

Authentication with privacy-preserving scheme for 5G-enabled vehicular networks

Mays A. Hamdan, Amel Meddeb Makhoulf, Hassene Mnif

NTS'COM Lab, ENET'COM, University of Sfax, Sfax, Tunisia

Article Info

Article history:

Received Jun 13, 2023

Revised Aug 3, 2023

Accepted Sep 12, 2023

Keywords:

5G-enabled vehicular network

Authentication

Cryptography

Efficient cryptography

Elliptic curve

Security and privacy

ABSTRACT

The 5G-enabled vehicular network is an innovative technology that has promise for intelligent transportation systems. It enables the transmitting of messages about traffic that deliver the most recent information on congestion, road conditions, and driving surroundings. The communication channel used by vehicle networks is inherently open, which unfortunately exposes the system to privacy and security concerns. To solve the problems of deploying a safe vehicular network, some academics have put forth plans. However, a number of current methods have significant computational or communication overhead costs. To solve this problem, an efficient and secure authentication with a privacy-preserving (ES-APP) scheme established elliptic curve encryption is introduced. With the proposed ES-APP, the data signed and verified for vehicle-to-vehicle and vehicle-to-infrastructure modes in the 5G-based vehicular network are more effective. The ES-APP scheme's goal is to meet the criteria for the security and privacy of the 5G-enabled automotive network. Ultimately, this work discusses the critical survey of the existing studies and the expected outcome for the ES-APP scheme and further works in the 5G-enabled vehicular network.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Amel Meddeb Makhoulf

NTS'COM Lab, ENET'COM, University of Sfax

Sfax, Tunisia

Email: amel.makhoulf@enetcom.usf.tn

1. INTRODUCTION

Intelligent transportation systems (ITSs) are designed to offer drivers and pedestrians with safer, wiser, and more effective services [1]–[6]. A key element of ITS is the vehicular network. With the arrival of the 5G era, every car joint to the vehicular system is now thought to be outfitted with cutting-edge wireless communication technology for vehicle-to-everything (V2X) connectivity [7]–[11].

Demand from a wide range of users has led to a fast increase in the number of urban vehicles [12]–[14]. Due to the current application environment's need for high-speed transmission and minimal delay, conventional vehicular ad hoc networks (VANETs) based on 4G networks fall short [15]–[19]. The 5G mobile system has both broad coverage and a high bandwidth. As a result, there are various possible issues with vehicle networks [20]–[23].

The data indicates that while the data transfer-based average rate is over 100 Mb/s, the data transmission-based peak rate via 5G wireless networks can reach 20 Gb/s [24]–[27]. The supported network can provide a more steady connection and has 1000 times the capacity of current networks [28], [29]. But, this feature is coupled by worries about privacy, performance effectiveness, and security. Therefore, it is important to prop-

erly research these issues in the vehicular network. As a result, before accepting received messages, receivers on-board units (OBUs) should verify their accuracy and integrity. Anonymous communication is necessary to maintain privacy and fulfil the unlinkability condition for the users.

The rest of this work is constructed as: section 2, provides taxonomy of existing privacy-preserving authentication schemes for vehicular network. Section 3, provides the background of this paper. Section 4, shows the proposed ES-APP scheme. Sections 5 and 6 show the expected results and conclusion of this paper, respectively.

2. LITERATURE REVIEW

This section provides a quick overview of the various authentication systems for vehicular networks that also protect users' privacy. Existing privacy-preserving authentication can be broken down into three main categories: group signature (GS), public key infrastructure and identity.

2.1. Public key infrastructure

To protect users' personal information, public key infrastructure(PKI)-based authentication schemes have the TA pressure a large number of private/public keys and corresponding certificates onto the OBUs of vehicles. These schemes [30]–[32] are based on PKI. The European Telecommunications Standards Institute (ETSI) has defined a PKI-based message authentication mechanism at the European level PKI in Cincilla *et al.* [30]. The vehicular PKI (VPKI) must be highly scalable if it is to support a large number of ITS stations (ITS-Ss). Joshi *et al.* [31] looked at issues with ITS's C2C architecture's network and security. Joshi *et al.* [31] proposed to develop an efficient method for C2C communication based on the concept of event-triggered broadcast. For data authenticity, their rely on PKI-based sender authentication. Asghar *et al.* [32] presented a system that does away with exponential growth in CRL size while simultaneously streamlining the authentication procedure. With simulations, Asghar *et al.* [32] demonstrated how the time it takes to authenticate a user is drastically cut down. Nevertheless, the major disadvantage of a public key infrastructure-based- privacy-preserving authentication schemes are:

- Certificate management becomes difficult when a large number of private/public key pairs and their matching certificates must be preloaded to the OBUs of the vehicles.
- With the loading of large keys and their related certifications, the amount of time a vehicle can be stored in a vehicle environment is restricted;
- To further increase computational and transmission costs, the verifier must validate the certificate that is embedded in the message signature.

2.2. Group signature

Multiple researchers collaborate to create a GS-based, privacy-preserving authentication scheme to overcome the drawbacks of using public key infrastructure. These protocols allow individuals within a group to anonymously sign on behalf of that group. The group manager has access to the sender's details in case of a disagreement. These schemes [33], [34] are based on GS. Tiwari *et al.* [33] showed the first comprehensive measuring campaign of an operational PKI that complies with ETSI standards. With a series of tests conducted on a network of hundreds of devices, we are able to evaluate the efficiency and scalability of PKI. Lim *et al.* [34] presented a practical key-management approach for GS-based authentication, where a group is expanded to include numerous roadside units. Besides from providing a safe method of transporting group keys to mobile nodes, Lim *et al.* [34] technique also guarantees other safety measures. However, the primary restrictions of GS-based authentication with privacy-preserving schemes are:

- It's essential to rebuild the entire team;
- The private keys of a network of moving nodes are not simple to update;
- If the group isn't very big, the enemy can easily pick out its members; and
- Once the number of vehicles revoked is high, the signature's verification technique becomes time-consuming for vehicular networks.

2.3. Identity (ID)

In order to address the shortcomings of preexisting approaches, like public key infrastructure-based and GS-based methods, several academics have developed a new identity-based privacy-preserving authentication methodology. In order to create a private key using the same identity information as the public key, the TA

must first extract the public key from the identity information. When a message is signed using a private key, only the sender and the verifier will be able to read it.

In order to achieve the goals of confidentiality, anonymity, and security in a VANET, Alazzawi *et al.* [35] suggested a novel pseudo-identity-based approach. In the event that the roadside unit (RSU) is compromised, the proposed approach uses a pseudonym in the joining procedure to conceal the true identity. A robust and efficient content-sharing mechanism for 5G-enabled vehicle networks was proposed by Cui *et al.* [36]. Vehicles with content download requests can swiftly sort through the nearby vehicles, select an appropriate proxy vehicle based on its capabilities and location, and request the proxy vehicle's content services. Bayat *et al.* [37] proposed a new method of securing vehicle-to-vehicle communications by introducing an innovative authentication technique for VANETs. The suggested technique is an RSU-based scheme, with the trusted authority's (TA) master key placed in a tamper-proof device at the RSUs. To combat these issues plaguing VANETs, Cui *et al.* [38] offered a mutual authentication technique that is both secure and private. In this research, Al-Shareeda *et al.* [39] offered a secure and efficient conditional privacy-preserving authentication (CPPA) technique for protecting against impersonation attacks and increasing performance efficiency. Messages are signed and verified with the use of bilinear pair cryptography in the proposed SE-CPPA scheme. To ensure safe communication in VANET, Alshudukhi *et al.* [40] presented a lightweight authentication mechanism that also protects conditional privacy. Combining tamper-proof device (TPD) based schemes with roadside unit (RSU) based schemes, the suggested strategy is well-suited for tackling security and privacy concerns. To address the security concerns of 5G-enabled automotive networks, Al-Shareeda *et al.* [41] provided an efficient data-sharing mechanism that does not require RSU. Our process consisted of six steps: initializing the TA (TASetup), creating pseudonym identities (PIDGen), creating keys (KeyGen), signing messages (MsgSign), verifying individual signatures (SigVerify), and verifying groups of signatures (BSigVerify). Identity schemes are categorized into Table 1.

Table 1. The existing identity established authentication with privacy-preserving schemes

Author's name	Algorithm	Limitation
Alazzawi <i>et al.</i> [35]	Elliptic curve cryptography	i) vulnerable to side-channel attacks; ii) suffer from privacy-preserving requirements; and iii) not satisfying unlinkability requirements.
Cui <i>et al.</i> [36]	Elliptic curve cryptography	i) used a large number of ECC operations and ii) massive computation cost.
Bayat <i>et al.</i> [37]	Bilinear pair cryptography	i) massive computation and communication costs; ii) used time-consuming (MAP-to-point); and iii) not satisfying revocation requirement.
Cui <i>et al.</i> [38]	Elliptic curve cryptography	i) vulnerable to replay and modification attacks; ii) not satisfying authentication, integrity, non-repudiation; iii) suffer from privacy-preserving requirements; and iv) not satisfying unlinkability requirements.
Al-Shareeda <i>et al.</i> [39]	Bilinear pair cryptography	i) massive computation costs; ii) massive communication costs; and iii) used time-consuming operations.
Alshudukhi <i>et al.</i> [40]	Elliptic curve cryptography	i) vulnerable to side-channel attacks and ii) high computation and communication costs.
Al-Shareeda <i>et al.</i> [41]	Elliptic curve cryptography	i) vulnerable to side-channel attacks and ii) high computation and communication costs.

3. BACKGROUND

3.1. Proposed objectives

Research in this area aims to provide a system to improve authentication with privacy-preserving strategies in a 5G-enabled vehicle network. The following are some of the sub-goals that will help bring this overall objective closer to fruition:

- To propose a scheme with the aim of satisfying security and privacy requirements.
- To design a scheme for resisting common security attacks.
- To improve the efficiency performance for signing and verifying messages.
- To evaluate the efficiency of the proposal with regard to its message signing, single verification, batch verification, and communication costs.
- To compare with exiting schemes in terms of performance evaluating and security requirements.

3.2. Achieved work

According to the related work section, several of the recent existing schemes have to suffer limitations, as a result, are not suitable to deploy in the vehicular network. To address the security and privacy issues, a sophisticated privacy-preserving authentication scheme should be proposed and deployed. The following several limitation points are:

- Security issues: the authentication, integrity, and revocation needs of the vehicle network leave various existing systems open to attack.
- Privacy issues: many currently-available techniques fall short of what is needed to guarantee unlinkability.
- Security attacks: there are already a number of techniques, but many of them are vulnerable to attacks including replay, modification, impersonation, and side-channel.
- Consuming operation: several already-in-use systems have prohibitively high computational and communication overhead.

3.3. Research problem

The overarching goal of this investigation is to develop better conditional privacy-preserving authentication systems for 5G-enabled automotive networks. The following are some instances of the problem:

- The existing schemes are failed to satisfy the quite requirements concerning security and privacy
- The existing schemes are vulnerable to common security attacks such as man-in-the-middle, replay, modification, and impersonation attacks.
- The existing schemes have large performance overheads in terms of computation and communication costs.

3.4. Elliptic curve cryptography

Miller [42] first introduced elliptic curve cryptography (ECC) in 1985, and it has since become a popular technique for creating digital signatures and security algorithms. It assumes that F_p represents a finite field of non-singular elliptic curve E based prime number order p . It also assumes that a group of points on E over F_p utilises (1) with the discriminant $\Theta = 4a^3 + 27b^2 \neq 0$.

$$y^2 \equiv x^3 + ax + b \quad (1)$$

where $a, b \in F_p$. It also assumes an infinity on E based point O . Therefore, O and other points (such as K , R , and D) on E build up a group G of cyclic additive with a generator P and an order q , where q is a large prime number.

4. DESIGN OF THE PROPOSED ES-APP SCHEME

4.1. Privacy and security requirements

In this section, we briefly show that our proposed efficient and secure authentication with a privacy-preserving (ES-APP) method satisfies the following privacy and security requirements for secure communication in a 5G-enabled vehicle network. Identity privacy-preservation: vehicles that form VANETs must do so incognito. Specifically, no other vehicle or RSU should be able to determine the identify of the sender vehicle by analyzing the received messages. Unlinkability: two or more malicious messages from the same vehicle shouldn't be able to be cross-matched. Message authentication and integrity: any data must have been transmitted by an authentic node, and a verify process node must be able to ensure this and rule out any tampering. Traceability: only the TA is authorised to establish the true identification of a vehicle in the event of a false message transmission. Revocation: only the TA has the authority to revoke the original identification of the vehicle in the event of a false message transmission. Model attacks: the potential attacks are vulnerable to break communication among vehicles. Thus, the proposed ES-APP scheme will resist them. The description of these attacks are as: forgery attacks, modify attacks, replay attacks, man-in-the-middle attacks, and side-channel attacks. Note that these attacks try to damage the communication among vehicles by impersonating (forgery the real identity) and modify (modification of messages) which precise the these attacks targeting the authentication schemes.

4.2. Proposal phases

Here, we lay out the steps of the proposed an ES-APP method, which aims to reduce the system's overhead while still meeting security and privacy criteria. Initialization, vehicle registration, parameter renewal,

message signing, single verification, and batch verification are the six stages that make up the proposed ES-APP method, as shown in Figure 1. Table 2 lists the symbol used and their explanation in this paper. These stages are discussed in length.

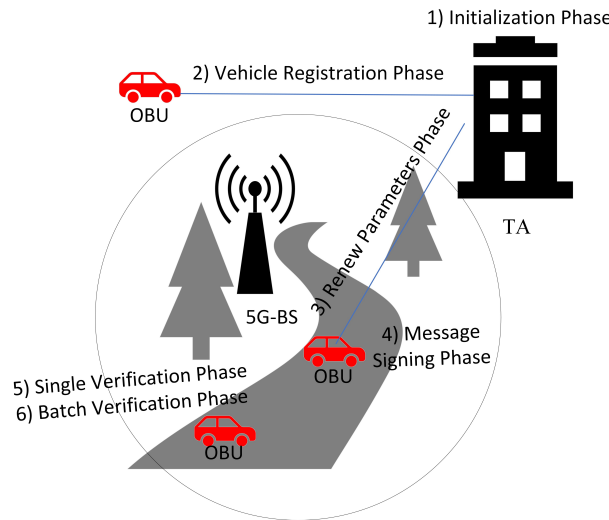


Figure 1. Phases of proposed ES-APP scheme

Table 2. Symbol used and their explanations

Symbol	Explanations
G	An additive group of rank q
P	Generator
p and q	Two huge prime values
E	Elliptic curve
h_1	Cryptographic hash function
$ENC(\cdot)/DEC(\cdot)$	Encryption and decryption function symmetric
$s \in Z_q$	Private key
r	Random number integer
$LPIDv$	pseudonym-IDs
$Pub = s.P$	public key
ps	The pseudonym
TS	timestamp

4.2.1. Initialization phase

In this phase, TA is responsible for creating security parameters based on elliptic curve, encryption/decryption and hash functions.

- An additive group G of rank q and generator P is chosen by the TA, along with two huge prime values p and q . All points on the elliptic curve E with a definition in terms of $y^2 = x^3 + ax + b \text{ mod } p$, where $a, b \in F_p$, belong to the additive group G .
- The private key is a randomly generated number $s \in Z_q$, and the public key is calculated as $Pub = s.P$ by the TA.
- The TA chooses the cryptographic hash function h_1 and encryption and decryption $ENC(\cdot)/DEC(\cdot)$ function symmetric.
- TA sets the system parameters $\{Pub, h_1, p, q, G, ENC(\cdot), DEC(\cdot), a, b\}$ as a public parameters.

4.2.2. Vehicle registration phase

In this phase, vehicle should be registered with TA before leaving factories. Before preloading the public parameters, TA computes a list of pseudonym-IDs and relevant signature keys according to a short valid period. These parameters will preloads to OBU's vehicle.

- In this step, the user provides the TA with their authentic identity (using their RID_v and password PW) over a secure connection to begin the procedure. TA saves personal identification into vehicle registration list.
- The TA computes the pseudonym $ps = h_1(RID_v || s || d)$ to protect and renew RID_v , where d is random number. The TA saves d and RID_v into registration list of vehicle for renew parameters phase.
- TA computes and preloads list of pseudonym-IDs and relevant signature keys to OBU as: the list of pseudonym-IDs are $LPID_v = \{LPID_{vi}^1, LPID_{vi}^2\} = \{PID_{vi}^1 = r.P, PID_{vi}^2 = ps \oplus h_1(r.Pub)\}$. The relevant signature keys are $LSk_i = s.h_1(TS || PID_{vi}^1 || PID_{vi}^2)$. Where TS is a timestamp and r is a random number integer.
- TA submits and saves the system parameter and list of pseudonym-IDs and relevant signature keys to OBU in order to generate signatures and verify messages.

4.2.3. Renew parameters phase

When the timer is about to run out, the car sends a request to TA to have its parameters renewed. After verifying the request and time stamp, TA generates a new pseudonym and lists of pseudonym IDs and related signature keys with a new, brief valid duration. TA uses an elliptic curve to generate symmetric key sharing between TA and vehicles to encrypt the lists. Once receiving new lists, the vehicle uses parameters to generate symmetric key sharing between TA and vehicles in order to decrypt the lists and check the validity of these parameters. The side-channel attack has been resisted in this phase by renewing new parameters before revealing them.

- Vehicle sends request renew parameters to TA through 5G-BS node. By using one of the pseudonym-ID such as PID_{vi}^1 and PID_{vi}^2 , the TA reveals the old real identity with using its master key and then computes new list of pseudonym-IDs.
- Vehicle computes $\sigma_{req} = h_1(PID_{vi}^1 || PID_{vi}^2 || T_1)$ of request and sends tuple $\{PID_{vi}^1, PID_{vi}^2, T_1, \sigma_{req}\}$ to TA through 5G-BS.
- The TA checks freshness of the timestamp T_1 by using the following process. As a preliminary step, it verifies that timestamp T_1 is legitimate. The following is checked for every time stamp T : Let's pretend T_r is the time of reception and T is the time lag. T holds if and only if $(T < T_r - T)$. When that doesn't happen, the message is deleted. Assuming T_1 is true, the next step is proceed.
- The TA checks the signature $\sigma_{req}^- = \sigma_{req} = h_1(PID_{vi}^1 || PID_{vi}^2 || T_1)$ for avoiding any modification through third party. Meanwhile, TA reveals and checks $ps = PID_{vi}^2 \oplus h_1(s.PID_{vi}^1)$ saved its registration lists. Then matching with RID_v .
- Once the TA issues the new pseudonym $ps_{new} = h_1(RID_v || s || d_{new})$, the TA computes and preloads new list of pseudonym-IDs and relevant signature keys to OBU as follows. The list of pseudonym-IDs are $LPID_v^{new} = \{LPID_{vi}^1, LPID_{vi}^2\} = \{PID_{vi}^1 = r_{new}.P, PID_{vi}^2 = ps_{new} \oplus h_1(r_{new}.Pub)\}$. The relevant signature keys are $LSk_i = s.h_1(PID_{vi}^1 || PID_{vi}^2)$. Where d_{new} and r_{new} are a random number integer.
- The TA encrypts a new $LPID_v^{new}$ and LSk_i by using elliptic curve parameters as shared symmetric key. Then these parameters are decrypted through vehicle for using in the next steps.

4.2.4. Message signing phase

In this phase, the vehicle selects randomly unused pseudonym-ID and corresponding signature keys from a list sent from TA in advance. Before broadcasting the message, the vehicle signs the message with these parameters. This phase doesn't use a scalar multiplication operation based on an elliptic curve, therefore, an this multiplication operation is used instead. Additionally, a signed vehicle computes a single multiplication operation to support the verifier. Meanwhile, to avoid replay attacks, the proposed ES-APP scheme uses the current timestamp for each signing message. Finally, the vehicle broadcasts message-signature-tuple including signature, timestamp, and pseudonym-IDs.

- The vehicle randomly selects PID_{vi}^1, PID_{vi}^2 and signature LSk_i from list saved in OBU.
- The vehicle signs the signature-based message $\sigma_{Msg} = LSk_i.h_1(M || PID_{vi}^1 || PID_{vi}^2 || T_i)$, where T_i is timestamp and m is message exchanged.
- The vehicle broadcasts tuple-based message $\{M, PID_{vi}^1, PID_{vi}^2, T_i, \sigma_{Msg}\}$ to other vehicles.

4.2.5. Single verification phase

Another vehicle v_j receives a message-signature-tuple that is exchanged by the vehicle in order to accept it. Before the data is accepted, the vehicle should be checked for authenticity and validity of the message with a freshness timestamp. In the proposed ES-APP scheme, the public key of the system is used to verify the signature and to prove the message doesn't have to change via a third party. Thus, the proposed scheme will resist security attacks.

- Once the verifying vehicle v_j received tuple-based message $\{M, PID_{vi}^1, PID_{vi}^2, T_i, \sigma_{M_{sg}}\}$, the received timestamp T_i firstly checked in term of freshness.
- The verifier performs the following checks to ensure the message's validity and authenticity when using a signature.

$$\sigma_{M_{sg}}.P = ? h_1(PID_{vi}^1 || PID_{vi}^2).h_1(M || PID_{vi}^1 || PID_{vi}^2 || T_i)Pub \tag{2}$$

4.2.6. Batch verification phase

The proposed method is compatible with batch verification. The verifier vehicle v_j examines all signatures simultaneously using the system's public key once it has received numerous message-signature-tuples from multiple vehicles. At this step, the proposals also protect against replay attacks by ensuring timestamps are up-to-date. All of these criteria are validated by the verifier using the public key. The vehicle checks (3). Note that these above phases are briefly introduced in Figure 2.

$$\sum_{i=1}^n \sigma_{M_{sg}}.P = ? \sum_{i=1}^n h_1(PID_{vi}^1 || PID_{vi}^2).h_1(M || PID_{vi}^1 || PID_{vi}^2 || T_i)Pub \tag{3}$$

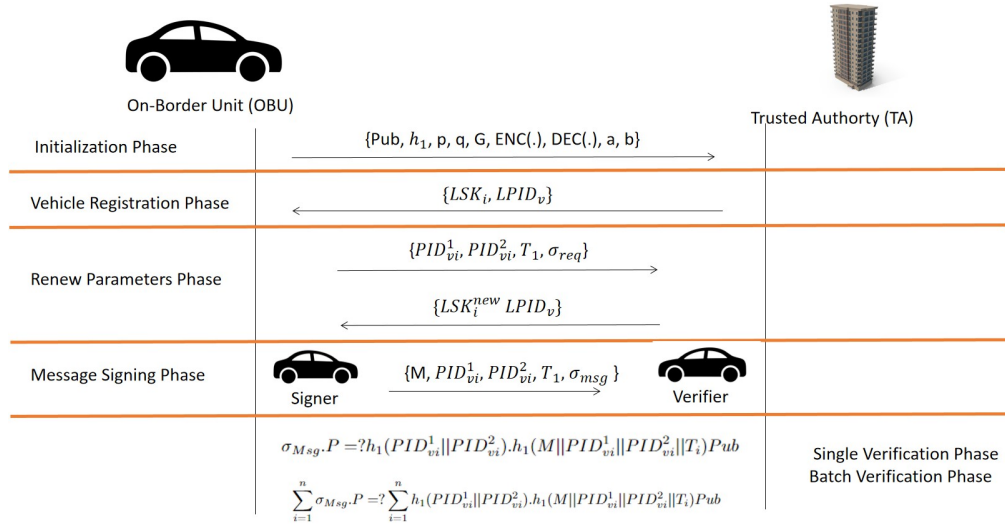


Figure 2. Phases of proposed ES-APP scheme

5. RESULT

Here, we assess the effectiveness of the proposed ES-APP system and compare it to previous works by [39]–[41]. In order to determine how long certain cryptographic procedures take, this work makes use of the MIRACL cryptographic library [43]. The processor is a 1.80 GHz Intel(R) Core(TM) i7-8550u with 8 GB of RAM and Windows 10 as the operating system.

5.1. Computation costs

Timing requirements for cryptographic procedures are as: $T_{bp} = 5.811$ ms stands for the time it takes to do a bilinear pairing procedure. In G_1 , $T_{sm}^{bp} = 1.5654$ ms represents the time required to execute the scalar multiplication operation with respect to the bilinear pairing. Time required to execute the point addition on the bilinear pairing in G_1 is denoted by $T_{pa}^{bp} = 0.0106$. Specifically, $T_{mtp} = 4.1724$ ms is the amount of

cost it takes to run the map-to-point function on the bilinear pairing in G_1 . The cost required to do scalar multiplication about the ECC in an additive group G is denoted by $T_{sm}^{ecc} = 0.6718$ ms. The time required to execute the point-addition operation about the ECC in an additive group G is denoted by $T_{pa}^{ecc} = 0.0031$ ms. Secure hash cryptography has a time cost of $T_h = 0.001$ ms seconds per function call. Figure 3 summarizes the computation costs of the proposal and other schemes.

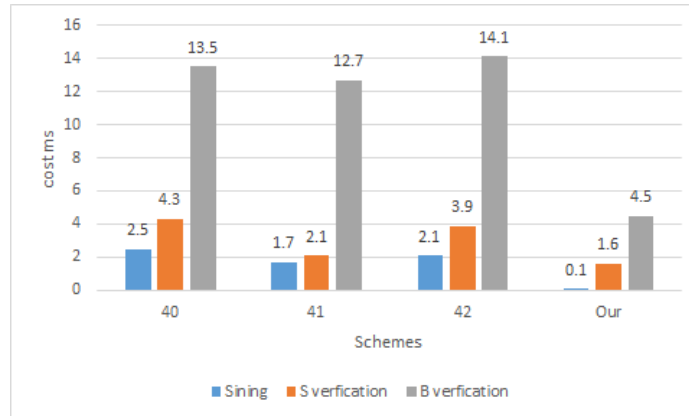


Figure 3. Analysis of computation costs

5.2. Communication costs

The communication cost of the proposed ES-APP and other schemes is compared and analyzed here. The key concern is the amount of data transferred for the signature tuple, which includes pseudonym-IDs, signatures, and timestamps. If each item in G_1 is 128 bytes in size, then pis 64 bytes in size. Given that p is 20 bytes in length, we may deduce that each item in G takes up 40 bytes. When the message's contents are not included, we assume that the output sizes of the timestamp, the secure hash function, and the item in the integer group Z_q are 4, 20, and 20 bytes, respectively. Figure 4 summarizes communication costs for our proposal and others.

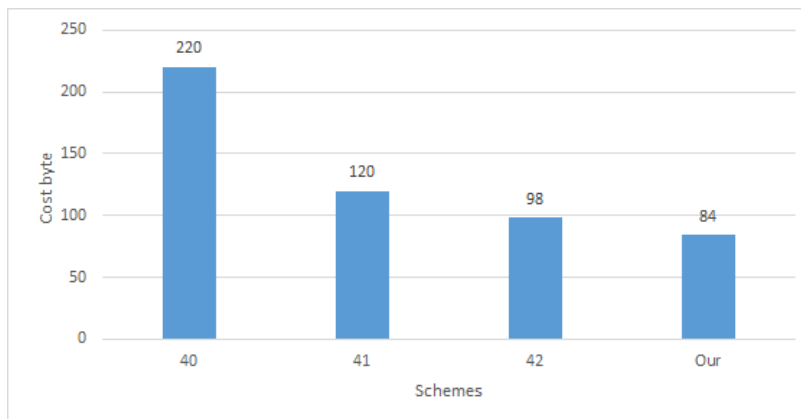


Figure 4. Comparing the expenses of different methods of communicating

5.3. Security comparison

In this part, we describe the expected result of the ES-APP proposal. The proposed ES-APP scheme will be compared to current ID-based security and privacy schemes in terms of security (messaging integrity and authentication, traceability, and revocation), privacy (privacy-preserving and unlinkability), attack-resistance (resistance to forgery, modification, replay, man-in-the-middle attacks, and side-channel attacks), and performance evaluation (computational cost and communicative overhead). Comparing the proposed ES-APP scheme to current ID-based schemes with regard to security and privacy is presented in Table 3.

Table 3. A review of hybrid-based security mechanisms

	[39]	[40]	[41]	ES-APP
Security requirements	Yes	Yes	Yes	Yes
Privacy requirements	Yes	Yes	Yes	Yes
Resistant to replay attacks	Yes	Yes	Yes	Yes
Resistant to forgery attacks	Yes	Yes	Yes	Yes
Resistant to modify attacks	Yes	Yes	Yes	Yes
Resistant to MITM attacks	Yes	Yes	Yes	Yes
Resistant to side-channel attacks	No	No	No	Yes
Performance evaluation	High	Medium	Medium	Low

As shown in Table 3, the ES-APP scheme proposes renewing the parameter phase to renew pseudonym-ID, and lists in order to avoid side-channel attacks from revealing the real identity and used to disrupt the system. Unlike the other work, they never renew the original identity of the vehicle, which cause a side-channel attack to occur. Meanwhile, since signers just select pseudonym IDs and relevant signature keys from lists, there are no extra computation costs for the signer side. Since the proposed uses a less operations-based elliptic curve, the communication costs are very low compared with others.

6. CONCLUSION




Open access channels used by 5G-enabled vehicle networks create a number of security and privacy concerns. To safeguard V2X communication in a 5G network, this work presents an ES-APP mechanism. The proposed ES-APP has two primary goals: i) to protect against attacks on model security and ii) to accommodate needs for confidentiality and safety in a mobile network. In the proposed list-based mechanism, the messages are checked by a public system. In addition to traditional ID-based techniques, the ES-APP also makes use of the elliptical curve parameter. The proposed ES-APP lessens computational and transmission overheads by serially signing and certifying the message while broadcasting. Implementing the proposed security and privacy plan, future research will compare and contrast the proposed ES-computation APP's and communication model's performance parameters to those of existing ID-based systems.

REFERENCES




- [1] M. A. Hamdan, A. M. Maklouf, and H. Mnif, "Review of Authentication with Privacy-preserving Schemes for 5G-enabled Vehicular Networks," *2022 15th International Conference on Security of Information and Networks*, pp. 1-6, 2022, doi: 10.1109/SIN56466.2022.9970554.
- [2] H. Su, S. Dong, N. Wang, and T. Zhang, "An efficient privacy-preserving authentication scheme that mitigates ta dependency in vanets," *Vehicular Communications*, vol. 45, 2024, doi: 10.1016/j.vehcom.2024.100727.
- [3] M. S. AlMarshoud, A. H. Al-Bayatti, and M. S. Kiraz, "Security, privacy, and decentralized trust management in vanets: A review of current research and future directions," *ACM Computing Surveys*, 2024, doi: 10.1145/3656166.
- [4] X. Cheng, R. Zhang, and L. Yang, "Wireless toward the era of intelligent vehicles," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 188–202, 2019, doi: 10.1109/JIOT.2018.2884200.
- [5] G. Adele, A. Borah, A. Paranjothi and M. S. Khan, "A Survey and Comparative Analysis of Methods for Countering Sybil Attacks in VANETs," *2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2024, pp. 0178-0183, doi: 10.1109/CCWC60891.2024.10427979.
- [6] M. A. Al-Shareeda and S. Manickam, "MSR-DoS: Modular Square Root-Based Scheme to Resist Denial of Service (DoS) Attacks in 5G-Enabled Vehicular Networks," in *IEEE Access*, vol. 10, pp. 120606-120615, 2022, doi: 10.1109/ACCESS.2022.3222488
- [7] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in vanets," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3235–3248, 2017, doi: 10.1109/TVT.2015.2406877.
- [8] M. Prakash and K. Saranya, "Vanet authentication with privacy-preserving schemes—a survey," in *Proceedings of Fourth International Conference on Communication, Computing and Electronics Systems: ICCCES 2022*, Springer, 2023, pp. 465–480, doi: 10.1007/978-981-19-7753-4_36.
- [9] C. Lai, R. Lu, D. Zheng, and X. Shen, "Security and privacy challenges in 5g-enabled vehicular networks," *IEEE Network*, vol. 34, no. 2, pp. 37–45, 2020, doi: 10.1109/MNET.001.1900220.
- [10] H. J. Nath and H. Choudhury, "Privacy-preserving authentication protocols in vanet: A review," *Authorea Preprints*, pp. 1-41, 2023.
- [11] Z. Qiao et al., "An Anonymous and Efficient Certificate-Based Identity Authentication Protocol for VANET," in *IEEE Internet of Things Journal*, vol. 11, no. 7, pp. 11232-11245, 2024, doi: 10.1109/JIOT.2023.3330580.
- [12] C. B. Tan, M. H. A. Hijazi, and P. N. E. Nohuddin, "A comparison of different support vector machine kernels for artificial speech detection," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 21, no. 1, pp. 97–103, 2023, doi: 10.12928/telkomnika.v21i1.24259.
- [13] A. Balaram, P. Chandana, S. A. Nabi, and M. SilpaRaj, "A survey of vanet routing attacks and defense mechanisms in intelligent transportation system," *Self-Powered Cyber Physical Systems*, pp. 213–226, 2023, do: 10.1002/9781119842026.ch10.

- [14] V. Goel, M. Aggarwal, A. K. Gupta, and N. Kumar, "A blockchain-based aadhar system: distributed authentication system," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 20, no. 6, pp. 1239–1247, 2022, doi: 10.12928/telkomnika.v20i6.24231.
- [15] C. Lai, M. Zhang, J. Cao, and D. Zheng, "Spir: A secure and privacy-preserving incentive scheme for reliable real-time map updates," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 416–428, 2020, doi: 10.1109/JIOT.2019.2953188.
- [16] S. A. Jan, N. U. Amin, M. Othman, M. Ali, A. I. Umar, and A. Basir, "A Survey on Privacy-Preserving Authentication Schemes in VANETs: Attacks, Challenges and Open Issues," in *IEEE Access*, vol. 9, pp. 153701–153726, 2021, doi: 10.1109/ACCESS.2021.3125521.
- [17] A. Yang, J. Weng, N. Cheng, J. Ni, X. Lin, and X. Shen, "Deqos attack: Degrading quality of service in vanets and its mitigation," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 4834–4845, 2019, doi: 10.1109/TVT.2019.2905522.
- [18] J. Cheng, G. Yuan, M. Zhou, S. Gao, C. Liu, and H. Duan, "A fluid mechanics-based data flow model to estimate vanet capacity," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 6, pp. 2603–2614, 2020, doi: 10.1109/TITS.2019.2921074.
- [19] F. Azam, S. K. Yadav, N. Priyadarshi, S. Padmanaban, and R. C. Bansal, "A Comprehensive Review of Authentication Schemes in Vehicular Ad-Hoc Network," in *IEEE Access*, vol. 9, pp. 31309–31321, 2021, doi: 10.1109/ACCESS.2021.3060046.
- [20] X. Cheng, R. Zhang, S. Chen, J. Li, L. Yang, and H. Zhang, "5G enabled vehicular communications and networking," in *China Communications*, vol. 15, no. 7, pp. iii–vi, 2018, doi: 10.1109/CC.2018.8424577.
- [21] P. Mundhe, S. Verma, and S. Venkatesan, "A comprehensive survey on authentication and privacy-preserving schemes in vanets," *Computer Science Review*, vol. 41, p. 100411, 2021, doi: 10.1016/j.cosrev.2021.100411.
- [22] J. Polpong and P. Wuttidittachotti, "Authentication and password storing improvement using sxr algorithm with a hash function," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 6, pp. 6582–6591, 2020, doi: 10.11591/ijece.v10i6.pp6582-6591.
- [23] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, "Unmanned aerial vehicle: a review and future directions," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 30, no. 2, pp. 778–786, 2023, doi: 10.11591/ijeecs.v30.i2.pp778-786.
- [24] K. S. V. Prasad, E. Hossain, and V. K. Bhargava, "Energy efficiency in massive mimo-based 5g networks: Opportunities and challenges," *IEEE Wireless Communications*, vol. 24, no. 3, pp. 86–94, 2017, doi: 10.1109/MWC.2016.1500374WC.
- [25] A. K. Goyal, G. Agarwal, A. K. Tripathi, and G. Sharma, "Systematic study of vanet: Applications, challenges, threats, attacks, schemes and issues in research," *Green Computing in Network Security*, pp. 33–52, 2022.
- [26] A. A. Jabbar and W. S. Bhaya, "Secure private cloud using machine learning and cryptography," in *AIP Conference Proceedings*, vol. 2547, no. 1, 2022, p. 060002, 2022, doi: 10.1063/5.0112135.
- [27] B. A. Mohammed *et al.*, "FC-PA: fog computing-based pseudonym authentication scheme in 5G-enabled vehicular networks," *IEEE Access*, vol. 11, pp. 18571–18581, 2023, doi: 10.1109/ACCESS.2023.3247222.
- [28] G. Kumar, M. Lydia, and Y. Levron, "Security challenges in 5g and iot networks: A review," *Secure Communication for 5G and IoT Networks*, pp. 1–13, 2022, doi: 10.1007/978-3-030-79766-9_1.
- [29] H. A. Abdulmalik and A. A. Yassin, "Secure two-factor mutual authentication scheme using shared image in medical health-care environment," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 12, no. 4, pp. 2474–2483, 2023, doi: 10.11591/eei.v12i4.4459.
- [30] P. Cincilla, O. Hicham, and B. Charles, "Vehicular PKI scalability-consistency trade-offs in large scale distributed scenarios," in *2016 IEEE Vehicular Networking Conference*, pp. 1–8, 2016, doi: 10.1109/VNC.2016.7835970.
- [31] A. Joshi, P. Gaonkar, and J. Bapat, "A reliable and secure approach for efficient car-to-car communication in intelligent transportation systems," in *2017 International Conference on Wireless Communications, Signal Processing and Networking*, pp. 1617–1620, 2017, doi: 10.1109/WiSPNET.2017.8300034.
- [32] M. Asghar, R. R. M. Doss, and L. Pan, "A scalable and efficient pki based authentication protocol for vanets," in *2018 28th International Telecommunication Networks and Applications Conference*, pp. 1–3, 2018, doi: 10.1109/ATNAC.2018.8615224.
- [33] D. Tiwari, M. Bhushan, A. Yadav, and S. Jain, "A novel secure authentication scheme for vanets," in *2016 Second International Conference on Computational Intelligence and Communication Technology*, pp. 287–297, 2016, doi: 10.1109/CICT.2016.64.
- [34] K. Lim, K. M. Tuladhar, X. Wang, and W. Liu, "A scalable and secure key distribution scheme for group signature based authentication in vanet," in *2017 IEEE 8th annual ubiquitous computing, electronics and mobile communication conference*, pp. 478–483, 2017, doi: 10.1109/UEMCON.2017.8249091.
- [35] A. Alazzawi, H. Lu, A. A. Yassin, and K. Chen, "Efficient conditional anonymity with message integrity and authentication in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 71 424–71 435, 2019, doi: 10.1109/ACCESS.2019.2919973.
- [36] J. Cui, J. Chen, H. Zhong, J. Zhang, and L. Liu, "Reliable and efficient content sharing for 5g-enabled vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 2, pp. 1247–1259, 2022, doi: 10.1109/TITS.2020.3023797.
- [37] M. Bayat, M. Pournaghi, M. Rahimi, and M. Barmshoory, "NERA: A new and efficient rsu based authentication scheme for vanets," *Wireless networks*, vol. 26, no. 5, pp. 3083–3098, 2020, doi: 10.1007/s11276-019-02039-x.
- [38] J. Cui, W. Xu, Y. Han, J. Zhang, and H. Zhong, "Secure mutual authentication with privacy preservation in vehicular ad hoc networks," *Vehicular Communications*, vol. 21, p. 100200, 2020, doi: 10.1016/j.vehcom.2019.100200.
- [39] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "SE-CPPA: A secure and efficient conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *Sensors*, vol. 21, no. 24, p. 8206, 2021, doi: 10.3390/s21248206.
- [40] J. S. Alshudukhi, Z. G. Al-Mekhlafi, and B. A. Mohammed, "A lightweight authentication with privacy-preserving scheme for vehicular ad hoc networks based on elliptic curve cryptography," *IEEE Access*, vol. 9, pp. 15633–15642, 2021, doi: 10.1109/ACCESS.2021.3053043.
- [41] M. A. Al-Shareeda *et al.*, "Provably secure with efficient data sharing scheme for fifth-generation (5G)-enabled vehicular networks without road-side unit (RSU)," *Sustainability*, vol. 14, no. 16, p. 9961, 2022, doi: 10.3390/su14169961.
- [42] V. S. Miller, "Use of elliptic curves in cryptography," in *Conference on the theory and application of cryptographic techniques*, pp. 417–426, 1985, doi: 10.1007/3-540-39799-X_31.
- [43] M. Scott, "MIRACL-A multiprecision integer and rational arithmetic C/C++ library," *Shamus Software Ltd*, 2003.




BIOGRAPHIES OF AUTHORS

Mays A. Hamdan    received her bachelor's degree from Diyala University, Iraq in 2013 and Master's degree from Modern University for Business and Sciences, Lebanon in 2020 and is currently studying for her Ph.D. degree in National School of Electronics and Telecommunications of Sfax, University of Sfax. Her research interests include security and privacy issues in VANETs. She can be contacted at email: maysmubs@gmail.com.



Amel Meddeb Makhoulf    received the Ph.D. degree from SUP'COM, Tunisia, in 2010, and the Habilitation degree, in December 2020. From 2001 to 2004, she worked as the Chief of the Certification Unit, NDCA. Since September 2010, she has been working as an Assistant Professor at ENET'COM, Sfax, Tunisia. Since 2020, she has been the Head of the Department of Telecommunication. She was a supervisor of more than 30 master's projects and 14 Ph.D. She coauthored more than 40 papers, published in international journals and refereed conferences. Her research interests include security of vehicular networks, cloud networks, and BSN. She can be contacted at email: amel.makhoulf@enetcom.usf.tn.



Hassene Mnif    was born in Sfax, Tunisia, in 1975. He received the Engineer and Master Diplomas in electrical engineering from the University of Sfax (ENIS) in 1999 and 2000, respectively, the Ph.D. degree in Electronics from the University of Bordeaux I, France, in 2004 and the HDR degree from the University of Sfax in 2011. He is currently full Professor and the President of the Ph.D Committee in the National School of Electronics and Telecommunications of Sfax, University of Sfax. He was the Director of this school between 2014 and 2020, where he has multiple innovative engineering education initiatives. He is a member of the Electronic and Information Technology Laboratory. His research interests include energy harvesting, design of radio-frequency integrated circuits, characterization, and compact modeling of both high frequency devices and future emerging technologies like carbon nanotube field effect transistor (CNTFET). He also participates in research for real time image and video text extraction and micro mobility systems. He has authored and co-authored about 90 journal publications and conference papers and has gathered significant scientific coordination experience within national and international collaborative research projects. He participated in the organization of several IEEE conferences and workshops, in particular ICECS 2009 and MELECON 2012. He served as the Tunisia Section Treasurer Between 2011 and 2013, he is actually the IEEE Tunisia Section Chair-Elect. He can be contacted at email: hassene.mnif@ieee.org.