Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.053854

ARTICLE

Check for updates

Message Verification Protocol Based on Bilinear Pairings and Elliptic Curves for Enhanced Security in Vehicular Ad Hoc Networks

Vincent Omollo Nyangaresi[1,2], Arkan A. Ghaib[3], Hend Muslim Jasim[4], Zaid Ameen Abduljabbar[4,5,6,*], Junchao Ma[5,*], Mustafa A. Al Sibahee[7,8], Abdulla J. Y. Aldarwish[4], Ali Hasan Ali[9,10] and Husam A. Neamah[11]

[1]Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Bondo, 40601, Kenya

[2]Department of Applied Electronics, Saveetha School of Engineering, SIMATS, Chennai, Tamilnadu, 602105, India

[3]Information Technology Department, Management Technical College, Southern Technical University, Basrah, 61004, Iraq

[4]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, 61004, Iraq

[5]College of Big Data and Internet, Shenzhen Technology University, Shenzhen, 518118, China

[6]Huazhong University of Science and Technology, Shenzhen Institute, Shenzhen, 518000, China

[7]National Engineering Laboratory for Big Data System Computing Technology, Shenzhen University, Shenzhen, 518060, China

[8]Computer Technology Engineering Department, Iraq University College, Basrah, 61004, Iraq

[9]Department of Mathematics, College of Education for Pure Sciences, University of Basrah, Basrah, 61004, Iraq

[10]Institute of Mathematics, University of Debrecen, Debrecen, H-4002, Hungary

[11]Department of Electrical Engineering and Mechatronics, Faculty of Engineering, University of Debrecen, Debrecen, 4028, Hungary

*Corresponding Authors: Zaid Ameen Abduljabbar. Email: zaid.ameen@uobasrah.edu.iq; Junchao Ma. Email: majunchao@sztu.edu.cn

Received: 11 May 2024 Accepted: 01 September 2024 Published: 15 October 2024

ABSTRACT

Vehicular ad hoc networks (VANETs) provide intelligent navigation and efficient route management, resulting in time savings and cost reductions in the transportation sector. However, the exchange of beacons and messages over public channels among vehicles and roadside units renders these networks vulnerable to numerous attacks and privacy violations. To address these challenges, several privacy and security preservation protocols based on blockchain and public key cryptography have been proposed recently. However, most of these schemes are limited by a long execution time and massive communication costs, which make them inefficient for on-board units (OBUs). Additionally, some of them are still susceptible to many attacks. As such, this study presents a novel protocol based on the fusion of elliptic curve cryptography (ECC) and bilinear pairing (BP) operations. The formal security analysis is accomplished using the Burrows–Abadi–Needham (BAN) logic, demonstrating that our scheme is verifiably secure. The proposed scheme's informal security assessment also shows that it provides salient security features, such as non-repudiation, anonymity, and unlinkability. Moreover, the scheme is shown to be resilient against attacks, such as packet replays, forgeries, message falsifications, and impersonations. From the performance perspective, this protocol yields a 37.88% reduction in communication overheads and a 44.44% improvement in the supported security features. Therefore, the proposed scheme can be deployed in VANETs to provide robust security at low overheads.

KEYWORDS
Attacks; bilinear; elliptic curve cryptography (ECC); privacy; security; vehicular ad hoc network (VANET)

1 Introduction

The continuously increasing volume of vehicles on roads has led to difficulties in urban traffic management. Additionally, frequent accidents and heavy traffic jams pose numerous challenges to traffic management systems. This situation has led to the development of vehicular ad hoc networks (VANETs) to offer efficient and intelligent transport management [1–3]. VANETs are a special case of self-organizing mobile networks, in which vehicles share information through vehicle-to-vehicle (V2V) or vehicle-to-roadside unit (V2R) transmission modes. As explained in Reference [4], rapid advancements in microelectronic and wireless technologies have contributed to the speedy developments in VANETs. A typical VANET environment comprises vehicles, trusted authorities (TAs), and roadside units (RSUs). According to Reference [5], the on-board unit (OBU) installed in each vehicle detects safety messages from its environment (e.g., customers, pedestrians, other vehicles, Internet, traffic lights, cloud, parking areas, and sensors). TAs register all RSUs and vehicles within the VANET, whilst RSUs act as relays during data exchanges amongst vehicles [6]. For message exchanges, vehicle-to-infrastructure (V2I) and V2V are two major modes deployed in VANETs [7].

OBUs use dedicated short-range communication (DSRC) to transmit safety messages to surrounding vehicles or infrastructure at a distance of up to 300 m every 100–300 milliseconds. The broadcast messages may include vehicle location, speed, traffic status, and route. These messages serve to boost safety and reduce accidents on roads. They also help VANETs in offering efficient, secure traffic and route management on roads [8]. Accidents can also be significantly reduced through emergency and rule violation warnings [9]. Additionally, infotainment applications, e.g., intelligent navigation, file sharing, parking, multimedia services, and toll collection, can boost comfort. Ultimately, this configuration results in time savings, cost reductions, and efficiency enhancements on roads. As explained in Reference [10], the resulting intelligent transportation system (ITS) consisting of the internet of vehicles (IoV) facilitates traffic route management. This system can also enhance driving safety and minimize traffic congestion [11].

Despite the many benefits of VANET deployments, the open nature of the wireless channels deployed during communication exposes these networks to numerous security and privacy violations [12]. Some serious issues in VANETs include data leakages, eavesdropping, and session hijacking attacks. Additionally, replays, man-in-the-middle (MitM) attacks, impersonations, and message fabrications can be present in these networks [7]. Attackers can also implant malicious vehicles in these networks to execute malevolent activities, such as the misuse of the offered route management [13]. Although beacons and messages are signed, the lack of encryption before broadcast has been noted to be a serious issue in VANETs [8,14]. Therefore, attackers can intercept these messages and, hence, violate privacy [15–17]. Additionally, adversaries can exploit these messages for malicious activities. Another serious challenge in VANETs is heterogeneity occasioned by the deployment of hardware from different manufacturers. Such heterogeneity results in different protocols for message transmission and authentication, thereby potentially causing inconsistencies in security and privacy implementations [8].

Numerous schemes have been developed recently to address the security and privacy issues above. The majority of these solutions are based on public key infrastructure (PKI) [18], blockchain, certificates, and physically unclonable functions (PUFs). Unfortunately, most of these schemes still face serious privacy, performance, and security setbacks. Additionally, the majority of the current traffic route management schemes incur high computation and communication overheads [10]. Limited bandwidths, heavy data volumes, scalability, short communication periods, and strict real-time operations call for efficient communication protocols. High mobility in VANETs likewise implies a short authentication and communication time amongst different entities. Therefore, the efficiency of the current authentication protocols must be improved. The major contributions of this study are as follows:

- We develop an authentication method based on elliptic curve cryptography (ECC) and bilinear pairings (BPs) to offer efficient and secure source and message verification.
- Stochastic one-time secret keys are incorporated in the proposed scheme during mutual validations to boost vehicle and RSU privacy. Additionally, these dynamic stochastic one-time secret keys help thwart adversarial linkability and traceability.
- Conditional privacy is preserved in the proposed protocol so that malicious network entities can be identified and revoked by a fully trusted network entity. This aspect is crucial in preventing malicious parties from overwhelming VANETs with fake messages that can cause denial of service (DoS), traffic jams, and accidents.
- A formal security analysis is conducted to demonstrate that the proposed scheme is provably secure. Additionally, an informal security analysis demonstrates that our scheme can withstand numerous attacks, such as message falsifications, forgeries, packet replays, impersonations, and MitM attacks. The protocol can also offer mutual authentication, perfect key secrecy, anonymity, unlinkability, non-repudiation, and source and message integrity.
- We perform extensive comparative performance evaluations, demonstrating that the proposed scheme incurs relatively low computation costs and the least communication overheads. Therefore, it is concluded that the scheme offers robust security at low overheads.

1.1 This Sub-Section Aims to Present Some Mathematical Formulations upon Which the Proposed Protocol Is Based. The Two Building Blocks for the Proposed Protocol Are BP and Elliptic Curve (EC) Operations.

1.1.1 BP

Let λ_1, λ_2, and λ_3 represent a cyclic group consisting of prime numbers, the order of which is p. Additionally, let g_i be the generator of cyclic group λ_i. We also denote the one-to-one mapping from λ_2 to λ_1 as $I(g_2)$. The computable bilinear map is represented as $I(g_2) = g_2$. B_M: $\lambda_1 \times \lambda_2 \rightarrow \lambda_3$. In this scenario, BP has the following properties:

Computability: For any cyclic group generators $g_f \in \lambda_1$ and $g_2 \in \lambda_2$, there exists an efficient algorithm that can derive the bilinear map B_M as B_M: $\lambda_1 \times \lambda_2 \rightarrow \lambda_3$.

Bilinearity: For all cyclic group generators $g_i \in \lambda_i$ and $m,\ n \in z_p^*$, bilinearity is denoted by $B_M\left(g_f^m\right),\ g_2^n = B_M(g_f,\ g_2)^{mn}$. Particularly, $z_p^* = \{j|1 \leq j \leq p-1|\}$.

Non-degeneracy: If $I\lambda_3$ denotes the identity in cyclic group λ_3, then bilinear map $B_M(g_f,\ g_2) \neq I\lambda_3$.

1.1.2 ECC

Let p and q be large prime numbers, whilst F_p is a finite field, the order of which is p. Additionally, let E represent an EC denoted by $y^2 = x^3 + ax + b \bmod p$, where $a,\ b \in F_p$ are constants. Also, let G be an additive group of order q and P the generator of G. Specifically, G comprises the point at infinity $\ddot{I}$ and all points on E. The following concepts are utilized in the proposed protocol:

Point addition: Suppose that P and Q are two points of group G. We denote an intersection of the straight line connecting P and Q and the EC E as R. Thereafter, $R = P + Q$, provided that the two points are different. On condition that $P = Q$, intersection R is denoted as $R = P + Q$. However, when $P = -Q$, $P + Q = 0$.
Point multiplication: Suppose that $m \in Z_q^*$. Accordingly, the EC scalar multiplication is denoted as $m.P = P + P + \ldots P$ (for a total of m times).

The strength of the resulting ECC-based security protocol is based on the difficulties of solving the elliptic curve discrete logarithm problem (ECDLP) and the elliptic curve computational Diffie-Hellman problem (ECCDHP). The two problems can be mathematically formulated as follows:

ECDLP: Suppose that points P and Q are random points on E, such that $P,\ Q \in G$ and $Q = x.P$. Taking P_T as the probabilistic polynomial time, computing integer x from Q in P_T should be cumbersome.
ECCDHP: Let x and y be some two unknown integers and Q and R be two random points on E. Additionally, let $\{x.P,\ y.P,\ P\}$ be some values such that $x,\ y \in Z_q^*$. Hence, there exists no probabilistic polynomial time algorithm that can derive the value of $x.y.P$.

1.2 Security and Privacy Requirements

Without strong privacy and security protections, VANET message exchanges are exposed to numerous malicious entities and activities. As such, the proposed protocol must fulfill the following requirements to uphold strong privacy and security in this environment:

Anonymity: The actual identities of vehicles and RSUs should be hidden from adversaries. This strategy ensures that eavesdroppers cannot determine these unique identities for malicious activities.
Conditional privacy: TAs could determine the real identity and trace and eliminate any malicious RSU from the network. This situation prevents these malicious entities from transmitting high volumes of falsified messages that can lead to accidents or DoS.
Mutual authentication: All parties in the VANET must validate one another before exchanging any messages.
Source and message integrity: It should be impossible for attackers to change the messages exchanged in the VANET environment.
Backward key secrecy: Attackers should be unable to use the present session keys to derive any keys utilized in previous data exchange sessions.
Forward key secrecy: Adversaries with access to the present session keys should be unable to use these keys to compute the keys to be deployed in subsequent communication processes.
Unlinkability: Eavesdroppers in the network should be unable to associate any transmitted messages to a particular vehicle or RSU.
Nonrepudiation: Communicating entities should not be in a position to deny having participated in message exchange.

1.3 Threat Model

This section models adversarial capabilities that could compromise the proposed protocol. In our protocol, adversary $\mathring{A}$ is thought to have the capabilities advocated in the Canetti-Krawczyk (C-K) model. In this model, $\mathring{A}$ is capable of the following attacks:

- Intercepting, eavesdropping, impersonating, modifying, and deleting the exchanged packets;
- Physically capturing OBUs and retrieving all security tokens stored in their memories;
- Capturing the session states and keys negotiated amongst the vehicles and RSUs.

The proposed protocol is required to avert all these adversarial attack vectors and guarantee strong privacy and security protection.

1.4 Motivation

Message transmission in VANETs is executed over open public channels prone to attacks. In this environment, attackers can intercept, delete, replay, and modify messages. Adversaries could also impersonate legitimate and authorized entities and broadcast fake information. Additionally, the inability of the VANET entities to establish message and source authenticity may result in accidents and traffic jams. Therefore, all VANET entities must validate message source authenticity, determine message integrity, and preserve confidentiality. Equally important is to maintain the anonymity and privacy of vehicles and RSUs, without which these entities are exposed to numerous attacks. For example, attackers may obtain the vehicle's real identity, travel routes, and current location, which enables the adversaries to perform tracking [19–21] of network entities. Performance is another important metric that must be enhanced in VANETs so that multiple messages are processed immediately. This particular case involves vehicles moving at high speeds, in which receivers should be capable of processing multiple messages within 100–300 ms [22]. Given that OBUs installed in vehicles are not as endowed in computation and storage as TAs and RSUs, they can be easily overwhelmed with high computational overheads when numerous high-mobility vehicles broadcast multiple messages. This is particularly the case in dense traffic regions. Hence, there is a need to reduce this complexity.

2 Related Works

Numerous security and privacy preservation solutions have been developed to secure the communication process in VANETs. For example, the identity-based scheme (IBS) is presented in Reference [23]. However, key escrow problems continue to be a serious issue in IBS-based approaches [24]. A signature-based scheme utilizing public key infrastructure and identity is developed in Reference [25], whilst a conditional privacy preservation scheme is introduced in Reference [26]. Unfortunately, message verification and identity detection tend to have long execution durations, which degrades the performance of the two approaches above [27]. In addition, the scheme in Reference [26] incurs huge storage overheads for large pools of identities and secret keys. Privacy-preserving authentication protocols using group signatures are developed in Reference [28,29]. However, identifying malicious vehicles within a network may be cumbersome [30]. Reference [31] presents a signature-based batch verification scheme in VANETs, though failing to offer key secrecy, conditional privacy, and unlinkability. Meanwhile, the algorithm in Reference [32] is only evaluated against collusion attacks, and the protocol in Reference [33] does not consider non-repudiation and unlinkability. A lightweight authentication solution is introduced in Reference [34] based on the difficulty of ECCDHP. During registration, each vehicle is issued a smart card, which is used in conjunction with passwords for login. Similarly, an authentication approach utilizing passwords is presented in Reference [35].

Unfortunately, the technique in Reference [34] cannot withstand smart card loss and password-guessing attacks [7], and the approach in Reference [35] is not robust against attacks such as password guessing, sensor capturing, traceability, and impersonations [36].

To address the issues in Reference [34], message authenticated codes (MACs) are deployed in Reference [37] instead of passwords. Although MAC offers protection against attacks such as impersonations, privileged insiders, DoS, and packet replays, it has not been evaluated against MiTM attacks, forgeries, and message falsifications. The issues in Reference [35] are handled by the two-factor authentication technique in Reference [36], which deploys biometric templates instead of passwords. Although this scheme is robust against smart cards, stolen sink nodes, and replay attacks, it incurs high storage complexity in the sink node's memory. Additionally, the revocation of malicious entities is not considered and has high communication and computation overheads [7]. A privacy-preserving scheme using a law executor is introduced in Reference [38], and a two-factor security protocol is meanwhile developed in Reference [39], both incurring low computation costs. However, session keys derived in References [38,39] are not secured against the C-K adversary attack [7]. For secure VANETs, techniques deploying PUFs are developed in References [40–42]. Although these techniques minimize redundant authentications [7], PUFs have instability issues [43]. Reference [44] introduces a privacy-preserving hybrid signcryption security solution. Other signcryption-based protocols are presented in References [8,33].

However, the use of several time-consuming operations in these schemes reduces their efficiency [44]. For example, the generation, distribution, processing, validation, and revocation of certificates result in long delays. Additionally, PKI-based signcryption protocols render it cumbersome for vehicles to manage large pools of certificates and key pairs. The scheme in Reference [8] also fails to offer key secrecy.

To enable vehicles to execute batch validation of other nearby vehicles, a privacy-preserving scheme is presented in Reference [45]. A similar batch authentication approach is developed in Reference [8]. Meanwhile, a mutual authentication technique for an IoV environment is introduced in Reference [14]. Although these schemes are provably secure and efficient, they fail to provide message confidentiality [44]. A security protocol using BP operations is introduced in Reference [46]. Meanwhile, a pairing-free security solution is presented in Reference [47]. Unfortunately, the technique in Reference [46] involves three pairing operations, which increases its computation complexity. Although the approach in Reference [47] is efficient owing to the deployment of ECC, it fails to offer anonymity and traceability. Besides, it cannot resist message replays [44]. A security technique based on pairing operations is introduced in Reference [7], but it fails to consider message integrity, non-repudiation, and conditional privacy. To curb some of the preceding challenges, schemes based on blockchain technology have been developed and shown to offer anonymity, immutability, and decentralization. For example, a blockchain certificate-based technique is developed in Reference [48].

However, it requires frequent interactions between certificate authorities and vehicles [49], thereby increasing its communication overheads. Similarly, blockchain-based protocols are developed in References [50–53]. However, blockchain technology incurs huge storage overheads [54] and, hence, is not energy-efficient [55,56]. Additionally, the protocol in Reference [53] does not consider message falsifications, non-repudiations, and impersonations. Nevertheless, a combination of pseudonyms and blockchains is deployed in Reference [57] to establish distributed trust in VANETs.

Similarly, a blockchain-based technique was introduced in Reference [58] to facilitate vehicle revocability without the need for TA's assistance. However, the scheme in Reference [50] results in significant communication costs and delays due to the frequent involvement of the certificate authority

(CA) in public key updates. Meanwhile, a fault tolerance technique was introduced in Reference [59], while an anti-jamming technique was developed in Reference [60]. Despite these advancements, it is crucial to conduct extensive formal and informal security analyses in these schemes. Table 1 offers a detailed summary of these related studies.

Table 1: Summary of related works

Author(s)	Scheme	Gap(s)
Bagga et al. [7]	Bilinear pairing-based	Fails to consider message integrity, non-repudiation and conditional privacy
Ali et al. [8]	ECC-based	High computation complexities and Fails to offer key secrecy
Bagga et al. [14]	Batch verification-based	Fails to provide message confidentiality
Li et al. [23]	Identity-based	Key escrow
Wang et al. [25]	Signature based	High computation costs
Al-Shareeda et al. [26]	ECC-based	Huge storage overheads and high computation costs
Wang et al. [28]	Group signatures	Difficult to identify malicious entities
Islam et al. [29]		
Shen et al. [31]	Signature based	Cannot offer key secrecy, conditional privacy and unlinkability
Rabieh et al. [32]	Bilinear pairing-based	Only evaluated against collusion attacks
Luo et al. [33]	Signcryption-based	Does not consider non-repudiation and unlinkability
Ying et al. [34]	ECC-based	Cannot withstand smart card loss and password guessing attacks
Yu et al. [35]	Password-based	Not robust against password guessing, sensor capture, traceability and impersonation attacks
Sadri et al. [36]	Biometric-based	High storage, communication and computation complexity
Chen et al. [37]	MAC-based	Not evaluated against MiTM, forgery and message falsifications
Wu et al. [38]	Law executor-based	Not secure under the Canetti-Krawczyk (CK) model
Vasudev et al. [39]		Not secure under the (CK) model
Alfadhli et al. [40], Aman et al. [41], Alladi et al. [42]	PUF-based	Instability issues
Ali et al. [44]	Hybrid signcryption	High computation complexities
Sutrala et al. [45]	Batch verification-based	Fails to provide message confidentiality
Liu et al. [46]	Bilinear pairing-based	High computation complexities
Cui et al. [47]	Pairing-free-based	Fails to offer anonymity and traceability
		Cannot resist message replays
Zhang et al. [49]	Blockchain-based	High communication overheads

(Continued)

Table 1 **(continued)**

Author(s)	Scheme	Gap(s)
Lin et al. [50], Shawky et al. [51,52], Tan et al. [53], Yang et al. [57], Son et al. [58]	Blockchain-based	Huge storage overheads
Syed et al. [59]	IRS aided	Lacks extensive formal and informal security analyses
Yao et al. [60]	Anti-jamming technique	Lacks extensive formal and informal security analyses

The preceding review shows that most current VANET security solutions are PKI-, identity-, ECC-, blockchain-, certificateless-, or PUF-based. These schemes still face serious privacy, performance, and security setbacks. For example, most identity-based approaches have key escrow and revocation challenges. Conversely, security solutions based on PKI incur huge storage costs. Although certificateless solutions solve the key escrow issues in identity-based protocols, the key revocation challenge is still challenging in these approaches. Owing to frequent mobility in VANETs, authentication and message exchange durations are extremely short. As such, a need arises to enhance the efficiency of authentication and communication procedures. The proposed protocol is robust and efficient, helping address many of these challenges.

3 The Proposed Protocol

Fig. 1 depicts the main entities in the proposed scheme: vehicles, RSUs, and TA. Before data exchange amongst vehicles and RSUs, they must register at the TA and be issued security tokens to deploy during the authentication and data exchange phases.

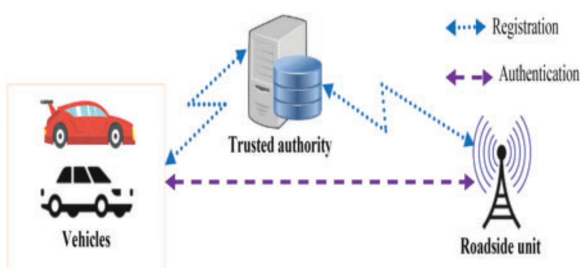

Figure 1: Network model

Registration between the RSU and the TA, as well as vehicles and TA, is executed over secured communication channels. However, authentication and data exchange procedures are carried over wireless communication channels. Table 2 details the notations used in this paper.

The proposed scheme is executed in three major phases: system setup, registration, and mutual authentication.

Table 2: Notations

Symbol	Description
TA	Trusted authority
RSU	Roadside unit
T_{SK}	TA secret key
T_{PK}	TA public key
λ_i	Multiplicative cyclic groups
g_i	Generator of λ_i
RSU_i	RSUi
ID_R	Unique identity of RSU_i
V_j	Vehicle j
R_{SK}	RSU_i secret key
R_{PK}	RSU_i public key
V_{SK}	Vehicle V_j secret key
V_{PK}	Vehicle V_j public key
V_{AT}	Vehicle V_j access token
$\mathbb{R}$	A set of random numbers
R_j	One-time secret key for V_j
$\check{R}_i$	One-time secret key for RSU_i
PU_j	One-time public key for V_j
h (.)	One-way hashing function
B_M	Bilinear map
$\|$	Concatenation operation
$\mathbb{C}_1$, $\mathbb{C}_2$	V_j and RSU_i certificates, respectively
$\mathbb{Z}_1$, $\mathbb{Z}_2$	V_j and RSU_i signatures, respectively
${P_L}^V$, ${P_L}^R$	V_j and RSU_i payloads, respectively
T_i	Timestamp i

3.1 System Setup Phase

First, TA randomly selects p and q, where $p,\ q \in z_p^*$. Second, it chooses collision-resistant one-way hash functions $h:\ \{0,\ 1\}^* \rightarrow Z_p^*$ before selecting $T_{SK} \in z_p^*$ as its private key. Third, TA derives its public key as $T_{PK} = g_1^{T_{SK}+p}$. Lastly, TA forwards the derived parameters $\{\lambda_1, \lambda_2, \lambda_3\ p, B_M, g_1, T_{PK}, h(.)\}$ to all vehicles in the network, as shown in Fig. 2.

3.2 Registration Phase

Each vehicle and RSU must register at the TA before proceeding to other phases, such as authentication and data exchanges. The execution of the following four steps facilitates this process:

Step 1: Roadside unit RSUi sends request *Req-1* to TA through secured communication channels. Upon receiving this request, TA selected ID_R as RSU_i's unique identity. Thereafter, it chooses some secret key R_{SK} for RSU_i, where $R_{SK} \in z_p^*$.

Step 2: *TA* computes public key R_{PK} for RSU_i, where $R_{PK} = g_f^{R_{SK}+q}$. After that, *TA* composes registration response message *Res-1* = $\{R_{SK}\}$, which is forwarded to RSU_i over secure channels before publicly broadcasting R_{PK}.

Step 3: First, vehicle V_j sends registration request Req_2 to *TA*, which chooses random nonce $V_{SK} \in z_p^*$ as its private key. Second, it derives its equivalent public key V_{PK} as $V_{PK} = g_f^{V_{SK}+p}$. Third, registration message $Res_2 = \{V_{SK}\}$ is constructed and sent to V_j over secure channels. Lastly, it publicly broadcasts V_{PK}, as shown in Fig. 2.

Step 4: *TA* generates and offers the vehicle access token $V_{AT} = R_{PK}^p * g_f^p$ to the *RSU*, which it deploys to securely access any information from vehicle V_j. Meanwhile, *TA* maintains parameter set $\{ID_R, R_{PK}^{p*q}\}$ in its access list ACL.

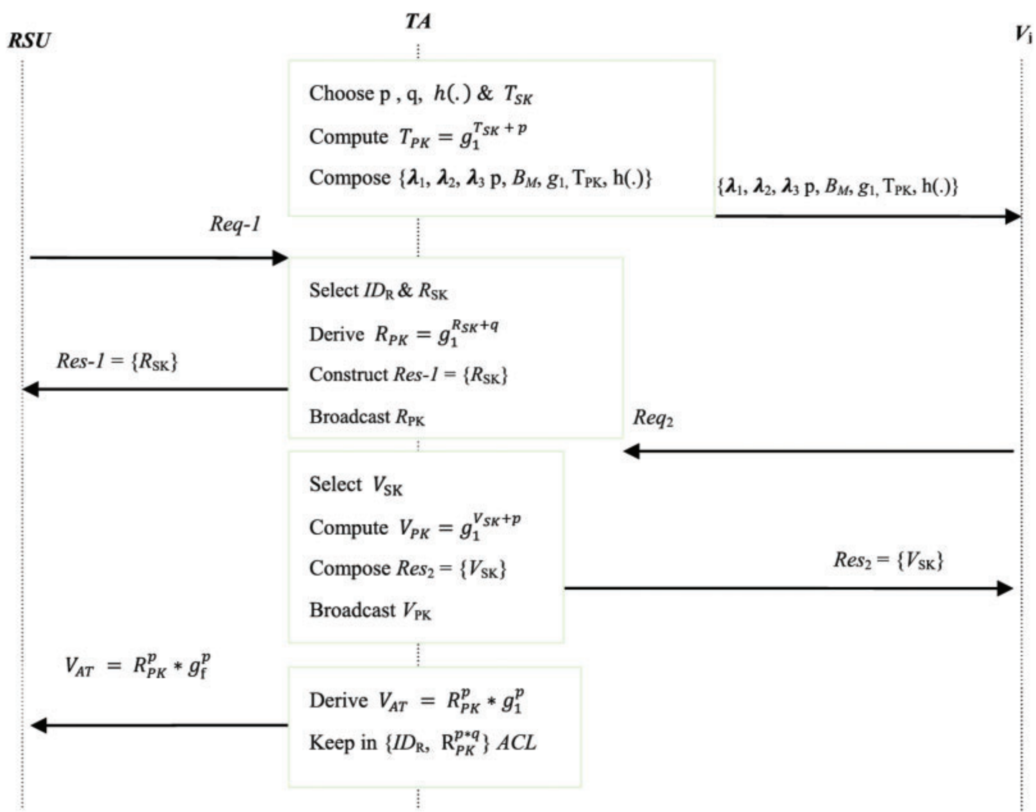

Figure 2: System setup and registration phases

3.3 Authentication Phase

In the authentication phase, the communicating parties derive signatures and certificates used to ensure the integrity of the transmitted payload P_L^V and P_L^R. The first part of this phase is vehicle-to-RSU_i authentication, while the second part is *RSU*- to-vehicle authentication. The goal of $V_j \rightarrow RSU_i$ authentication is to transfer data from vehicles to RSUs securely. As detailed in *Step 1→ Step 6*, this process upholds the privacy of vehicle V_j communication from the rest of the vehicles. However, the second phase of the authentication process aims to transfer sensitive data from RSUs to vehicles securely. The specific details of the authentication procedures are described as follows:

Step 1: Vehicle V_j chooses some random number R_j from the set of random numbers $\mathbb{R}$ to act as its one-time secret key, where $R_1, R_2, \ldots R_{\mathbb{R}} \in Z_p^*$. This procedure is followed by the computation of its corresponding public key as $PU_j = g_f^{R_j+V_{SK}}$, where $j = 1, 2, \ldots \mathbb{R}$.

Step 2: V_j stochastically chooses a random nonce $A_1 \in Z_p^*$ and derives $A_2 = g_f^{V_{SK}}$ and $A_3 = g_f^{V_{SK}+A_1}$. Thereafter, it calculates parameters $A_4 = h\,(PU_j \| A_2 \| A_3 \| T_{PK})$, $A_2^* = g_f^{R_j - A_1}$ and $A_3^* = (g_f^{R_j})^{-1}$. Lastly, it computes certificate $\mathbb{C}_1 = \{PU_j \| A_2^* \| A_3^* \| A_4\}$.

Step 3: Vehicle V_j derives signature $\mathbb{Z}_1 = g_2^{(R_j+V_{SK}+h(P_L^V)^{-1}}$ and composes authentication message *Msg-1* $= (P_L{}^V \| \mathbb{Z}_1 \| PU_j \| \mathbb{C}_1 \| T_s)$, which it forwards to RSU_i, as illustrated in Fig. 3.

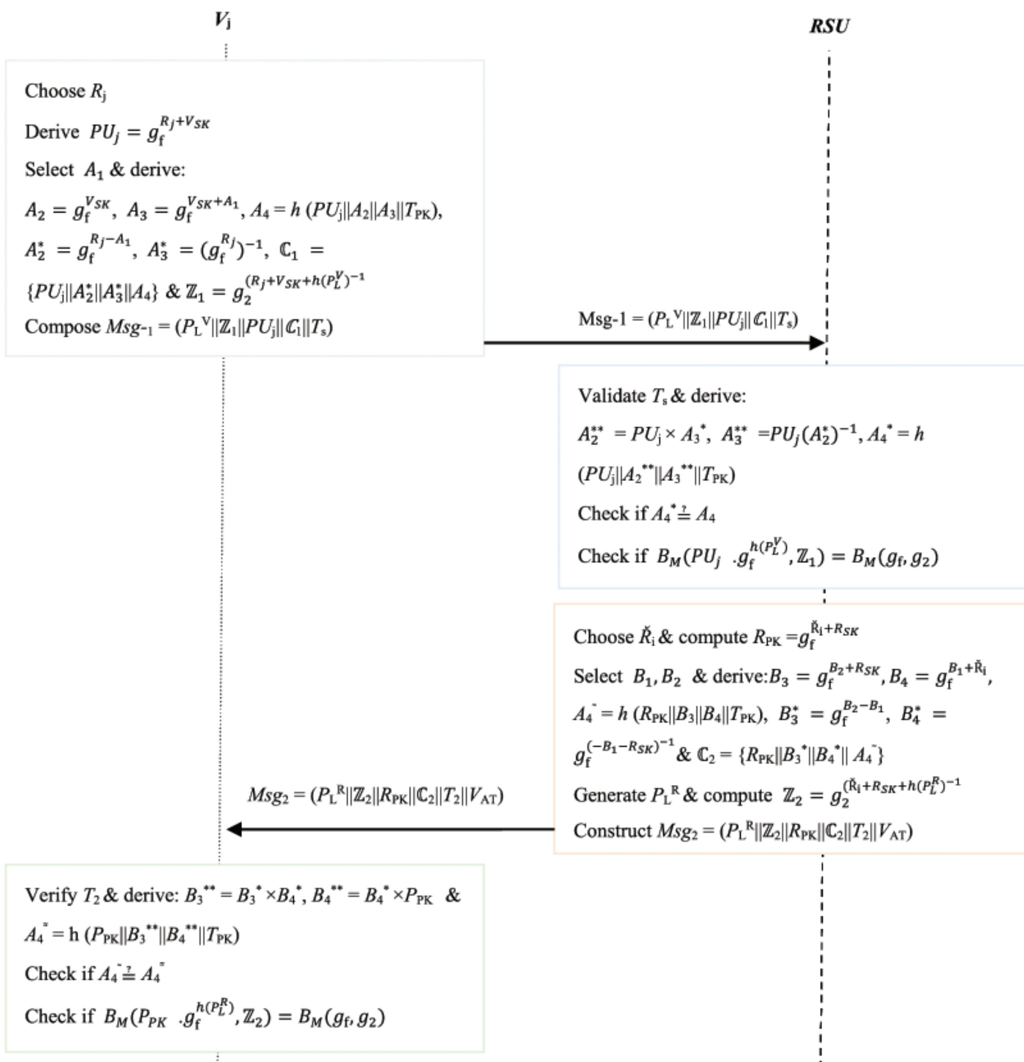

Figure 3: Authentication phase

Step 4: After obtaining *Msg-1*, RSU_i confirms the freshness of timestamp T_s. In particular,, authentication is aborted if the timestamp freshness check flops. Otherwise, payload and source integrity are checked next.

Step 5: RSU_i derives $A_2^{**} = PU_j \times A_3^*$, $A_3^{**} = PU_j(A_2^*)^{-1}$ and $A_4^* = h\ (PU_j \| A_2^{**} \| A_3^{**} \| T_{PK})$. After that, it checks whether or not $A_4^* \stackrel{?}{=} A_4$, such that authentication is aborted when the two values are unequal. Otherwise, RSU_i has successfully validated PU_j and $\mathbb{C}_1$, confirming V_j's authenticity. The reason is that the parameters computed at V_j and RSU_i are equal. Consequently, A_2^{**} and A_3^{**} computed at RSU_i should equal A_2^* and A_3^*derived at V_j. Given that $A_2^{**} = PU_j \times A_3^*$, $A_2^{**} = g_f^{R_j+V_{SK}} \times = (g_f^{R_j})^{-1}$. That is, $A_2^{**} = g_f^{R_j+V_{SK}-R_j} = g_f^{V_{SK}} = \mathrm{A}_2$. Similarly, $A_3^{**} = PU_j(A_2^*)^{-1}$. Hence, $A_3^{**} = g_f^{R_j+V_{SK}}(g_f^{R_j-A_1})^{-1} = g_f^{R_j+V_{SK}-R_j+A_1} = g_f^{V_{SK}+A_1} = \mathrm{A}_3$. This step completes the certificate verification process.

Step 6: RSU_i verifies the integrity of the transmitted payload using the signature derived previously. To accomplish this step, it checks whether or not $B_M(PU_j.\ g_f^{h(P_L^V)}, \mathbb{Z}_1) = B_M(g_f, g_2)$. The reason is that $B_M(PU_j.\ g_f^{h(P_L^V)},\ \mathbb{Z}_1) = B_M(g_f^{R_j+V_{SK}}.g_f^{h(P_L^V)},\ g_2^{(R_j+V_{SK}+h(P_L^V)^{-1}})$, implying that the following condition holds: $B_M(PU_j.\ g_f^{h(P_L^V)},\ \mathbb{Z}_1) = B_M\left(g_f^{R_j+V_{SK}+h(P_L^V)},\ g_2^{(R_j+V_{SK}+h(P_L^V)^{-1}}\right) = B_M(g_f, g_2)$. provided the preceding condition holds, the payload P_L^V passes the integrity verification and is accepted by RSU_i. Otherwise, RSU_i rejects the payload P_L^V. This step completes the $V_j \rightarrow RSU_i$ authentication procedures. Therefore, the $RSU_i \rightarrow V_j$ authentication is executed next, as elaborated in the following steps:

Step 7: RSU_i chooses some random number $\check{R}_i$ from $\mathbb{R}$ to act as its one-time secret key, where $\check{R}_1, \check{R}_2, \ldots \check{R}_{\mathbb{R}} \in Z_p^*$. Thereafter, RSU_i derives its corresponding pubic key as $R_{PK} = g_f^{\hat{\mathrm{R}}_i+R_{SK}}$, where $i = 1, 2, \ldots.\ \mathfrak{R}$.

Step 8: RSU_i derives certificate $\mathbb{C}_2$ by randomly choosing parameters $B_1,\ B_2 \in Z_p^*$ and computing values $B_3 = g_f^{B_2+R_{SK}}$ and $B_4 = g_f^{B_1+\hat{\mathrm{R}}_i}$. Thereafter, it computes parameters $A_4^{\sim} = h\,(R_{PK} \| B_3 \| B_4 \| T_{PK})$, $B_3^* = g_f^{B_2-B_1}$, $B_4^* = g_f^{(-B_1-R_{SK})^{-1}}$ and $\mathbb{C}_2 = \{R_{PK} \| B_3^* \| B_4^* \|\ A_4^{\sim}\}$.

Step 9: To preserve the integrity of the payload $P_L{}^R$ generated at RSU_i, it computes signature $\mathbb{Z}_2 = g_2^{(\hat{\mathrm{R}}_i+R_{SK}+h(P_L^R)^{-1}}$. Thereafter, it constructs message $Msg_2 = (P_L{}^R \| \mathbb{Z}_2 \| R_{PK} \| \mathbb{C}_2 \| T_2 \| V_{AT})$ that it sends to V_j.

Step 10: After receiving message Msg_2, V_j validates the freshness of timestamp T_2, such that the session is aborted upon verification failure. This step is followed by the validity check of the source (RSU_i) and the integrity checks of message Msg_2. These checks are accomplished by computing parameters $B_3^{**} = B_3^* \times B_4^*$ and $B_4^{**} = B_4^* \times P_{PK}$. Thereafter, it computes value $A_4^{\tilde{\sim}} = \mathrm{h}\ (P_{PK} \| B_3^{**} \| B_4^{**} \| T_{PK})$ and checks whether or not $A_4^{\sim} \stackrel{?}{=} A_4^{\tilde{\sim}}$. If the two values are equivalent, P_{PK} and certificate $\mathbb{C}_2$ pass the verification checks. Therefore, RSU_i is successfully authenticated by vehicle V_j. Ideally, parameter $A_4^{\tilde{\sim}}$ computed by V_j should equal parameter $A_4^{\sim}$ derived at RSU_i. Additionally, $B_3^{**} = B_3$ and $B_4^{**} = B_4$. Given that $B_3^{**} = B_3^* \times B_4^*$, $B_3^{**} = g_f^{B_2-B_1} \times g_f^{(-B_1-R_{SK})^{-1}} = g_f^{B_2-B_1} \times g_f^{(B_1+R_{SK})}$. That is, $B_3^{**} = g_f^{B_2-B_1+B_1+R_{SK}}$. Hence, $B_3^{**} = g_f^{B_2+R_{SK}} = B_3$. Similarly, $B_4^{**} = B_2^* \times P_{PK} = g_f^{(-B_1-R_{SK})^{-1}} \times g_f^{\hat{\mathrm{R}}_i+R_{SK}}$. That is, $B_4^{**} = g_f^{\hat{\mathrm{R}}_i+R_{SK}+B_1-R_{SK}}$. Therefore, $B_4^{**} = g_f^{\hat{\mathrm{R}}_i+B_1} = B_4$.

Step 11: Upon successful verification of certificate $\mathbb{C}_2$, V_j proceeds to validate the integrity of payload $P_L{}^R$. To accomplish this step, it checks whether or not $B_M(P_{PK}.\ g_f^{h(P_L^R)},\ \mathbb{Z}_2) = B_M(g_f,\ g_2)$. The reason is as follows:

$$B_M(P_{PK} \cdot g_f^{h(P_L^R)},\ \mathbb{Z}_2) = B_M(g_f^{\hat{\mathrm{R}}_i+R_{SK}}.g_f^{h(P_L^R)}, g_2^{(\hat{\mathrm{R}}_i+R_{SK}+h(P_L^R)^{-1}})$$

Therefore, $B_M(P_{PK}.\ g_f^{h(P_L^R)},\ \mathbb{Z}_2) = B_M\ (g_f^{\hat{\mathrm{R}}_i+R_{SK}+h(P_L^R)}, g_2^{(\hat{\mathrm{R}}_i+R_{SK}+h(P_L^R)^{-1}}) = B_M(g_f, g_2)$. provided that the preceding condition holds, the payload P_L^R passes the integrity verification. Therefore, it is accepted by V_j; otherwise, it is rejected. This step completes the $RSU_i \rightarrow V_j$ authentication procedures. Lastly, *Step 12* is invoked to provide some levels of conditional tracing of any malicious RSU_j.

Step 12: In this phase, the payload P_L^{R*} is assumed to originate from a malicious RSU_j. As such, RSU_j's real identity needs to be established. Accordingly, the vehicle access token $V_{AT} = R_{PK}^p * g_f^p$ is deployed. The idea is to check RSU_j's real identity ID_R in TA's access control list ACL. The following procedure is invoked to retrieve record $\{ID_R, R_{PK}^{p*q}\}$ from ACL:

$$(V_{AT})^q (g_f^{p*q})^{-1} = (R_{PK}^p * g_f^p)^q (g_f^{p*q})^{-1} = (R_{PK}^{p*q} * g_f^{p*q})(g_f^{p*q})^{-1} = R_{PK}^{p*q}$$

Therefore, the proposed protocol could attain conditional privacy for all communicating entities. This aspect is essential in identifying and revoking malicious entities from the network.

4 Security Analysis

This section ultimately aims to offer some formal security analysis of the proposed scheme, followed by its informal security analysis. Formal security analysis demonstrates the semantic security of the authentication procedures. Conversely, informal security analysis shows our scheme's resilience against typical VANET attacks. The detailed illustration of the analyses is presented in the following sub-sections.

4.1 Formal Security Analysis

This sub-section deploys the BAN logic to analyze the proposed protocol. Accordingly, various postulates and notations of the BAN logic are used, including the nonce verification rule (NVR), message–meaning rule (MMR), jurisdiction rule (JR), and decomposition rule (DR). Table 3 presents some of the BAN logic notations.

Table 3: Notations in the BAN logic

Symbol	Description
z	Private key
$M\| \equiv N$	*M* trusts statement *N*
$M\| \sim N$	*M* once said *N*
$M \triangleleft N$	*M* receives statement *N*
#N	Statement *N* is fresh
$\{N\}_Z$	Statement *N* is enciphered by secret key *Z*
$M \overset{Z}{\leftrightarrow} N$	Secret key *Z* is shared between *M* and *N*

The BAN logic mathematical formulations of the various rules are described using the notations in Table 3.

MMR:

$$\frac{M| \equiv N \overset{Z}{\leftrightarrow} M,\ M \triangleleft \{A\}_Z}{M| \equiv N| \sim A}$$

This rule means that M believes N said A, provided that M believes that key Z is the shared key with N. Moreover, M sees A, which is enciphered using key Z.

JR:

$$\frac{M| \equiv N \Rightarrow A,\ M| \equiv N| \equiv A}{M| \equiv A}$$

This rule implies that M trusts A if M believes N has jurisdiction over A and M trusts that N believes A.

NVR:

$$\frac{M| \equiv \#(A),\ M| \equiv N| \sim A}{M| \equiv N| \equiv A}$$

This rule means that M believes N trusts A provided that M believes A has been transmitted recently, and N has said A.

DR:

i) $$\frac{M \lhd (A, B)}{M \lhd A}$$

ii) $$\frac{M| \equiv \#(A)}{M| \equiv \#(A, B)}$$

iii) $$\frac{M| \equiv (A, B)}{M| \equiv (A)}$$

The three postulates under DR are essential in decomposing the transmitted messages and validating their freshness. DR (i) implies that M can discern A provided that it observes all messages. Meanwhile, DR (ii) means that the combination of A and B is fresh provided that one of these components is fresh. However, the consequences of DR (iii) are that amalgamating an assortment of message components means that entities trust them independently.

The formal analysis of this scheme, a rigorous process that follows a systematic approach, proceeds as follows using the BAN logic notations and the preceding rules.

We obtain P1 in accordance with the provisions of MMR.

$\mathbf{P_1}$: $$\frac{RSU_i| \equiv RSU_i \overset{\mathbb{C}_1}{\leftrightarrow} V_j,\ RSU_i \lhd \{\text{Msg}_{-1}\}_{\mathbb{C}_1}}{RSU_i |\equiv V_j| \sim \{\text{Msg}_{-1}\}}$$

Using the NVR, P_2 is obtained as:

$\mathbf{P_2}$: $$\frac{RSU_i| \equiv \#(T_2),\ RSU_i| \equiv V_j| \sim \{\text{Msg}_{-1}\}}{RSU_i| \equiv V_j| \equiv \{\text{Msg}_{-1}\}}$$

Similarly, applying JR yields P_3, as shown below:

$\mathbf{P_3}$: $$\frac{RSU_i| \equiv V_j \Rightarrow \{\text{Msg}_1\},\ RSU_i| \equiv V_j| \equiv \{\text{Msg}_{-1}\}}{RSU_i| \equiv \{\text{Msg}_{-1}\}}$$

However, in accordance with DR, P_4 is obtained.

$\mathbf{P_4}$: $RSU_i| \equiv RSU_i \overset{\mathbb{C}_1}{\leftrightarrow} V_j$

This being the case, MMR is applied to yield P_5.

P$_5$: $\dfrac{V_j| \equiv V_j \overset{\mathbb{C}_2}{\leftrightarrow} RSU_i,\ V_j \lhd \{\mathrm{Msg}_2\}_{\mathbb{C}_2}}{V_j |\equiv RSU_i| \sim \{\mathrm{Msg}_2\}}$

Thereafter, the application of NVR yields P$_6$, as shown below:

P$_6$: $\dfrac{V_j| \equiv \#(T_1),\ V_j| \equiv RSU_i| \sim \{\mathrm{Msg}_2\}}{V_j| \equiv RSU_i| \equiv \{\mathrm{Msg}_2\}}$

However, the usage of JR yields P$_7$.

P$_7$: $\dfrac{V_j| \equiv RSU_i \Rightarrow \{\mathrm{Msg}_2\},\ V_j| \equiv RSU_i| \equiv \{\mathrm{Msg}_2\}}{V_j| \equiv \{\mathrm{Msg}_2\}}$

Thereafter, DR is applied to obtain P$_8$ and P$_9$.

P$_8$: $V_j| \equiv V_j \overset{\mathbb{C}_2}{\leftrightarrow} RSU_i$

Also,

P$_9$: $V_j| \equiv RSU_i| \equiv V_j \overset{\mathbb{C}_2}{\leftrightarrow} RSU_i$

Since $V_j| \equiv \#(T_1)$, P$_{10}$ is obtained as follows:

P$_{10}$: $V_j| \equiv \#(T_1 + 1)$

Consequently, we get P$_{11}$ as:

P$_{11}$: $V_j| \equiv \#\{(T_1 + 1)\mathbb{C}_1\}$.

This is because $V_j| \equiv \mathbb{C}_1$, and $V_j \lhd \{(T_2 + 1)\mathbb{C}_2\}$

Based on MMR, the following is obtained:

P$_{12}$: $V_j| \equiv RSU_i| \sim \{(T_2 + 1)\mathbb{C}_2\}$.

Similarly, NVR is deployed to yield P$_{13}$.

P$_{13}$: $V_j| \equiv RSU_i| \equiv \{(T_2 + 1)\mathbb{C}_2\}$

Then, it follows that:

P$_{14}$: $V_j| \equiv RSU_i| \equiv V_j \overset{\mathbb{C}_2}{\leftrightarrow} RSU_i$

Using the same logic, we obtain P$_{14}$ as:

P$_{14}$: $RSU_i| \equiv V_j| \equiv V_j \overset{\mathbb{C}_1}{\leftrightarrow} RSU_i$

The BAN logic proves that the messages exchanged in this protocol are fresh. Hence, replay attacks are easily detected. Additionally, the BAN logic proves that this protocol offers a secure mechanism for validating the exchanged messages through the certificates encapsulated in the messages.

4.2 Informal Security Analysis

This sub-section explains and verifies some theorems to prove that our technique provides the desired security and privacy characteristics. The theorems formulated are also deployed to prove that this approach is robust against some common VANET attack vectors.

Theorem 1: This protocol can withstand packet replays.

Proof: Timestamps are incorporated in all messages exchanged between V_j and RSU_i to curb packet replay attacks. For instance, message *Msg-1* $= (P_L{}^V \| \mathbb{Z}_1 \| PU_j \| \mathbb{C}_1 \| T_s)$ sent from V_j to RSU_i contains timestamp T_s. The freshness of this timestamp is verified at RSU_i. Particularly, the session is aborted when the freshness check flops. Similarly, message $Msg_2 = (P_L{}^R \| \mathbb{Z}_2 \| R_{PK} \| \mathbb{C}_2 \| T_2 \| V_{AT})$ forwarded from RSU_i towards V_j incorporates timestamp T_2 that is also validated by V_j. The authentication session is aborted when T_2 fails the freshness check.

Theorem 2: Robust authentication is executed.

Proof: To keep intruders at bay, this protocol utilizes certificates attached to all exchanged messages. For example, vehicle V_j derives certificate $\mathbb{C}_1 = \{PU_j \| A_2^* \| A_3^* \| A_4\}$, where PU_j is the one-time public key for V_j, $A_2^* = g_f^{R_j - A_1}$, $A_3^* = (g_f^{R_j})^{-1}$ and $A_4 = h\ (PU_j \| A_2 \| A_3 \| T_{PK})$. After that, this certificate is encapsulated in message $Msg\text{-}1 = (P_L{}^V \| \mathbb{Z}_1 \| PU_j \| \mathbb{C}_1 \| T_s)$ that is forwarded to RSU_i. Similarly, RSU_i derives certificate $\mathbb{C}_2 = \{R_{PK} \| B_3{}^* \| B_4{}^* \|\ A_4{}^\sim\}$, where R_{PK} is the public key of RSU_i, $B_3^* = g_f^{B_2 - B_1}$, $B_4^* = g_f^{(-B_1 - R_{SK})^{-1}}$ and $A_4{}^\sim = h\ (R_{PK} \| B_3 \| B_4 \| T_{PK})$. These certificates are mutually validated before the messages received are accepted.

Theorem 3: MitM and message falsification attacks are prevented.

Proof: To prevent these attacks, V_j and RSU_i validate all received messages. This objective is achieved using the signatures and certificates derived by these entities. For example, to validate the correctness of message $Msg\text{-}1 = (P_L{}^V \| \mathbb{Z}_1 \| PU_j \| \mathbb{C}_1 \| T_s)$ sent from V_j, RSU_i computes $A_2^{**} = PU_j \times A_3{}^*$, $A_3^{**} = PU_j(A_2^*)^{-1}$ and $A_4{}^* = h\ (PU_j \| A_2{}^{**} \| A_3{}^{**} \| T_{PK})$ before checking whether or not $A_4{}^* \stackrel{?}{=} A_4$. The authentication procedures are terminated when the verification flops. Otherwise, PU_j and $\mathbb{C}_1$ in $Msg\text{-}1$ are successfully verified. Hence, V_j is authentic. Similarly, upon receiving message $Msg_2 = (P_L{}^R \| \mathbb{Z}_2 \| P_{PK} \| \mathbb{C}_2 \| T_2 \| V_{AT})$ from RSU_i, V_j computes parameters $B_3{}^{**} = B_3{}^* \times B_4{}^*$, $B_4{}^{**} = B_4{}^* \times P_{PK}$ and $A_4{}^{\tilde{\sim}} = \mathrm{h}\ (P_{PK} \| B_3{}^{**} \| B_4{}^{**} \| T_{PK})$. This step is followed by checking whether or not $A_4{}^\sim \stackrel{?}{=} A_4{}^{\tilde{\sim}}$. If the two values are equivalent, P_{PK} and certificate $\mathbb{C}_2$ in Msg_2 pass the verification checks. Therefore, RSU_i is successfully authenticated by vehicle V_j.

Theorem 4: Source and message integrity are preserved in this scheme.

Proof: In this protocol, signatures are used to ensure that messages are not changed over the communication channels as they are transmitted among the communicating parties. For example, V_j computes signature $\mathbb{Z}_1 = g_2^{(R_j + V_{SK} + h(P_L^V)^{-1}}$, where R_j is the one-time secret key for V_j, V_{SK} is the secret key for vehicle V_j, and $P_L{}^V$ is the payload that V_j wants to exchange with RSU_i. Thereafter, this signature is encapsulated in message $Msg\text{-}1 = (P_L{}^V \| \mathbb{Z}_1 \| PU_j \| \mathbb{C}_1 \| T_s)$, which is transmitted to RSU_i. Upon receipt of $Msg\text{-}1$, RSU_i derives $A_4{}^* = h\ (PU_j \| A_2{}^{**} \| A_3{}^{**} \| T_{PK})$ that it deploys to validate the integrity of the payload and its source. This objective is accomplished by checking whether or not $A_4{}^* \stackrel{?}{=} A_4$ and to abort the session if the two values are dissimilar. Similarly, RSU_i derives signature $\mathbb{Z}_2 = g_2^{(\hat{R}_i + R_{SK} + h(P_L^R)^{-1}}$, where $\check{R}_i$ is the one-time secret key for RSU_i, R_{SK} is the secret key for RSU_i, and $P_L{}^R$ is the payload that RSU_i wants to exchange with V_j. Thereafter this signature is incorporated in message $Msg_2 = (P_L{}^R \| \mathbb{Z}_2 \| R_{PK} \| \mathbb{C}_2 \| T_2 \| V_{AT})$ that is forwarded to V_j also follows a verification process to derive $A_4{}^{\tilde{\sim}} = h\ (P_{PK} \| B_3{}^{**} \| B_4{}^{**} \| T_{PK})$ that is utilized to verify source and message integrity. To accomplish this step, it checks whether or not $A_4{}^\sim \stackrel{?}{=} A_4{}^{\tilde{\sim}}$ and aborts the session when the validation flops.

Theorem 5: Anonymity of the network entities is preserved.

Proof: Suppose that adversary $\mathring{A}$ is interested in establishing the actual identity of roadside unit RSU_i (i.e., ID_R). To achieve this objective, $\mathring{A}$ intercepts messages $Msg\text{-}1 = (P_L{}^V \| \mathbb{Z}_1 \| PU_j \| \mathbb{C}_1 \| T_s)$ and $Msg_2 = (P_L{}^R \| \mathbb{Z}_2 \| R_{PK} \| \mathbb{C}_2 \| T_2 \| V_{AT})$, where $P_L{}^V$ and $P_L{}^R$ are the vehicle and RSU payloads, respectively. Meanwhile, $\mathbb{Z}_1 = g_2^{(R_j + V_{SK} + h(P_L^V)^{-1}}$, $PU_j = g_f^{R_j + V_{SK}}$, $\mathbb{C}_1 = \{PU_j \| A_2^* \| A_3^* \| A_4\}$, $\mathbb{Z}_2 = g_2^{(\hat{R}_i + R_{SK} + h(P_L^R)^{-1}}$, $R_{PK} = g_f^{R_{SK} + q}$, $\mathbb{C}_2 = \{R_{PK} \| B_3{}^* \| B_4{}^* \|\ A_4{}^\sim\}$, $A_4 = h\ (PU_j \| A_2 \| A_3 \| T_{PK})$, $A_2^* = g_f^{R_j - A_1}$ and $A_3^* = (g_f^{R_j})^{-1}$, $\mathrm{A}_3 = g_f^{V_{SK} + A_1}$,

$A_4\tilde{} = h\ (R_{PK}\|B_3\|B_4\|T_{PK})$, $B_3^* = g_f^{B_2-B_1}$, $B_4^* = g_f^{(-B_1-R_{SK})^{-1}}$ and $V_{AT} = R_{PK}^p * g_f^p$. Evidently, *Msg-1* and Msg_2 do not contain any information that can help $\mathring{A}$ in successfully recovering ID_R. Similarly, none of the parameters in the messages contain any information that may help $\mathring{A}$ in uniquely identifying V_j.

Theorem 6: The proposed scheme prevents forgery attacks.

Proof: Suppose adversary $\mathring{A}$ is interested in forging the derived signatures and certificates. In the proposed scheme, the derived signatures incorporate one-time secret keys and private keys of the communicating entities. For example, the signature $\mathbb{Z}_2 = g_2^{(\hat{R}_i+R_{SK}+h(P_L^R)^{-1}}$ is derived by RSU_i, where $\check{R}_i$ is the one-time secret key for RSU_i, R_{SK} is its secret key, and $P_L{}^R$ is its payload. Consequently, attacker $\mathring{A}$ is unable to forge this signature. The reason is that $\check{R}_i$ is only known to RSU_i while R_{SK} is only known to RSU_i and TA, and, hence, not available to $\mathring{A}$. Similarly, the signature $\mathbb{Z}_1 = g_2^{(R_j+V_{SK}+h(P_L^V)^{-1}}$ is computed by V_j, where R_j is its one-time secret key, V_{SK} is its secret key, and $P_L{}^V$ is its payload. However, R_j is only known to V_j, and V_{SK} is only known to TA and V_j. Devoid of these parameters, $\mathring{A}$ can never forge signature $\mathbb{Z}_1$. The same principle applies to certificates $\mathbb{C}_1 = \{PU_j\|A_2^*\|A_3^*\|A_4\}$ and $\mathbb{C}_2 = \{R_{PK}\|B_3{}^*\|B_4{}^*\|A_4\tilde{}\}$ owing to the incorporation of secrets PU_j, R_{PK}, R_{SK}, T_{PK}, $\check{R}_i$ and R_j, all of which are unavailable to $\mathring{A}$.

Theorem 7: Key secrecy is preserved.

Proof: Let's consider a scenario where the attacker has intercepted the one-time private key for for V_j (i.e., R_j) and the one-time secret key $\check{R}_i$ for RSU_i for the current session. The attacker's objective is to use these keys to compute subsequent communication session certificates $\mathbb{C}_1^* = \{PU_j\|A_2^*\|A_3^*\|A_4\}$ and $\mathbb{C}_2^* = \{R_{PK}\|B_3{}^*\|B_4{}^*\|A_4\tilde{}\}$, where $A_4 = h(PU_j\|A_2\|A_3\|T_{PK})$, $A_2^* = g_f^{R_j-A_1}$, $A_3^* = (g_f^{R_j})^{-1}$, $A_4\tilde{} = h\ (R_{PK}\|B_3\|B_4\|T_{PK})$, $B_3 = g_f^{B_2+R_{SK}}$, $B_4 = g_f^{B_1+\hat{R}_i}$, $B_3^* = g_f^{B_2-B_1}$ and $B_4^* = g_f^{(-B_1-R_{SK})^{-1}}$. However, the parameters R_j and $\check{R}_i$ are refreshed after every session because they are one-time keys. This key refreshment is a crucial security measure that significantly hampers the attacker's efforts, making this derivation ineffective.

Theorem 8: Impersonation attacks are prevented.

Proof: Suppose that adversary $\mathring{A}$ is interested in masquerading as vehicle V_j or roadside unit RSU_i. To achieve this scenario, an attempt is made to compute signatures $\mathbb{Z}_1 = g_2^{(R_j+V_{SK}+h(P_L^V)^{-1}}$, $\mathbb{Z}_2 = g_2^{(\hat{R}_i+R_{SK}+h(P_L^R)^{-1}}$ and certificates $\mathbb{C}_1 = \{PU_j\|A_2^*\|A_3^*\|A_4\}$ and $\mathbb{C}_2 = \{R_{PK}\|B_3{}^*\|B_4{}^*\|A_4\tilde{}\}$. Specifically, $A_4 = h\ (PU_j\|A_2\|A_3\|T_{PK})$, $A_2^* = g_f^{R_j-A_1}$, $A_3^* = (g_f^{R_j})^{-1}$, $A_4\tilde{} = h\ (R_{PK}\|B_3\|B_4\|T_{PK})$, $B_3^* = g_f^{B_2-B_1}$ and $B_4^* = g_f^{(-B_1-R_{SK})^{-1}}$. However, as described in *Theorem 6*, this step requires access to R_j and $\check{R}_i$ (one-time secret keys), secret keys V_{SK} and R_{SK}, TA's public key T_{PK}, R_{PK} (public key of RSU_i) and PU_j (one-time public key for V_j), amongst other parameters. Additionally, $\mathring{A}$ needs to guess random nonces B_1, $B_2 \in Z_p^*$ correctly . Although message $Msg\text{-}1 = (P_L{}^V\|\mathbb{Z}_1\|PU_j\|\mathbb{C}_1\|T_s)$ contains PU_j, it is encapsulated in other parameters $\mathbb{Z}_1$, $\mathbb{C}_1$, T_s, and payload $P_L{}^V$. Similarly, message $Msg_2 = (P_L{}^R\|\mathbb{Z}_2\|R_{PK}\|\mathbb{C}_2\|T_2\|V_{AT})$ contains R_{PK}, but it is encapsulated in parameters $\mathbb{Z}_2$, $\mathbb{C}_2$, T_2, V_{AT}, and payload $P_L{}^R$. As such, adversarial impersonation of these signatures and certificates will flop.

Theorem 9:Communication session unlinkability is preserved.

Proof: To achieve communication session unlinkability, the proposed protocol deploys stochastic one-time secret keys $\check{R}_i$ and R_j to derive the distinct signatures $\mathbb{Z}_1$, $\mathbb{Z}_2$ and certificates $\mathbb{C}_1$ and $\mathbb{C}_2$ for each session. Particularly, $\mathbb{Z}_1 = g_2^{(R_j+V_{SK}+h(P_L^V)^{-1}}$, $\mathbb{Z}_2 = g_2^{(\hat{R}_i+R_{SK}+h(P_L^R)^{-1}}$, $\mathbb{C}_1 = \{PU_j\|A_2^*\|A_3^*\|A_4\}$, $\mathbb{C}_2 = \{R_{PK}\|B_3{}^*\|B_4{}^*\|A_4\tilde{}\}$, $A_4\tilde{} = h\ (R_{PK}\|B_3\|B_4\|T_{PK})$, $B_3^* = g_f^{B_2-B_1}$, $B_3 = g_f^{B_2+R_{SK}}$ and $B_4 = g_f^{B_1+\hat{R}_i}$ and

$B_4^* = g_1^{(-B_1 - R_{SK})^{-1}}$. Since that $\check{R}_i$ and R_j are frequently refreshed, the generated signatures and certificates are always unique for each communication session, making it difficult for the adversary $\mathring{A}$ to associate the source of the transmitted messages to any particular RSU_i or V_j.

Theorem 10: The proposed protocol provides conditional privacy for the communicating entities.

Proof: In this scheme, RSUs and vehicles deploy signatures and certificates instead of their actual identities. This method effectively hides their actual identities from other communicating parties. Based on *Theorem 9*, adversarial tracking of RSU_i and V_j is not feasible. However, TA can trace the exact identity of any RSU_i. This goal is accomplished by deploying its certificate $\mathbb{C}_2 = \{R_{PK} \| B_3{}^* \| B_4{}^* \| A_4{}^{\sim}\}$. Suppose a malicious RSU_j has sent that payload P_L^{R*}, and TA is interested in establishing the real identity of this RSU_i. To attain this objective, the vehicle access token $V_{AT} = R_{PK}^p * g_f^p$ is deployed. This step encompasses checking RSU_j 's real identity ID_R on TA'*s* access list. Therefore, the following procedure is invoked to retrieve record $\{ID_R, R_{PK}^{p*q}\}$ from the access list: $(V_{AT})^q (g_f^{p*q})^{-1} = (R_{PK}^p * g_f^p)^q (g_f^{p*q})^{-1} = (R_{PK}^{p*q} * g_f^{p*q})(g_f^{p*q})^{-1} = R_{PK}^{p*q}$. Having tracked this malicious certificate to a particular RSU_i, TA can confidently flag this RSU_i as malicious and eliminate it from the network.

Theorem 11: The proposed protocol assures nonrepudiation of exchanged messages.

Proof: In this scheme, receivers can always validate the authenticity of the sender using certificates $\mathbb{C}_f = \{PU_j \| A_2^* \| A_3^* \| A_4\}$ and $\mathbb{C}_2 = \{R_{PK} \| B_3{}^* \| B_4{}^* \| A_4{}^{\sim}\}$. Additionally, the integrity of the exchanged messages is verified using signatures $\mathbb{Z}_1 = g_2^{(R_j + V_{SK} + h(P_L^V)^{-1}}$ and $\mathbb{Z}_2 = g_2^{(\hat{R}_i + R_{SK} + h(P_L^R)^{-1}}$. The verification procedures are described in *Steps 5*, *6*, *10*, and *Step 11* of the *authentication phase* in Section 3.3. Suppose that a dispute on the exchanged messages has emerged. In this case, the concerned parties can contact TA so that the disputed message can be tracked to its actual sender. This goal is accomplished by invoking the procedures in *Theorem 10*, after which this particular entity, if found to be the malicious actor, will be promptly eliminated from the network.

Theorem 12: Our scheme supports scalability and adaptability.

Proof: During the registration phase, all the vehicles and RSUs must register at the TA and be issued with security tokens deployable in the subsequent phases. After the successful registration phase, the TA stores the parameter set $\{ID_R, R_{PK}^{p*q}\}$ in its access list ACL. After this, the TA will not be involved in the authentication procedures between the V_j and RSU. As such, there is no need to search through the TA's ACL during the authentication process. Therefore, our scheme can accommodate the authentication of more vehicles without the TA becoming a bottleneck. This means that more vehicles can join the network to support more users without compromising the performance of the authentication procedures. Importantly, our scheme not only supports scalability but also renders the authentication process adaptable, ensuring it can flexibly handle varying user loads.

5 Performance Analysis

This sub-section aims to conduct a comparative analysis of our scheme. This goal is achieved using metrics commonly deployed in the evaluation of authentication schemes, including the computation overheads, the communication overheads, and the offered security features. The specific details of this comparative analysis are described below.

5.1 Computation Overhead

The proposed protocol incorporates certificates and signatures in all exchanged messages. As such, the time taken to verify these certificates and signatures is considered. Let T_H, T_{BP}, T_{PM}, T_{SE}, T_{BSM}, T_{BPA},

T_{BMH}, T_{PA}, and T_{E} denote the time taken for one-way hashing, BP, EC point multiplication, symmetric encryption, BP scalar multiplication, BP point addition, BP map to point hash, EC point addition, and exponential operations, respectively. Additionally, let $T_{G_{CS}}$ denote the time the sender takes to generate a single signature and certificate and let $T_{V_{CS}}$ represent the time that the receiver takes to verify the single signature and certificate. As such, the total computation time during authentication is denoted as $T_{G_{CS}} + T_{V_{CS}}$. During single signature and certificate generation, $5T_{\text{E}} + T_{\text{H}}$ are executed. Hence, $T_{G_{CS}} = 5T_{\text{E}} + T_{\text{H}}$. During source and integrity verification using the single certificate and signature, $1T_{\text{H}}$, $2T_{\text{BP}}$, and $2T_{\text{PM}}$ operations are executed. As such, $T_{V_{CS}} = 2T_{\text{BP}} + 2T_{\text{PM}} + T_{\text{H}}$. To establish the computation costs of the various cryptographic operations, we deploy the MIRACL cryptographic library. Additionally, a laptop with the features presented in Table 4 is utilized.

Table 4: Execution environment

Feature	Description
Clock frequency	2.4 GHz
RAM size	4 GB
Operating system	Ubuntu 18.04.5 LTS
Processor	Intel(R) Core i7-8565U

Using the execution durations in Table 4, the computation costs for the diverse cryptographic operations are given in Table 5.

Table 5: Computation costs for cryprographic operations

Operation	Execution time (ms)
One-way hashing, T_{H}	0.003
Map to point hash operation associated with BP, T_{BMH}	0.128
Point multiplication associated with EC, T_{PM}	2.063
Point addition associated with EC, T_{PA}	0.008
Symmetric encryption, T_{SE}	0.276
Bilinear pairing, T_{BP}	5.175
Exponentiation operation on λ, T_{E}	2.124
Point addition associated with BP, T_{BPA}	0.018
Scalar multiplication associated with BP, T_{BSM}	2.146

Based on the values in Table 5, $T_{G_{CS}} = 10.623$ ms, $T_{V_{CS}} = 14.479$ ms. Therefore, the proposed protocol takes 25.102 ms to generate and verify a single signature and certificate. Table 6 shows the execution time comparison of the other related schemes.

As shown in Table 6, the protocol in Reference [33] requires 26.998 ms to fully execute the authentication process, whilst the scheme in Reference [44] needs 18.68 ms. The protocols in References [53,8,32,31], take 31.83, 17.74, 37.31, and 15.51 ms, respectively. As illustrated in Fig. 4, the scheme in Reference [32] exhibits the longest execution time of 37.31 ms, which is attributed to the numerous pairing activities required during its authentication.

Table 6: Computation overheads comparisons

Scheme	Operations	Time (ms)
Bagga et al. [7]	$T_{\mathrm{E}} + T_{\mathrm{BP}} + 5T_{\mathrm{PA}} + 5T_{\mathrm{PM}} + 15T_{\mathrm{H}}$	17.74
Shen et al. [31]	$3T_{\mathrm{E}} + 4T_{\mathrm{BSM}} + 3T_{\mathrm{BPA}} + 6T_{\mathrm{H}}$	15.51
Rabieh et al. [32]	$3T_{\mathrm{E}} + 2T_{\mathrm{BSM}} + 5T_{\mathrm{BP}} + 6T_{\mathrm{BMH}}$	37.31
Luo et al. [33]	$2T_{\mathrm{BP}} + 8T_{\mathrm{PM}} + 8T_{\mathrm{BPA}}$	26.998
Ali et al. [44]	$2T_{\mathrm{BP}} + T_{\mathrm{E}} + 3T_{\mathrm{PM}}$	18.68
Tan et al. [53]	$2T_{\mathrm{E}} + 2T_{\mathrm{BP}} + 8T_{\mathrm{BSM}} + 2T_{\mathrm{BPA}} + 8T_{\mathrm{H}}$	31.83
Proposed	$2T_{\mathrm{BP}} + 2T_{\mathrm{PM}} + 5T_{\mathrm{E}} + 2T_{\mathrm{H}}$	25.10

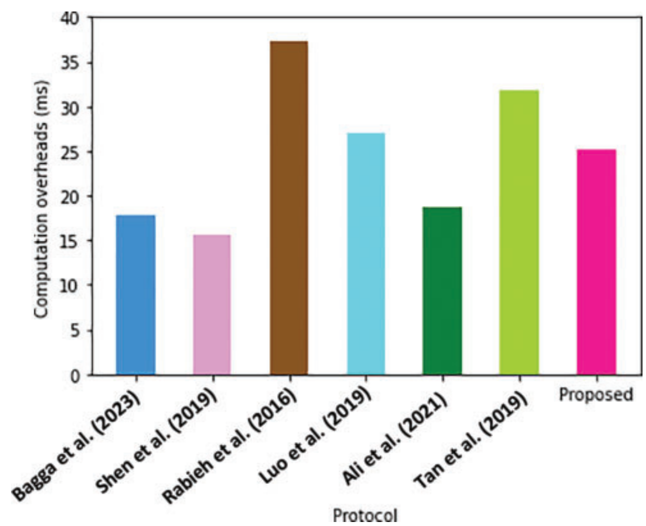

Figure 4: Computation overheads comparisons [7,31–33,44,53]

However, the protocol in Reference [31] takes the shortest time to fully execute. The reason is that it generally executes one-way hashing, scalar multiplication, point addition, and exponentiation operations on λ, all of which are lightweight compared with the BP operations in Reference [32]. The proposed protocol also executes two BP operations, rendering it relatively computationally extensive. However, it supports the highest number of security features, as shown in Table 9 of Section 5.3. Although the scheme in Reference [31] exhibits the shortest execution time, it does not offer backward key secrecy, conditional privacy, backward key secrecy, and unlinkability.

Similarly, the protocol in Reference [7] does not provide conditional privacy, nonrepudiation, and source and message integrity. Moreover, it has not been evaluated against forgeries and message falsifications. The scheme in Reference [44] fails to offer key secrecy and has not been evaluated against attacks such as MitM and impersonations.

5.2 Communication Overheads

The system setup and registration phases are carried out once, hence they are excluded in the derivation of the communication overheads of the authentication protocols. Accordingly, only the two messages exchanged during authentication are deployed to derive the communication costs of our protocol. The two messages are $Msg\text{-}1 = (P_L{}^V \| \mathbb{Z}_1 \| PU_j \| \mathbb{C}_1 \| T_s)$, which is constructed at V_j and forwarded to RSU_i; and $Msg_2 = (P_L{}^R \| \mathbb{Z}_2 \| R_{PK} \| \mathbb{C}_2 \| T_2 \| V_{AT})$, which is composed of RSU_i and transmitted to V_j. In this implementation, the output of T_H is 20 bytes [49], $ID_R = T_s = T_2 = V_{AT}$ = 4 bytes [49], $P_L^R = P_L^V = \mathbb{Z}_1 = \mathbb{Z}_2 = \mathbb{C}_1 = \mathbb{C}_2 = 20$ bytes [61], and $PU_j = R_{PK} = 16$ bytes [61]. Using these values, the communication costs of the proposed approach are derived and shown in Table 7.

Table 7: Derivation of communication costs

Message	Size (bytes)
$Msg\text{-}1 = (P_L{}^V \| \mathbb{Z}_1 \| PU_j \| \mathbb{C}_1 \| T_s)$	80
$P_L^V + \mathbb{Z}_1 + PU_J + \mathbb{C}_1 + \mathrm{T}_1$	
$Msg_2 = (P_L{}^R \| \mathbb{Z}_2 \| R_{PK} \| \mathbb{C}_2 \| T_2 \| V_{AT})$	84
$P_L^R + \mathbb{Z}_2 + R_{PK} + \mathbb{C}_2 + T_2 + V_{AT}$	
Total	164

As shown in Table 7, the two messages exchanged in the proposed protocol have a size of 164 bytes. Table 8 compares the communication costs of the various approaches. In Reference [53], the system parameter set $\{T_{SN}, ID_{RSU}, R, Q, Cert\}$ is broadcast. Thereafter, the authentication requests $\langle Request, ID_i, TS_2, \mathcal{R}_i, A_i, \mathcal{L}_i \rangle$ from n vehicles are distributed. Eventually, the acknowledgment message $\left\langle TS_3, ID_i^+, Cert_i^+ \right\rangle$ is transmitted to each verified vehicle. Hence, the entire process takes 300 bytes.

Table 8: Communication overheads comparisons

Scheme	No. of messages	Size (bytes)
Bagga et al. [7]	2	264
Shen et al. [31]	2	824
Rabieh et al. [32]	2	340
Luo et al. [33]	2	365
Ali et al. [44]	4	369
Tan et al. [53]	3	300
Proposed	2	164

Similarly, the protocol in Reference [7] requires two messages to fully execute authentication and key agreement. The first message is the authentication message $\{TID_i, VF_i, VG_i, \mathrm{VL}_i, r_1, TS_{Vi}\}$, which is sent from V_i to TA, the size of which is 116 bytes. The second message is the authentication replay $\{Q_i, V_2, V_3, V_4, TS_{TA_2}\}$, which is 148 bytes in length. Therefore, the entire process consumes 264 bytes. Meanwhile, the messages exchanged in Reference [46] include $\{OID_i, AID_{i,1}\}$ and $\{\Omega_i, AID_i, pk_{i,s}\}$ sent from V_i to the key generation center (KGC); $\{AID_i, psk_i\}$ and $\{pk_{i,r}\}$ sent from the KGC to V_i. The four messages are 369 bytes in length, as shown in Fig. 5. For the scheme in Reference [31], two messages are exchanged during the authentication phase. Specifically, V_i sends message $\{IDi, Ti, gi = (e(g, g)^{r_1}, r_2, \eta\}$, the size of which is s, to RSU. Thereafter, this message is relayed to the traffic center server (TCS), and the entire process requires 824 bytes. The communication overhead analyses for the protocols in References [32] and [33] are similar to the one in Reference [31]. However, their total lengths are 340 bytes and 365 bytes, respectively. As shown in Fig. 5, our scheme exhibits the smallest communication overhead at 164 bytes. The protocol in Reference [31] has a total message length of 824 bytes, which is the highest. It is followed by the schemes in References [7,32,33,44,60] in sequence.

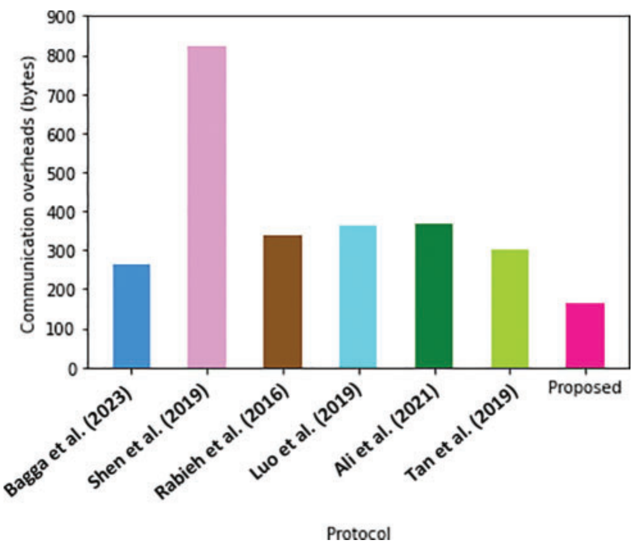

Figure 5: Comparative evaluation of communication overheads [7,31–33,44,53]

Considering the communication limitations in most VANET devices, such as OBUs, the proposed technique is the most applicable in this environment.

5.3 Supported Security Features

This sub-section evaluates our protocol and other related schemes against typical VANET attacks, including packet replays, message falsification, forgery, impersonation, and MitM. Additionally, these security techniques are analyzed based on whether or not they offer non-repudiation, authentication, conditional privacy, unlinkability, key secrecy, anonymity, and source and message integrity. Table 9 presents the results of this analysis.

Table 9: Supported security features comparisons

	[53]	[7]	[44]	[31]	[32]	[33]	Proposed
Security features							
Authentication	√	√	√	√	√	√	√
Source and message integrity	–	–	√	√	√	√	√
Anonymity	–	√	√	√	√	√	√
Backward key secrecy	–	√	–	–	–	√	√
Forward key secrecy	–	√	–	–		√	√
Unlinkability	–	√	√	–	√	–	√

(Continued)

Table 9 (continued)

	[53]	[7]	[44]	[31]	[32]	[33]	Proposed
Conditional privacy	√	–	√	–	√	√	√
Non-repudiation	×	–	√	√		–	√
Attacks resilience							
Packet replays	√	√	√	√	×	×	√
Message falsification	–	–	–	√	×	√	√
Forgery	√	–	√	√	×	√	√
Impersonation	–	√	–	√	×	×	√
MitM	×	√	–	√	×	×	√

As shown in Table 9, the protocol in Reference [53] supports only four security features. Therefore, it is the most vulnerable. Those follow this protocol in Reference [32], which supports only five security features. The schemes in References [7,33,44] support eight security features each. However, the scheme in [31] supports nine security features. Meanwhile, the proposed protocol supports all 13 features. Therefore, it is the most secure. Using the nine security features in Reference [31] as bases, our approach evidently offers a 44.44% enhancement in the supported privacy and security features. Note that our protocol improves communication overhead by 37.88%. The proposed scheme provides enhanced security at minor communication costs and moderately short execution time.

5.4 Implementation

This sub-section tests the performance of the proposed scheme under network simulators. Specifically, the proposed protocol is simulated in Network Simulator version 3 (NS3) in a 2000 m × 2000 m simulation area over a duration of 300 s. The MAC layer deployed is 802.11 p, while the transmission power is 50 mW. The data transmission rate is 6 Mbps, and broadcasting rate is 100 ms. In this environment, we test the efficiency of our protocol in terms of throughput, packet delivery ratio (PDR), and end-to-end (E2E) latency. In all simulation scenarios, the number of vehicles is increased from the initial value of 10 to a maximum of 100. As shown in Fig. 6, network throughput rises steadily as the number of vehicles is incremented.

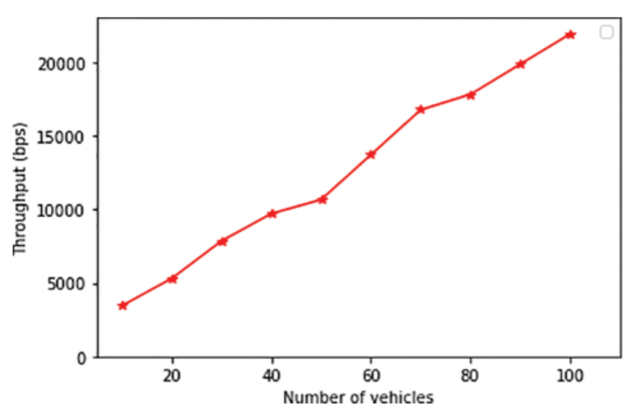

Figure 6: Network throughput

This finding is attributed to the high number of packets sent across the network when the number of vehicles surges. Fig. 7 shows the variations of packet delivery rate at different vehicle volumes.

As Fig. 7 demonstrates, PDR decreases as the number of vehicles increases. This decline is a direct result of network congestions, which are triggered by the surge in packet volume during high traffic. These congestions lead to packet drops, thereby reducing the number of successfully delivered packets. Fig. 8 further illustrates the impact of increasing vehicular traffic on E2E latencies.

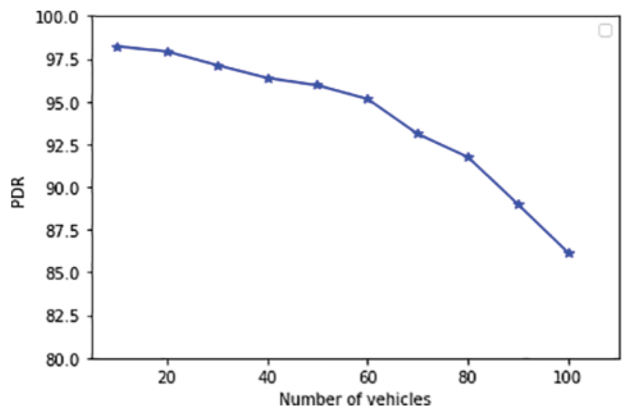

Figure 7: Network PDR

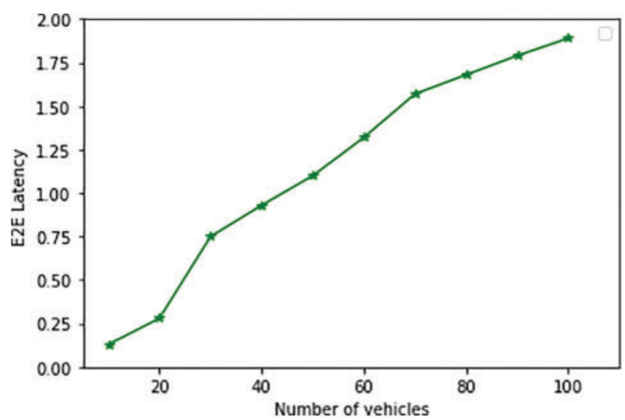

Figure 8: E2E latency

Fig. 8 shows an increase in E2E latencies as vehicles surge. At high traffic levels, end devices are overwhelmed with many data packets and requests that must be processed. Therefore, E2E generally increases as the number of vehicles in the network increases.

6 Conclusion

VANETs have been shown to face serious challenges in spite of their outstanding services, such as route management, intelligent navigation and file sharing. For example, malicious modification of driving route information can result in traffic jams, whilst illegitimate alteration of speed information can cause traffic accidents. Given that these issues directly affect human life and property safety, the development of strong message authentication schemes is extremely urgent. This aspect is particularly important because it will reduce the number of privacy and security violations that will eventually lead to the success of VANET applications. Hence, several security solutions have been presented in the recent past. Nevertheless, many of these schemes are either inefficient or are vulnerable to attacks. Accordingly, the proposed scheme has been demonstrated to be provably secure under the BAN logic model. It has also been shown to be robust against typical VANET attacks exampled by MitM, impersonations, forgery, replays and message falsification. The computation cost in our scheme is relatively lower compared with other BP-based techniques. Moreover, it results in a 44.44% improvement in the supported privacy and security features, as well as a 37.88% reduction in communication overheads.

Acknowledgement: Not applicable.

Funding Statement: This research is supported by Teaching Reform Project of Shenzhen University of Technology under Grant No. 20231016.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Vincent Omollo Nyangaresi, Arkan A. Ghaib, Hend Muslim Jasim, Zaid Ameen Abduljabbar, Junchao Ma; data collection: Mustafa A. Al Sibahee, Abdulla J. Y. Aldarwish, Ali Hasan Ali, Husam A. Neamah; analysis and interpretation of results: Vincent Omollo Nyangaresi, Arkan A. Ghaib, Hend Muslim Jasim, Zaid Ameen Abduljabbar, Junchao Ma; writing—original draft preparation: Mustafa A. Al Sibahee, Abdulla J. Y. Aldarwish, Ali Hasan Ali, Husam A. Neamah; writing—review and editing: Vincent Omollo Nyangaresi, Arkan A. Ghaib, Hend Muslim Jasim, Zaid Ameen Abduljabbar, Junchao Ma; supervision: Zaid Ameen Abduljabbar, Junchao Ma. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data that support the findings of this study are available from the corresponding author, upon reasonable request.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] X. Dai, Z. Xiao, H. Jiang, and J. C. S. Lui, "UAV-assisted task offloading in vehicular edge computing networks," *IEEE Trans. Mob. Comput.*, vol. 23, no. 4, pp. 2520–2534, 2023. doi: 10.1109/TMC.2023.3259394.

[2] G. Sun, Y. Zhang, H. Yu, X. Du, and M. Guizani, "Intersection fog-based distributed routing for V2V communication in urban vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 6, pp. 2409–2426, 2019. doi: 10.1109/TITS.2019.2918255.

[3] Y. Ren, Z. Lan, L. Liu, and H. Yu, "EMSIN: Enhanced multi-stream interaction network for vehicle trajectory prediction," *IEEE Trans. Fuzzy Syst.*, pp. 1–15, 2024. doi: 10.1109/TFUZZ.2024.3360946.

[4] J. Zhang and Q. Zhang, "On the security of a lightweight conditional privacy-preserving authentication in VANETs," *IEEE Trans. Inform. Forensic. Sec.*, vol. 18, pp. 1037–1038, 2021. doi: 10.1109/TIFS.2021.3066277.

[5] Z. Xiao, J. Shu, H. Jiang, G. Min, H. Chen and Z. Han, "Perception task offloading with collaborative computation for autonomous driving," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 2, pp. 457–473, 2022. doi: 10.1109/JSAC.2022.3227027.

[6] G. Sun, L. Song, H. Yu, V. Chang, X. Du and M. Guizani, "V2V routing in a VANET based on the autoregressive integrated moving average model," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 908–922, 2018. doi: 10.1109/TVT.2018.2884525.

[7] P. Bagga, A. K. Das, and J. J. Rodrigues, "Bilinear pairing-based access control and key agreement scheme for smart transportation," *Cyber Secur. Appl.*, vol. 1, 2023, Art. no. 100001. doi: 10.1016/j.csa.2022.100001.

[8] I. Ali, Y. Chen, N. Ullah, R. Kumar, and W. He, "An efficient and provably secure ECC-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1278–1291, 2021. doi: 10.1109/TVT.2021.3050399.

[9] G. Sun, Y. Zhang, D. Liao, H. Yu, X. Du and M. Guizani, "Bus-trajectory-based street-centric routing for message delivery in Urban vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7550–7563, 2018. doi: 10.1109/TVT.2018.2828651.

[10] J. Zhang, H. Fang, H. Zhong, J. Cui, and D. He, "Blockchain-assisted privacy-preserving traffic route management scheme for fog-based vehicular ad-hoc networks," *IEEE Trans. Netw. Serv. Manage.*, vol. 20, pp. 2854–2868, 2023. doi: 10.1109/TNSM.2023.3238307.

[11] Z. Qu, X. Liu, and M. Zheng, "Temporal-spatial quantum graph convolutional neural network based on schrödinger approach for traffic congestion prediction," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, pp. 8677–8686, 2022. doi: 10.1109/TITS.2022.3203791.

[12] K. A. -A. Mutlaq, V. O. Nyangaresi, M. A. Omar, and Z. A. Abduljabbar, "Symmetric key based scheme for verification token generation in internet of things communication environment," in *EAI Int. Conf. Appl. Cryptogr. Comput. Commun.*, Springer, 2022, pp. 46–64. doi: 10.1007/978-3-031-17081-2_4.

[13] G. Luo *et al.*, "EdgeCooper: Network-aware cooperative LiDAR perception for enhanced vehicular awareness," *IEEE J. Sel. Areas Commun.*, vol. 42, pp. 207–222, 2023. doi: 10.1109/JSAC.2023.3322764.

[14] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, K. -K. R. Choo and Y. Park, "On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1736–1751, 2021. doi: 10.1109/TVT.2021.3050614.

[15] H. Jiang, M. Wang, P. Zhao, Z. Xiao, and S. Dustdar, "A utility-aware general framework with quantifiable privacy preservation for destination prediction in LBSs," *IEEE/ACM Trans. Netw.*, vol. 29, no. 5, pp. 2228–2241, 2021. doi: 10.1109/TNET.2021.3084251.

[16] Z. Xiao *et al.*, "Understanding private car aggregation effect via spatio-temporal analysis of trajectory data," *IEEE Trans. Cybern.*, vol. 53, no. 4, pp. 2346–2357, 2021. doi: 10.1109/TCYB.2021.3117705.

[17] J. Ma and J. Hu, "Safe consensus control of cooperative-competitive multi-agent systems via differential privacy," *Kybernetika*, vol. 58, no. 3, pp. 426–439, 2022. doi: 10.14736/kyb-2022-3-0426.

[18] W. Li, W. Susilo, C. Xia, L. Huang, F. Guo and T. Wang, "Secure data integrity check based on verified public key encryption with equality test for multi-cloud storage," *IEEE Trans. Dependable Secur. Comput.*, pp. 1–15, 2024. doi: 10.1109/TDSC.2024.3375369.

[19] B. Chen, J. Hu, and B. K. Ghosh, "Finite-time tracking control of heterogeneous multi-AUV systems with partial measurements and intermittent communication," *Sci. China Inf. Sci.*, vol. 67, no. 5, 2024, Art. no. 152202. doi: 10.1007/s11432-023-3903-6.

[20] L. Zhao, H. Xu, S. Qu, Z. Wei, and Y. Liu, "Joint trajectory and communication design for UAV-assisted symbiotic radio networks," *IEEE Trans. Veh. Technol.*, vol. 73, pp. 8367–8378, 2024. doi: 10.1109/TVT.2024.3356587.

[21] X. Liu, Y. Wang, Z. Zhou, K. Nam, C. Wei and C. Yin, "Trajectory prediction of preceding target vehicles based on lane crossing and final points generation model considering driving styles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 8720–8730, 2021. doi: 10.1109/TVT.2021.3098429.

[22] J. Thota, N. F. Abdullah, A. Doufexi, and S. Armour, "V2V for vehicular safety applications," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 6, pp. 2571–2585, 2019. doi: 10.1109/TITS.2019.2920738.

[23] Y. Li, Y. Qi, and L. Lu, *Secure and Efficient V2V Communications for Heterogeneous Vehicle Ad Hoc Networks*. Los Alamitos, CA, USA: IEEE, 2017, pp. 93–99. doi: 10.1109/NaNA.2017.54.

[24] V. O. Nyangaresi, Z. A. Abduljabbar, I. Y. Maolood, M. A. A. Sibahee, J. Ma and A. J. Y. Aldarwish, *Transient Session Key Derivation Protocol for Key Escrow Prevention in Public Key Infrastructure*. Switzerland: Springer, 2022, pp. 103–116. doi: 10.1007/978-3-031-25222-8_9.

[25] Y. Wang, H. Zhong, Y. Xu, J. Cui, and F. Guo, "Efficient extensible conditional privacy-preserving authentication scheme supporting batch verification for VANETs," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 5460–5471, 2016. doi: 10.1002/sec.1710.

[26] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, S. Manickam, and S. M. Hanshi, "Efficient conditional privacy preservation with mutual authentication in vehicular ad hoc networks," *IEEE Access*, vol. 8, pp. 144957–144968, 2020. doi: 10.1109/ACCESS.2020.3014678.

[27] J. Zhang, Q. Zhang, X. Lu, and Y. Gan, "A novel privacy-preserving authentication protocol using bilinear pairings for the VANET environment," *Wirel. Commun. Mob. Comput.*, vol. 2021, no. 1, 2021, Art. no. 6692568. doi: 10.1155/2021/6692568.

[28] S. Wang and N. Yao, "LIAP: A local identity-based anonymous message authentication protocol in VANETs," *Comput. Commun.*, vol. 112, pp. 154–164, 2017. doi: 10.1016/j.comcom.2017.09.005.

[29] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Gener. Comput. Syst.*, vol. 84, pp. 216–227, 2018. doi: 10.1016/j.future.2017.07.002.

[30] Z. A. Abduljabbar *et al.*, "Session-dependent token-based payload enciphering scheme for integrity enhancements in wireless networks," *J. Sens. Actuator Netw.*, vol. 11, no. 3, 2022, Art. no. 55. doi: 10.3390/jsan11030055.

[31] J. Shen, D. Liu, X. Chen, J. Li, N. Kumar and P. Vijayakumar, "Secure real-time traffic data aggregation with batch verification for vehicular cloud in VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 807–817, 2019. doi: 10.1109/TVT.2019.2946935.

[32] K. Rabieh, M. M. Mahmoud, and M. Younis, "Privacy-preserving route reporting schemes for traffic management systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2703–2713, 2016. doi: 10.1109/TVT.2016.2583466.

[33] M. Luo, Y. Wen, and X. Hu, "Practical data transmission scheme for wireless sensor networks in heterogeneous IoT environment," *Wirel. Pers. Commun.*, vol. 109, no. 1, pp. 505–519, 2019. doi: 10.1007/s11277-019-06576-8.

[34] B. Ying and A. Nayak, "Anonymous and lightweight authentication for secure vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10626–10636, 2017. doi: 10.1109/TVT.2017.2744182.

[35] S. Yu, J. Lee, K. Lee, K. Park, and Y. Park, "Secure authentication protocol for wireless sensor networks in vehicular communications," *Sensors*, vol. 18, no. 10, 2018, Art. no. 3191. doi: 10.3390/s18103191.

[36] M. J. Sadri and M. R. Asaar, "A lightweight anonymous two-factor authentication protocol for wireless sensor networks in Internet of Vehicles," *Int. J. Commun. Syst.*, vol. 33, no. 14, 2020, Art. no. e4511. doi: 10.1002/dac.4511.

[37] C. -M. Chen, B. Xiang, Y. Liu, and K. -H. Wang, "A secure authentication protocol for internet of vehicles," *IEEE Access*, vol. 7, pp. 12047–12057, 2019. doi: 10.1109/ACCESS.2019.2891105.

[38] L. Wu *et al.*, "An efficient privacy-preserving mutual authentication scheme for secure V2V communication in vehicular ad hoc network," *IEEE Access*, vol. 7, pp. 55050–55063, 2019. doi: 10.1109/ACCESS.2019.2911924.

[39] H. Vasudev, V. Deshpande, D. Das, and S. K. Das, "A lightweight mutual authentication protocol for V2V communication in internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6709–6717, 2020. doi: 10.1109/TVT.2020.2986585.

[40] S. A. Alfadhli, S. Lu, K. Chen, and M. Sebai, "MFSPV: A multi-factor secured and lightweight privacy-preserving authentication scheme for VANETs," *IEEE Access*, vol. 8, pp. 142858–142874, 2020. doi: 10.1109/ACCESS.2020.3014038.

[41] M. N. Aman, U. Javaid, and B. Sikdar, "A privacy-preserving and scalable authentication protocol for the internet of vehicles," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 1123–1139, 2020. doi: 10.1109/JIOT.2020.3010893.

[42] T. Alladi, S. Chakravarty, V. Chamola, and M. Guizani, "A lightweight authentication and attestation scheme for in-transit vehicles in IoV scenario," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 14188–14197, 2020. doi: 10.1109/TVT.2020.3038834.
[43] V. O. Nyangaresi and N. Petrovic, "Efficient PUF based authentication protocol for internet of drones," in *2021 Int. Telecommun. Conf. (ITC-Egypt)*, Alexandria, Egypt, 2021, pp. 1–4. doi: 10.1109/ITC-Egypt52936.2021.9513902.
[44] F. Ali, Y. Chen, N. Ullah, M. Afzal, and H. E. Wen, "Bilinear pairing-based hybrid signcryption for secure heterogeneous vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 5974–5989, 2021. doi: 10.1109/TVT.2021.3078806.
[45] A. K. Sutrala, P. Bagga, A. K. Das, N. Kumar, J. J. P. C. Rodrigues and P. Lorenz, "On the design of conditional privacy preserving batch verification-based authentication scheme for internet of vehicles deployment," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5535–5548, 2020. doi: 10.1109/TVT.2020.2981934.
[46] J. Liu, A. Ren, L. Zhang, R. Sun, X. Du and M. Guizani, "A novel secure authentication scheme for heterogeneous internet of things," in *ICC, 2019-2019 IEEE Int. Conf. Commun. (ICC)*, Shanghai, China, 2019, pp. 1–6. doi: 10.1109/ICC.2019.8761951.
[47] M. Cui, D. Han, and J. Wang, "An efficient and safe road condition monitoring authentication scheme based on fog computing," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9076–9084, 2019. doi: 10.1109/JIOT.2019.2927497.
[48] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for VANETs," *IEEE Trans. Very Large-Scale Integr. (VLSI) Syst.*, vol. 27, no. 12, pp. 2792–2801, 2019. doi: 10.1109/TVLSI.2019.2929420.
[49] H. Zhang and F. Zhao, "Cross-domain identity authentication scheme based on blockchain and PKI system," *High-Confid. Comput.*, vol. 3, no. 1, 2023, Art. no. 100096. doi: 10.1016/j.hcc.2022.100096.
[50] C. Lin, D. He, X. Huang, N. Kumar, and K. -K. R. Choo, "BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks," *IEEE Trans. Intell. Trans. Syst.*, vol. 22, no. 12, pp. 7408–7420, 2020. doi: 10.1109/TITS.2020.3002096.
[51] M. A. Shawky *et al.*, "Blockchain-based secret key extraction for efficient and secure authentication in VANETs," *J. Inf. Secur. Appl.*, vol. 74, 2023, Art. no. 103476. doi: 10.1016/j.jisa.2023.103476.
[52] M. A. Shawky, M. Bottarelli, G. Epiphaniou, and P. Karadimas, "An efficient cross-layer authentication scheme for secure communication in vehicular ad-hoc networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 7, pp. 8738–8754, 2023. doi: 10.1109/TVT.2023.3244077.
[53] H. Tan and I. Chung, "Secure authentication and key management with blockchain in VANETs," *IEEE Access*, vol. 8, pp. 2482–2498, 2019. doi: 10.1109/ACCESS.2019.2962387.
[54] Z. A. Abduljabbar, V. O. Nyangaresi, J. Ma, M. A. Al Sibahee, M. S. Khalefa and D. G. Honi, "MAC-based symmetric key protocol for secure traffic forwarding in drones," in *Future Access Enablers for Ubiquitous and Intelligent Infrastructures*, Springer, 2022, pp. 16–36. doi: 10.1007/978-3-031-15101-9_2.
[55] J. Mou, K. Gao, P. Duan, J. Li, A. Garg and R. Sharma, "A machine learning approach for energy-efficient intelligent transportation scheduling problem in a real-world dynamic circumstance," *IEEE Trans. Intell. Trans. Syst.*, vol. 24, no. 12, pp. 15527–15539, 2022. doi: 10.1109/TITS.2022.3183215.
[56] Y. Yin, Y. Guo, Q. Su, and Z. Wang, "Task allocation of multiple unmanned aerial vehicles based on deep transfer reinforcement learning," *Drones*, vol. 6, no. 8, 2022, Art. no. 215. doi: 10.3390/drones6080215.
[57] Y. Yang, L. Wei, J. Wu, C. Long, and B. Li, "A blockchain-based multidomain authentication scheme for conditional privacy preserving in vehicular ad-hoc network," *IEEE Internet of Things J.*, vol. 9, no. 11, pp. 8078–8090, 2021. doi: 10.1109/JIOT.2021.3107443.
[58] S. Son, J. Lee, Y. Park, K. Park, and A. K. Das, "Design of blockchain-based lightweight V2I handover authentication protocol for VANET," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, pp. 1346–1358, 2022. doi: 10.1109/TNSE.2022.3142287.
[59] S. A. Syed *et al.*, "QoS aware and fault tolerance based software-defined vehicular networks using cloud-fog computing," *Sensors*, vol. 22, no. 1, 2022, Art. no. 401. doi: 10.3390/s22010401.

[60] Y. Yao, B. Zhao, J. Zhao, F. Shu, Y. Wu and X. Cheng, "Anti-jamming technique for IRS aided JRC system in mobile vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, pp. 12550–12560, 2024. doi: 10.1109/TITS.2024.3384038.

[61] X. Zeng, G. Xu, X. Zheng, Y. Xiang, and W. Zhou, "E-AUA: An efficient anonymous user authentication protocol for mobile IoT," *IEEE Internet of Things J.*, vol. 6, no. 2, pp. 1506–1519, 2018. doi: 10.1109/JIOT.2018.2847447.