the message $\{T, \gamma, \sigma_{Sk}\}$, it determines whether the timestamp T is the most recent by determining whether $(\triangle T > Tr - T)$ is true. If not, the message is declined; if it is accepted, the following procedures are followed.
6) The OBU computes the group key $Sk = \gamma \, mod \, x_i$ and checks if $\sigma_{Sk} = h(T \parallel Sk)$. If not, the communication is rejected; if so, Sk begins broadcasting real beacons.

4.4 The phase of mutual authentication

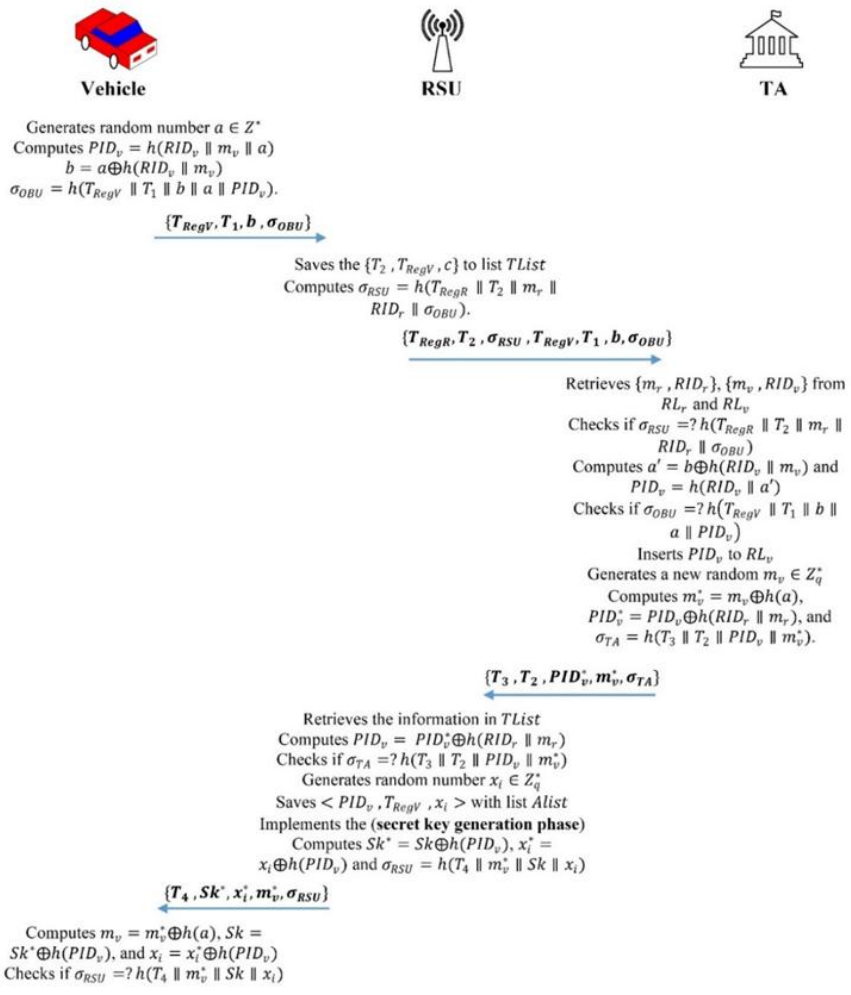
A robust mutual authentication is executed by OBU_i with the first RSU_j through the TA (mutual authentication of subsequent with other RSUs does not require to contain the TA, as demonstrated in the next phase). The driver of the vehicle should submit the own PWD and TID_v into the TPD on OBU_i for initializing. Once the vehicle joins the coverage area by the first RSU_j, the next steps are executed.

1) OBU_i- To - RSU_j: The OBU_i generates a random integer $a \in Z^*$ and computes $PID_v = h(TID_v \parallel m_v \parallel a)$ and $b = a \oplus h(TID_v \parallel m_v)$. Then, the OBU_i computes the signature $\sigma_{OBU} = h(T_V^{Reg} \parallel T_1 \parallel b \parallel a \parallel PID_v)$. Finally, it sends $\{T_V^{Reg}, T_1, b, \sigma_{OBU}\}$ to the RSU_j.
2) RSU_j- To - TA: When it receives the message $\{T_V^{Reg}, T_1, b, \sigma_{OBU}\}$, the RSU_j carries out the subsequent steps:
   - It determines the timestamp T_1 to see if it is the latest, i.e. the RSU_j checks whether $(\triangle T > Tr - T_1)$, where $\triangle T$ refer to pre-set time value and Tr is the receiving time.
   - It keeps the information $\{T_2, T_V^{Reg}\}$ to a temporary handshake list $TList$.
   - It computes $\sigma_{RSU} = h(T_R^{Reg} \parallel T_2 \parallel m_r \parallel TID_r \parallel \sigma_{OBU})$.
   - Finally, it sends $\{T_R^{Reg}, T_2, \sigma_{RSU}, T_V^{Reg}, T_1, b, \sigma_{OBU}\}$ to the TA.
3) TA - to - RSU_j: When TA receives the message $\{T_R^{Reg}, T_2, \sigma_{RSU}, T_V^{Reg}, T_1, b, \sigma_{OBU}\}$, it uses the next actions.
   - It determines the weather of the timestamp T_2 is it newest, i.e. the TA checks the value of $\triangle T, \, where \, (\triangle T > Tr - T_2)$. If $(\triangle T < Tr - T_2)$ the the subsequent steps are carried out.

- The TA retrieves $\{m_r , TID_r\}$, $\{m_v , TID_v\}$ from RL_r and RL_v according to T_R^{Reg} and T_V^{Reg} respectively.
- The TA checks whether $\sigma_{RSU} = ? h(T_R^{Reg} \| T_2 \| m_r \| TID_r \| \sigma_{OBU})$. If this is false, the following steps are carried out.
- TA computes $a' = b \oplus h(TID_v \| m_v)$ and $PID_v = h(TID_v \| a')$, and then checks whether $\sigma_{OBU} = ? h\left(T_V^{Reg} \| T_1 \| b \| a \| PID_v\right)$. The message is denied if they don't match; otherwise, the subsequent actions are taken.
- The TA inserts PID_v into RL_v and updates the number m_v by generating a new random number $m_v \in Z_q^*$.
- Finally, the TA sends $\{T_3 , T_2 , PID_v^*, m_v^*, \sigma_{TA}\}$ to the RSU_j, where $PID_v^* = PID_v \oplus h(TID_r \| m_r)$, $m_v^* = m_v \oplus h(a)$, and $\sigma_{TA} = h(T_3 \| T_2 \| PID_v \| m_v^*)$.

4) RSU_j- to OBU_i: When RSU_jreceives the message $\{T_3 , T_2 , PID_v^*, m_v^*, \sigma_{TA}\}$, it carries out the following steps:
- The RSU_jchecks the timestamp T_3 to see whether is it the latest, i.e. the RSU_jchecks whether ($\triangle T > Tr - T_3$) holds. If not, the message is rejected; else, the succeeding steps are carried out.
- The RSU_jretrieves the information in $TList$ according to T_2.
- The RSU_jcomputes $PID_v = PID_v^* \oplus h(TID_r \| m_r)$.
- The RSU_jchecks whether $\sigma_{TA} = ? h(T_3 \| T_2 \| PID_v \| m_v^*)$. Else, the following steps are carried out.
- The RSU_jgenerates a random integer $x_i \in Z_q^*$.
- The RSU_j saves $< PID_v , T_V^{Reg} , x_i >$ upon using the authentication $Alist$, this details each genuine automobile available in its line.
- The RSU_jimplements the group key generation phase to maintain backward secrecy for the group, which prevents the new vehicle from accessing previous group information.
- Finally, the RSU_j sends $\{T_4 , Sk^*, x_i^*, m_v^*, \sigma_{RSU}\}$ to the OBU_i where $Sk^* = Sk \oplus h(PID_v)$, $x_i^* = x_i \oplus h(PID_v)$ and $\sigma_{RSU} = h(T_4 \| m_v^* \| Sk \| x_i)$.

5) OBU_i: When the RSU_jreceives the message $\{T_4 , Sk^*, x_i^*, m_v^*, \sigma_{RSU}\}$, it applies the following steps:
- The OBU_ichecks the timestamp T_4 to see whether is it the latest, i..e the OBU_ichecks whether ($\triangle T > Tr - T_4$) holds. If not, the message is rejected; if it is, subsequent actions are taken.
- The OBU_icomputes $m_v = m_v^* \oplus h(a)$, $Sk = Sk^* \oplus h(PID_v)$, and $x_i = x_i^* \oplus h(PID_v)$.
- The OBU_i checks whether $\sigma_{RSU} = ? h(T_4 \| m_v^* \| Sk \| x_i)$. Unless, the message is rejected; else, complete mutual authentication and the OBU_i is prepared to broadcast beacons with the common group key Sk, which will be saved with the number x_i in TPD; at the same time, the vehicle will update the



saved number m_v with the received one.

Figure. (4). The mutual authentication steps with first RSU

4.5 Phase of handover

This phase explains how Sk is updated by RSU after leaving the vehicle the current RSU's coverage range and joins a coverage range of the new RSU, as well as shows how a mutual authentication with the new RSU is executed by leaving the vehicle. When the vehicle leaves are considered a member of the new group of RSU, which does not allow the vehicle obtains a new Sk for the previous group of RSU. The major aim of the handover phase is to offer forward secrecy and backward secrecy for vehicular communications as well as to mitigate the TA bottleneck problem since it is mitigated the computation overhead during mutual authentication.

1) When a vehicle leaves the range of an RSU, the following steps are implemented:
   - When a vehicle leaves the current RSU group, the current RSU notifies the next RSU by sending a secure message containing the information $< PID_v, T_V^{Reg}, x_i >$ about the leaving vehicle. The new RSU stores the vehicle's information on a special temporary list. This is used to save received information about a vehicle from nearby RSUs for a short time, and if the RSU does not receive a joining message from the vehicle, it removes this information from the list.
   - Following this, the current RSU and the vehicles within the current RSU's range update the Sk by implementing the group key generation phase after eliminating information from the leaving vehicle.
2) When the leaving vehicle creates a mutual authentication with a new RSU, the following steps will be implemented:
   - The vehicle sends a joining message to the new RSU. The content of the message is $\{T_1, \sigma_{OBU}\}$, where $\sigma_{OBU} = h(T_1 \parallel PID_v \parallel T_V^{Reg} \parallel x_i)$.
   - When the new RSU obtains the message $\{T_1, \sigma_{OBU}\}$, It examines the timestamp.T_1 to check the whether it is the latest. The message is rejected if it doesn't match the hash value of the data in the special temporary list with T_1 using $\sigma_{OBU} = ? h(T_1 \parallel PID_v \parallel T_V^{Reg} \parallel x_i)$. If it does, the message is accepted. If not, the message is rejected; otherwise, the new RSU saves the information of the vehicle $< PID_v, T_V^{Reg}, x_i >$ into $Alist$.
   - Following this, the new RSU and the vehicles within the new RSU's range update the Sk by implementing the group key generation phase.

4.6 The phase of broadcasting and verifying

The OBU's broadcasting and beacon verification processes in this phase describe. The three steps of this phase are as follows:

- **Broadcasting:** beacons begin to be broadcast by the OBU. The beacon is consist of $\{T, M, V, \sigma_m\}$, where $V = h(x_i \parallel T)$ and $\sigma_m = PID_v \oplus h(T \parallel M \parallel V \parallel Sk)$.
- **Notification Message:** the beacon is checks the timestamp T to see whether is it the latest, i.e. the RSU checks whether $(\triangle T > Tr - T)$. Else, the message is rejected; then, the following steps are carried out:

1) The RSU computes $PID_v = \sigma_m \oplus h(T \parallel M \parallel V \parallel Sk)$.
2) The RSU retrieves x_i from $Alist$ according to PID_v and checks whether $V = ? h(x_i \parallel T)$. In the absence of such, it adds V's hash value to the negative BF. Else, adds V's hash positive BF. The hash values of legal beacons are saved by the positive BF, while those of illegal beacons are saved by the negative BF.
3) Finally, the RSU then sends the notification message after adding the BF.
   - **Verification:** The OBU analyzes the timestamp T to see if it is the latest when it receives a beacon $\{T, M, V, \sigma_m\}$ from a vehicle and the notification message from the RSU. In other words, the OBU determines the value of $\triangle T$ $where$ $(\triangle T > Tr - T)$ holds. If not, the message is rejected; if it does, it looks to see if the Bloom filters contain V's hash value. As shown in Table II, there are three conceivable outcomes for the OBU.

Table (2) : Search Outputs

Case	Positive BF	Negative BF	Outcome
1	T (True)	F	Valid
2	F (False)	T	Invalid

3	F	F	Waiting

In Case 1, the RSU retrieved the beacon from a legal vehicle, in Case 2, it was recovered from an illegal vehicle, and in Case 3, the RSU didn't even look at the beacon. Therefore, the verification process must wait till the OBU receives the subsequent notification message from the RSU.

5. Security Analyses

Burrows-Abadi-Needham (BAN) (BAN) [33] Here we employ logic to show how the proposed LV2PA scheme's OBU and RSU may authenticate each other. Additionally, we show that the suggested LV2PA scheme is capable of meeting security and privacy needs..

5.1 Formal security analysis

The OBU and RSU's trustworthiness in their shared key and mutual authentication proof is established by employing BAN logic. The proposed LV2PA technique accomplishes the intended results because of the use of BAN logic. Here, we skip through the introductory material for BAN logic and instead direct the reader to [34-35] for more information.

Designed goals: The following aims will help meet the necessary authentication standards for vehicular connections.

Goals. If proposed scheme can accomplish the specific goals, then it will satisfy the essential needs of authentication for VANETs:

- **Goal1**: $TA|\equiv OBU| \equiv (a, PID_v)$
- **Goal2:** $TA|\equiv RSU| \equiv (\sigma_{RSU})$
- **Goal3**: $RSU| \equiv (\text{RSU} \overset{PID_v}{\longleftrightarrow} \text{OBU})$
- **Goal4:** $OBU|\equiv TA| \equiv (m_v)$
- **Goal5:** $OBU|\equiv RSU| \equiv (Sk, x_i)$

The idealized form. The following illustrates how proposed scheme plan has changed:

1) The protocol messages are:
   - **PM1**: OBU → RSU: $\{T_{RegV}, T_1, b, \sigma_{OBU}\}$.
   - **PM2:** $RSU \rightarrow TA$: $\{T_R^{Reg}, T_2, \sigma_{RSU}, T_V^{Reg}, T_1, b, \sigma_{OBU}\}$
   - **PM3:** $TA \rightarrow RSU$: $\{T_3, T_2, PID_v^*, m_v^*, \sigma_{TA}\}$
   - **PM4:** $RSU \rightarrow OBU$: $\{T_4, Sk^*, x_i^*, m_v^*, \sigma_{RSU}\}$
2) The protocol messages are idealized by:
   - **IM1:** OBU → TA: $(a, PID_v)_{h(TID_v \| m_v)}$
   - **IM2:** $RSU \rightarrow TA$: $(\sigma_{RSU})_{PID_v}$
   - **IM3:** $TA \rightarrow RSU$: $(\text{RSU} \overset{PID_v}{\longleftrightarrow} \text{OBU})_{h(TID_r \| m_r)}$
   - **IM4:** $TA \rightarrow OBU$: $(m_v)_{h(TID_v \| m_v)}$
   - **IM5:** $RSU \rightarrow OBU$: $(Sk, x_i)_{h(PID_v)}$

Assumptions. Our scheme's proof is based on the following notions:

- **A1:** RSU| $\equiv \#(T_1, T_3)$
- **A2:** TA| $\equiv \#(T_2)$
- **A3:** OBU| $\equiv \#(T_4)$
- **A4:** $OBU| \equiv OBU \overset{TID_v, m_v}{\longleftrightarrow} TA$
- **A5:** $TA| \equiv OBU \overset{TID_v, m_v}{\overset{TID_r, m_r}{\longleftrightarrow}} TA$
- **A6:** $RSU| \equiv RSU \overset{TID_r, m_r}{\longleftrightarrow} TA$
- **A7**: $TA| \equiv RSU \overset{PID_v}{\longleftrightarrow} TA$
- **A8:** $RSU| \equiv TA \Rightarrow RSU \overset{PID_v}{\longleftrightarrow} OBU$
- **A9:** $OBU| \equiv RSU \overset{PID_v}{\longleftrightarrow} OBU$

Proof. The proof is applied as the following:

Based on **IM1**, we get

- **S1:** TA $\lhd (a, PID_v)_{h(TID_v \| m_v)}$

Based on **S1, A5**, and by using **the message meaning rule**, we get

- **S2:** $TA|\equiv OBU|\sim(a, PID_v)$

Using S2, A2, the freshness rule, and the freshness rule, we obtain

- **S3**: $TA|\equiv OBU| \equiv (a, PID_v)$ **Goal1**

Based on **IM2**, we get

- **S4:** TA $\triangleleft$ (σ_{OBU})

Based on **S4, A7**, and by using **the message meaning rule**, we get

- **S5:** $TA|\equiv RSU|\sim(\sigma_{OBU})$

Based on S5, A2, and by using the freshness rule and nonce-verification rule, we get

- **S6:** $TA|\equiv RSU| \equiv (\sigma_{OBU})$ **Goal2**

Based on IM3, we get $_{PID_v}$

- **S7:** RSU $\triangleleft$ (RSU $\overset{PID_v}{\longleftrightarrow}$ OBU)$_{h(TID_r\|m_r)}$

Based on S7, A6, and by using the message meaning rule, we get

- **S8:** $RSU|\equiv TA|\sim$(RSU $\overset{PID_v}{\longleftrightarrow}$ OBU)

Based on S8, A1, and by using the freshness rule and nonce-verification rule, we get

- **S9:** $RSU|\equiv TA| \equiv$ (RSU $\overset{PID_v}{\longleftrightarrow}$ OBU)

Based on **S9, A9**, and by using **the Jurisdiction rule**, we get

- **S10:** $RSU| \equiv$ (RSU $\overset{PID_v}{\longleftrightarrow}$ OBU) **Goal3**

Based on IM4, we get

- **S11:** OBU $\triangleleft$ $(m_v)_{h(TID_v\|m_v)}$

Based on **S11, A4**, and by using the **message meaning rule**, we get

- **S12**: $OBU|\equiv TA|\sim(m_v)$

Based on S12, A3, and by using the freshness rule and nonce-verification rule, we get

- **S13:** $OBU|\equiv TA| \equiv (m_v)$ **Goal4**

Based on IM5, we get

- **S14:** OBU $\triangleleft$ $(Sk, x_i)_{h(PID_v)}$

Based on **S14, A9**, and by using **the message meaning** rule, we get

- **S15:** $OBU|\equiv RSU|\sim(Sk, x_i)$

Based on S15, A3, and by using the freshness rule and nonce-verification rule, we get

- S16: $OBU|\equiv RSU| \equiv (Sk, x_i)$ **Goal5**

Consistent with the above steps, we can easily deduce that our proposed scheme is capable of fulfilling all the above-mentioned goals. We can therefore say that our scheme is protected.

5.2 Informal Security Analysis

This subsection exhibits the safety and confidentiality of the planned LV2PA scheme. Table III shows how the proposed LV2PA scheme stacks up against competing approaches in terms of key privacy and security metrics.

1) In the proposed scheme, the genuine TID_v of the vehicle is known only to the TA, Privacy-preserving authentication. The beacon $\{T, M, V, \sigma_m\}$ broadcasts the authentication using a group key Sk, with $\sigma_m = PID_v \oplus h(T \| M \| V \| Sk)$ without disclosing the vehicle's TID_v. Therefore, our method meets all the criteria for private and secure authentication.
2) Without compromising the confidentiality of the sent data, the vehicle transmits the beacon coordinates $\{T, M, V, \sigma_m\}$ where $\sigma_m = PID_v \oplus h(T \| M \| V \| Sk)$. $PID_v = \sigma_m^{'} \oplus h(T \| M \| V \| Sk)$ is derived by using Sk as the group key. Therefore, the LV2PA scheme succeeds where message integrity is concerned.
3) Based on the beacon $\{T, M, V, \sigma_m\}$ where $V = h(x_i \| T)$ and $\sigma_m = PID_2 \oplus h(T \| M \| V \| Sk)$, we may determine that the vehicle transmits a unique signal each time. Our approach meets the unlinkability condition since an attacker can't link two beacons to the same vehicle.
4) Steps the TA can take to trace and revoke the malicious vehicle's access after receiving a report of fake messages sent from it are as follows,
   - As soon as the RSU receives the safety-related message "$\{T, M, V, \sigma_m\}$" from the malicious vehicle, it collects the vehicle's information as supplied in the second stage of the broadcasting and verification phase.
   - The RSU forwards $\{PID_v, T_V^{Reg}\}$ to TA.
   - Following the protocol of $\{PID_v, T_V^{Reg}\}$, the TA will get the real identity TID_v from the RL_v. The revocation is documented and the vehicle's information is removed from RL_v.
   - In order to prevent this vehicle from transmitting messages, the TA broadcasts informed the RSU of an updated list of revocations.
   - To eliminate the threat posed by the infected vehicle, the RSU first removes it from the a list, and then it

executes the shared group key generation phase, which causes Sk to be updated.
Therefore, the proposed LV2PA scheme for vehicular communications satisfies the conditions of traceability and revocation.

5) Nonrepudiation: Based on the value of σ_m in the beacon $\{T, M, V, \sigma_m\}$, which is computed as $\sigma_m = PID_v \oplus h(T \parallel M \parallel V \parallel Sk)$, where $V = h(x_i \parallel T)$, vehicles cannot send out the same beacon because each one has a different value for x_i. There is no way for any vehicle to claim it did not transmit a signal. Therefore, the need for non-repudiation is met by our system.
6) Based on the information in the beacon, our technique is resistant to replay attacks $\{T, M, V, \sigma_m\}$, where $\sigma_m = PID_v \oplus h(T \parallel M \parallel V \parallel Sk)$, None of the other Ts are available to the attacker. For this reason, our scheme is secure against replay attacks.
7) To prevent an impersonation attack, the suggested approach requires the attacker to know the x_i and PID_v before they may legitimately emit a beacon while disguised as a moving vehicle. If the beacon contains the data $\{T, M, V, \sigma_m\}$ where $V = h(x_i \parallel T)$ and $\sigma_m = PID_v \oplus h(T \parallel M \parallel V \parallel Sk)$ then the attacker cannot compute V and σ_m without knowing x_i and PID_v. Thus, our scheme can withstand forgery attempts.
8) Each beacon is protected from a modification attack since σ_m is hardcoded into it. This means that our system is resistant to attackers that attempt to make changes to it.
9) The proposed scheme offers sufficient safety against a fake information attack. It is recommended that the vehicle uses the valid pseudonym PID_v and its unusual random integer x_i to calculate the beacon's signature. If a legitimate beacon is sent out with false data, our technique can identify the sender and, during the revocation phase, cancel the registration of the sender's car. Because of this, our method is secure against fake information attacks.

Table (3) : Comparisons Of Security And Privacy Requirements

Properties	[18]	[22]	[25]	[28]	LV2PA
Authentication and privacy-preserving	No	Yes	Yes	Yes	Yes
Integrity	Yes	Yes	Yes	Yes	Yes
Unlinkability	Yes	Yes	Yes	Yes	Yes
Traceability	Yes	Yes	Yes	Yes	Yes
Revocation	No	No	Yes	No	Yes
Non-repudiation	Yes	Yes	Yes	No	Yes
Location tracking attack	Yes	Yes	Yes	Yes	Yes
Sybil attack	No	No	Yes	No	Yes
replay attack	Yes	Yes	Yes	Yes	Yes
bogus information attack	No	Yes	Yes	No	Yes
modification attack	Yes	Yes	Yes	Yes	Yes
MITM attack	Yes	Yes	Yes	No	Yes
impersonation attack	Yes	Yes	Yes	Yes	Yes
Forward secrecy and backward secrecy	---	----	----	Yes	Yes

Low overhead	No	N0	No	No	Yes

10) Resistance against man-in-the-middle attacks: the proposed approach relies on vehicle-to-infrastructure (V2I) mutual authentication, with the onus of beacon validation falling on the RSU. To pull off a Man-in-the-Middle assault, an adversary must first trick the sender and verifier into believing they are communicating with the real thing. However, the previous formal security analysis proves that an attacker cannot conduct an MITM attack. For this reason, our scheme is immune to man-in-the-middle assaults.
11) Resistance to a Sybil attack: This attack requires the adversary to forge fake identities of several vehicles. Our scheme requires each vehicle firstly to create a V2I mutual authentication before broadcasting valid information. Moreover, the RSU notifies the vehicle with valid and invalid beacons by using the Bloom filter with each notification message; thus, an adversary cannot launch this attack. Our scheme is therefore resistant to Sybil attacks.
12) Location tracking attack: According to our scheme can offer an un-linkability requirement, an adversary cannot launch this attack. Our scheme is therefore resistant to location-tracking attacks.
13) The proposed scheme ensures forward and backward secrecy by having the RSU update the shared group key whenever a vehicle leaves or joins the group. As a result, once a vehicle quits the group, it can no longer access any data collected after its departure, and similarly, a vehicle that joins the group cannot access any data collected before it did so. Our approach, therefore, satisfies the conditions for forward and backward secrecy.
14) The processing time in the RSU and OBU can be considerably reduced and network latency can be decreased because the new technique has a low overhead and a short beacon size (44 bytes per beacon, on average).

6. Performance Evaluation

In this part, we evaluate the LV2PA in comparison to other schemes in terms of computational and communication overhead.

6.1 Computation cost

We describe the computation cost between the LV2PA and Xie et al., [18], Kamil and Ogundoyin [22], Cui et al., [25], and Cui et al., [28] schemes. The cryptography operations in the schemes of Xie et al., [18], Kamil and Ogundoyin [22] and Cui et al., [25] use ECC, while the cryptography operation in the scheme of Cui et al., [28] is used the AES algorithm. The cryptography hash function is used in the proposed LV2PA scheme. The security level is 80- bit in ECC, and the additive group G is computed according to the equation $y^2 = x^2 + ax + b \bmod p$, where p is an integer. The execution times are adapted in this paper for cryptographic operations [25], as follows. And Table IV presents the running time of the cryptographic operations.

Table (4) : The Execution Time For Cryptography-Related Operations

Operations	Execution time (ms)	Descriptions
T_{ecc}^{sm}	0.3476	The elliptic curve (EC) point multiplication
T_{ecc}^{sm-s}	0.0246	The small-scale scalar point multiplication-based EC.
T_{ecc}^{pa}	0.002	The EC point addition
T_h	0.0012	The cryptography hash function
T_{aes}^{enc}	0.183	Encryption operation on AES
T_{aes}^{dec}	0.157	Decryption operation on AES

For simplicity, let AMG, SMV, and BMV denote message generation, single message verification, and verification of batch messages, respectively.

In the scheme of Xie et al., [18], the computation costs for AMG, SMV, and BMV are ($2T_{ecc}^{sm} + 2T_h$ = 0.6976 ms), ($2T_{ecc}^{sm} + T_{ecc}^{pa} + T_h$= 0.6984 ms) and ($3T_{ecc}^{sm} + nT_{ecc}^{sm-s} + nT_{ecc}^{pa} + nT_h$ = 1.0428 + 0.0278n ms), respectively.

In the scheme of Kamil and Ogundoyin [22], the computation costs for AMG, SMV, and BMV are ($3T_{ecc}^{sm} + 2T_{ecc}^{pa} + 3\ T_h$ = 1.0504 ms), ($2T_{ecc}^{sm} + T_{ecc}^{pa} + T_h$ = 0.6984ms), and ($2T_{ecc}^{sm}$ + (3n) $T_{ecc}^{sm-s} + nT_{ecc}^{pa} + nT_h$ = 0.6952+0.077nms) respectively.

In the scheme of Cui et al., [25], the computation costs for AMG, SMV, and BMV are ($2T_{ecc}^{sm} + 2T_h$= 0.6976 ms), ($2T_{ecc}^{sm} + T_{ecc}^{pa} + T_h$= 0.6984 ms) and ($2T_{ecc}^{sm} + nT_{ecc}^{sm-s} + nT_{ecc}^{pa} + nT_h$ = 0.06952 + 0.0278n ms), respectively.

In the scheme of Cui et al., [28], the computation costs for AMG, SMV, and BMV are ($T_{aes}^{enc} + 2T_h$ = 0.1854 ms), ($T_{aes}^{dec} + 4T_h$ = 0.1618 ms) and ($nT_{aes}^{dec} + (4n)T_h$ = 0.1618n ms), respectively.

Nevertheless, in the LV2PA scheme, the computation costs for AMG, SMV, and BMV are ($2T_h$= 0.0024 ms), ($2T_h$ = 0.0024 ms) and ($(2n)T_h$ = 0.0024n ms) respectively. A comparison of these results is presented in Table 5.

Table (5) : Comparison Of Computation Cost

Schemes	ABG (ms)	SBV (ms)	NBV (ms)
Xie et al., [18]	0.6976	0.6984	$1.0428 + 0.0278n$
Kamil et al., [22]	1.0504	0.6984	$0.6952 + 0.077n$
Cui et al., [25]	0.6976	0.6984	$0.6952 + 0.0278n$
Cui et al., [28]	0.1854	0.1618	$0.1618n$
LV2PA	0.0024	0.0024	$0.0024n$

We can conclude as presented in Table V, the improvements of the proposed LV2PA scheme are 99.6%, 99.8%, 99.6%, and 98.7% in the AMG cost compared with these schemes of Xie et al., [18], Kamil and Ogundoyin [22], Cui et al., [25] and Cui et al., [28], respectively. Moreover, the improvements of the proposed LV2PA scheme are 99.6%, 99.6%, 99.6%, and 98.5% in the SMV cost compared with these schemes of Xie et al., [18], Kamil and Ogundoyin [22], Cui et al.,[25] and Cui et al., [28], respectively. The improvements of the proposed LV2PA scheme are 95.1%, 99.9%, 94.2%, and 98.5% in the BMV cost for 60 messages compared with Xie et al., [18], Kamil and Ogundoyin [22], Cui et al., [25] and Cui et al., [28], respectively. The improvements offered by the proposed LV2PA scheme over the other schemes are presented in Table 6.

Table (6): The Improvements Of The Lv2pa Scheme Over Others In Terms Of The Computation

Schemes	ABG	SBV	NBV (50 beacons)
Xie et al [18]	99.6%	99.6%	95.1%
Kamil et al [22]	99.8%	99.6%	99.9%
Cui et al [25]	99.6%	99.6%	94.2%
Cui et al [28]	98.7%	98.5%	98.5%

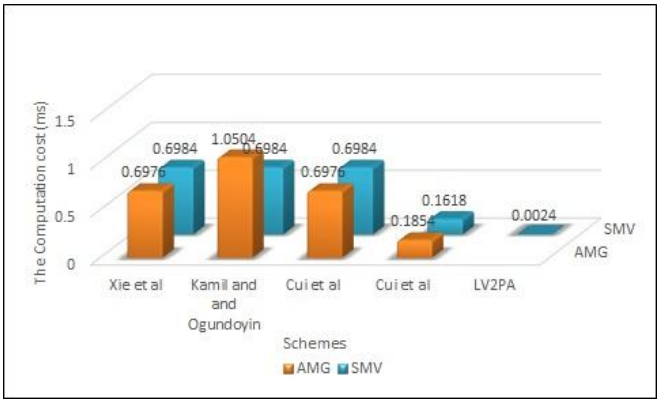


Figure. (5). The computation costs of AMG and SMV

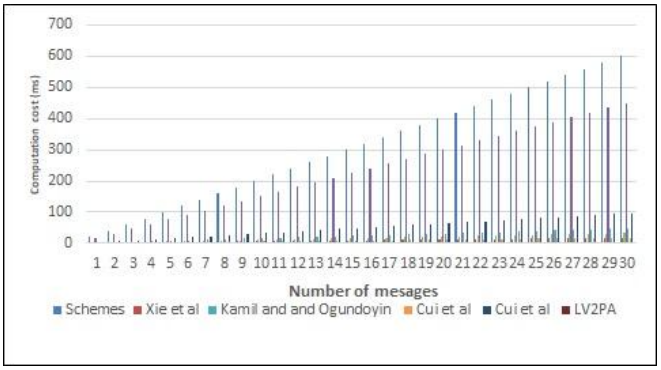


Figure. (6). The computation costs of BMV for a different

Figure 5 shows the difference in AMG and SMV computation costs between the proposed LV2PA method and other existing schemes. Figure 6 displays the BMV computation costs for various message counts. The suggested LV2PA system is demonstrated to be more efficient than the schemes of Xie et al., [18], Kamil and Ogundoyin [22], Cui et al. [25], and Cui et al. [28] in terms of computing costs for AMG, SMV, and BMV.

6.2 Communication cost

The communication costs between the proposed and related schemes [18], [22], [25], and [28] are described. Each p and G element takes up 40 bytes of storage space. Furthermore, we assume that the size of the output of the cryptography hash function and the element in Z q* is 20 bytes, and that the size of the timestamp is 4 bytes. In Table VII, we see a comparison of communication prices, where factors like message size have been removed.

According to Xie et al. [18], the cost of communicating a safety-related message of the form $\{M, U, T, PID, \sigma\}$ where $\{\sigma \in Z_q^*\}$, $\{PID, U \in G\}$, and T is a timestamp, is 40+40+4+20=104 bytes. The communication cost for all the other existing schemes is calculated using the same technique. In contrast, the proposed LV2PA system requires the vehicle to broadcast the safety-related message $\{T, M, V, \sigma_m\}$, where $\{\sigma_m, \mathrm{V} \in Z_q^*\}$ and T is a timestamp, therefore the total communication cost is 4+20+20=44 bytes. Therefore, the suggested LV2PA method has lower communication costs than the schemes of Xie et al. [18], Kamil and Ogundoyin [22], Cui et al. [25], and Cui et al. [28].

Table (7) : The Comparison Of Communication Costs

Schemes	The size of the beacon (byte)
Xie et al [18]	104
Kamil et al [22]	144
Cui et al [25]	84
Cui et al [28]	152

LV2PA	44

6.3 Discussion

This performance comparison clearly shows that the LV2PA scheme provides significant improvements in both computational and communication costs compared to existing schemes such as Cui et al. [28] and Kamil et al. [22]. These improvements stem from the use of lightweight cryptographic hash functions instead of heavier operations like ECC or AES, resulting in much faster message generation and verification times—critical in high-density vehicular environments. Additionally, LV2PA reduces the size of safety messages, decreasing channel congestion and improving communication reliability. These advantages make LV2PA highly efficient and well-suited for real-world vehicular network scenarios requiring timely and secure data exchange.

7. Conclusion

This paper developed the LV2PA scheme, which is a lightweight verification with privacy-preserving authentication, which employs RSU-based groups and depends on the BF and Chinese remainder theorem techniques with a cryptography hash function. In the proposed LV2PA scheme, concerns such as inadequate network latency as well as security and privacy issues are efficiently handled. The proposed LV2PA scheme utilizes a handover phase, which allows it to solve the TA bottleneck issue that arises during mutual authentication between the OBU and the RSU. The formal and informal analyses of the security of the proposed LV2PA scheme demonstrate its authenticity and the fact that it satisfies security and privacy needs. Moreover, the proposed LV2PA system not only maintains the backward secrecy and forward secrecy but withstands attacks such as location tracking, Sybil, replay, false information, modification MITM, and impersonation attacks. When compared to other existing schemes, the LV2PA's computation and communication expenses have a minimal overhead.

References

[1] 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, vol. 21, no. 2, pp. 2422–2433, 2020.

[2] H. Lin, Q. Zhang, and X. Chen, “Blockchain-based conditional privacy-preserving authentication with PUF for VANETs,” Journal of Network and Computer Applications, vol. 210, Feb. 2025.

[3] M. I. Ghafoor, A. B. Naeem, B. Senapati, M. S. Islam Sudman, et al., “Privacy-Preserving and Lightweight V2I and V2V Authentication Protocol Using Blockchain Technology,” Intelligent Automation & Soft Computing, vol. 39, no. 5, pp. 1–10, 2024.

[4] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, “VANET Security Surveys,” Computer Communications, vol. 44, pp. 1–13, 2014.

[5] S. S. Manvi and S. Tangade, “A survey on authentication schemes in vanets for secured communication,” Vehicular Communications, vol. 9, pp. 19–30, 2017.

[6] M. Raya and J.-P. Hubaux, “Securing Vehicular Ad hoc Networks,” Journal of Computer Security, vol. 15, no. 1, pp. 39–68, 2007.

[7] U. Rajput, F. Abbas, H. Eun, R. Hussain, and H. Oh, “A two level privacy preserving pseudonymous authentication protocol for vanet,” in 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, 2015, pp. 643–650.

[8] X. Lin, X. Sun, P.-H. Ho, and X. Shen, “GSIS: A secure and privacy preserving protocol for vehicular communications,” IEEE Transactions on vehicular technology, vol. 56, no. 6, pp. 3442–3456, 2007.

[9] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227–1239, 2010.

[10] C. Zhang, R. Lu, X. Lin, P. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in IEEE INFOCOM 2008-The 27th Conference on Computer Communications. IEEE, 2008, pp. 246–250.

[11] C. Zhang, P.-H. Ho, and J. Tapolcai, "On batch verification with group testing for vehicular communications," Wireless Networks, vol. 17, no. 8,p. 1851, 2011.

[12] D. Huang, S. Misra, M. Verma, and G. Xue, "Pacp: An efficient pseudonymous authentication-based conditional privacy protocol for vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 12, no. 3, pp. 736–746, 2011.

[13] S.-J. Horng, S.-F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, and M. K. Khan, "b-SPECS+: Batch Verification For Secure Pseudonymous Authentication in VANET," IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1860–1875, 2013.

[14] H. Zhong, J. Wen, J. Cui, and S. Zhang, "Efficient conditional privacy-preserving and authentication scheme for secure service provision in vanet," Tsinghua Science and Technology, vol. 21, no. 6, pp. 620–629,2016.

[15] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 5, pp. 1319–1328, 2015.

[16] L. Wu, J. Fan, Y. Xie, J. Wang, and Q. Liu, "Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks," International Journal of Distributed Sensor Networks, vol. 13,no. 3, p. 1550147717700899, 2017.

[17] M. A. Al-shareeda, M. Anbar, S. Manickam, I. H. Hasbullah, N. Abdullah, M. M. Hamdi, and A. S. Al-Hiti, "Ne-cppa: A new and efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks (vanets)," Appl. Math, vol. 14, no. 6, pp. 1–10, 2020.

[18] Y. Xie, L. Wu, J. Shen, and A. Alelaiwi, "Eias-cp: new efficient identity-based authentication scheme with conditional privacy-preserving for vanets," Telecommunication Systems, vol. 65, no. 2, pp. 229–240, 2017.

[19] M. A. Alazzawi, H. Lu, A. A. Yassin and K. Chen, "Efficient Conditional Anonymity With Message Integrity and Authentication in a Vehicular Ad-Hoc Network," in IEEE Access, vol. 7, pp. 71424-71435, 2019, doi: 10.1109/ACCESS.2019.2919973.

[20] M. A. Al-Shareeda, M. Anbar, S. Manickam, and A. A. Yassin, "Vppcs: Vanet-based privacy-preserving communication scheme," IEEE Access, vol. 8, pp. 150 914–150 928, 2020.

[21] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in International conference on the theory and application of cryptology and information security. Springer, 2003, pp. 452–473.

[22] Y. Ming and X. Shen, "PCPA: A Practical Certificateless Conditional Privacy Preserving Authentication Scheme for Vehicular Ad hoc Networks,"Sensors, vol. 18, no. 5, p. 1573, 2018.

[23] A. Kamil and S. O. Ogundoyin, "An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks," Journal of information security and applications, vol. 44, pp. 184–200, 2019.

[24] Y. Ming and H. Cheng, "Efficient Certificateless Conditional Privacy-Preserving Authentication Scheme in VANETs," Mobile Information Systems, vol. 2019, 2019.

[25] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "Spacf: A secure privacy-preserving authentication scheme for vanet with cuckoo filter," IEEE Transactions on Vehicular Technology, vol. 66, no. 11, pp. 10 283–10 295, 2017.

[26] 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, 2017.

[27] J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, "An efficient message authentication scheme based on edge computing for vehicular ad hoc networks," IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 5, pp. 1621–1632, 2018.

[28] J. Cui, X. Tao, J. Zhang, Y. Xu, and H. Zhong, "Hcpa-gka: A hash function-based conditional privacy-preserving authentication and group key agreement scheme for vanets," Vehicular communications, vol. 14, pp. 15–25, 2018.

[29] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "Pa-crt: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," IEEE Transactions on Dependable and Secure Computing, 2019.

[30] C. Zhou, G. Zhu, B. Zhao, and W. Wei, "Study of one-way hash function to digital signature technology," in 2006 International Conference on Computational Intelligence and Security, vol. 2. IEEE, 2006, pp. 1503–1506.

[31] J. Zhou and Y.-h. Ou, "Key tree and Chinese remainder theorem based group key distribution scheme," in International Conference on Algorithms and Architectures for Parallel Processing. Springer, 2009, pp. 254–265.

[32] T. W. Chim, S.-M. Yiu, L. Hui, and V. Li, "SPECS: Secure and Privacy Enhancing Communications Schemes for VANETs," Ad Hoc Networks, vol. 9, no. 2, pp. 189–203, 2011.

[33] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, vol. 426, no. 1871, pp. 233–271, 1989.

[34] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K.-K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," Computer Networks, vol. 129, pp. 429–443, 2017.

[35] M. A. Al-Shareeda, M. Anbar, M. A. Alazzawi, S. Manickam, and A. S. Al-Hiti, "Lswbvm: A lightweight security without using batch verification method scheme for a vehicle ad hoc network," IEEE Access, vol. 8, pp. 170 507–170 518, 2020.