applied sciences

MDPI

Article

Password-Guessing Attack-Aware Authentication Scheme Based on Chinese Remainder Theorem for 5G-Enabled Vehicular Networks

Mahmood A. Al-Shareeda, Mohammed Anbar *, Selvakumar Manickam and Iznan H. Hasbullah

National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Gelugor 11800, Penang, Malaysia; m.alshareeda@nav6.usm.my (M.A.A.-S.); selva@usm.my (S.M.); iznan@nav6.usm.my (I.H.H.)

* Correspondence: anbar@nav6.usm.my; Tel.: +60-4-653-4633

Abstract: The new fifth-generation (5G) cellular networks dramatically improve the speed of message transmissions. Most existing authentication schemes that secure 5G communication rely heavily on the vehicle's tamper-proof device (TPD) and roadside units (RSUs) to store the system's master key. However, it only takes a single compromised TPD to render the whole system insecure. We propose a password-guessing attack-aware authentication scheme based on the Chinese Remainder Theorem (CRT) to secure inter-vehicle communication on 5G-enabled vehicular networks to address this issue. The trusted authorities (TAs) in the proposed scheme generate and broadcast new group keys to the vehicles assisted by CRT. Moreover, since the system's master key does not need to be preloaded, the proposed scheme only requires realistic TPDs. The proposed scheme overcomes password-guessing attacks and guarantees top-level security for entire 5G-enabled vehicular networks. The security analysis indicates that the proposed scheme is secure against adaptive chosen-message attacks under the random oracle model and meets the security requirements of a 5G-enabled vehicular network. Since cryptographic operations based on elliptic curve cryptography are employed, the performance evaluation shows that the proposed scheme outperforms the eight existing schemes in terms of computation and communication costs.

Keywords: fifth-generation (5G) cellular networks; 5G-enabled vehicular networks; Chinese remainder theorem (CRT); password-guessing attacks; tamper-proof device (TPD)

Citation: Al-shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. Password-Guessing Attack-Aware Authentication Scheme Based on Chinese Remainder Theorem for 5G-Enabled Vehicular Networks. *Appl. Sci.* **2022**, *12*, 1383. https://doi.org/10.3390/app12031383

Academic Editor: Liang-Bi Chen

Received: 18 December 2021
Accepted: 24 January 2022
Published: 27 January 2022

1. Introduction

Road accidents cause approximately 1.3 million fatalities and 20 to 50 million injuries globally [1]. Hence, the principal aim of intelligent transportation systems (ITSs) is to reduce the number of road accidents by offering transportation safety. One of the fundamental components of an ITS is to provide vehicular networks that connect vehicles, pedestrians, roadside devices, drivers, and passengers [1,2].

The latest trend in the advent of wireless communication technologies is the application and development of fifth-generation (5G) cellular networks spurred by massive government investment in many regions [3–5]. A 5G network obtains a multiple-fold increase in speed compared with current fourth-generation (4G) networks due to the characteristic of 5G, increasing the mobile data per unit area by 1000 times and the transmission rate to up to 10 Gbps. Furthermore, 5G achieves a five times latency reduction and extends the battery life of devices tenfold, which opens up enormous possibilities for mobile ad hoc networks (MANET), especially for the Internet of vehicles (IOVs). For example, one type of vehicular ad hoc network (VANET) distribution relies on IOVs for inter-vehicle communication to share information with others through their on-board unit (OBU) in a wireless network environment. Vehicles can realize many types of infotainment and safety-related services by making use of the shared information [6].

VANET typically coexists with other networks, such as satellite, 2G/3G cellular, and long-term evolution (LTE). However, in VANET communications, these networks utilize

different protocols and standards, which could lead to disjointed information interaction and inefficient data processing. For example, the literature [7,8] has demonstrated that IEEE 802.11p and LTE standards do not effectively support latency and scalability for vehicular communications. Moreover, roadside units (RSUs) are usually required in these networks to participate in the authentication process, which increases the system's latency. Furthermore, a study [9] has shown that a compromised RSU leads to leakage of sensitive data stored in the RSU. Therefore, rendering the whole system exposed and insecure. Nevertheless, the advantages provided by the 5G mobile wireless system, such as wide-area coverage, high speed, and low latency, can make inter-vehicle communication in VANET more effective in terms of performance and cost.

These 5G mobile wireless systems have a double-layer network: a macro and a device layer. The macro layer is responsible for the communication between terminal devices and the base station. On the other hand, the device layer, device-to-device (D2D) communication, is the crucial component of these 5G wireless systems, which realizes direct communication between terminal devices without involving or requiring additional infrastructure [10,11]. Compared with the VANET architecture, 5G-enabled vehicular networks have longer communication ranges and can connect with more vehicles per base station. To the best of the authors' knowledge, this is the first password-guessing attack authentication scheme based on the Chinese remainder theorem (CRT) for 5G-enabled vehicular networks. To be specific, three primary contributions of the paper are summarized as follows.

- First, a new authentication scheme based on CRT for 5G-enabled vehicular networks, which require neither RSU nor tamper-proof device (TPD);
- Second, a significant reduction in the computational complexity imposed on the trusted authorities (TAs) since vehicles joining or leaving a multicast domain execute one modulo division operation using CRT in the proposed scheme;
- Third, an authentication scheme that withstands password guess attacks, in which the driver holds two secret authentication parameters, preventing illegal users from taking control of a registered participating vehicle.

The rest of the paper is structured as follows: Section 2 discusses the latest related work. Section 3 presents the preliminaries. Section 4 describes the proposed scheme for 5G-enabled vehicular networks, followed by its security analysis in Section 5. The performance evaluation and comparison are in Section 6. Finally, Section 7 concludes this paper.

2. Related Work

Authentication plays a significant role in securing inter-vehicle communication in vehicular networks. The related work can be categorized into five distinct groups as follows.

2.1. PKI-Based

The first group comprises existing authentication schemes that rely on the public key infrastructure (PKI) approach [12–20] to ensure message authentication and integrity. However, to satisfy privacy, each vehicle in the network requires a massive pool of certificates and their matching private–public key pairs to prevent adversaries from linking multiple messages to the same sender.

Moreover, the TA suffers from the burden of storing the certificates since the certificates, and their matching private–public key pairs must be kept for all registered vehicles. In addition, certificate verification is an involved process, which adds extra computational cost on the verifier's side.

2.2. GS-Based

To address the weaknesses of PKI-based authentication schemes, the second group utilized a group signature (GS) approach [21–24]. However, compared with traditional signature schemes, this approach suffers higher verification costs due to the member revocation problem. Furthermore, when the group size is small, the adversary can identify group members, rendering the system insecure.

2.3. ID-Based BP

The third group comprises schemes that utilize an identity (ID) approach based on a bilinear pair (BP) to overcome the member revocation problem of GS-based approaches [25–30]. This approach supports a batch verification process to verify multiple messages simultaneously. However, the operations of bilinear pairs in this approach are time-consuming and complex, which introduce huge system overheads in signing and verifying messages.

2.4. ID-Based ECC

Existing schemes in the fourth group aim to minimize the system costs of the ID-based BP approach by utilizing an identity (ID) approach based on elliptic curve cryptography (ECC) [31–37], which are more efficient.

The ID-based ECC and ID-based BP schemes need participating RSUs for the authentication process. Some schemes in this group store the system's master key in the TPD of RSU. Nevertheless, the limitations of RSU utilization are as follows: (i) a single compromised RSU is enough to render the whole system insecure; (ii) RSU are expensive; and (iii) some existing schemes add a TPD to both OBU and the RSU, making the system even more costly.

2.5. 5G-Enabled Vehicular Networks

The final group comprises 5G-enabled vehicular networks without involving any RSU in the authentication process [38,39] to satisfy the security and privacy requirements. In the scheme proposed by [38], a TA preloads the system's master key in the TPD of OBU for legitimate users. The main issue of this scheme is that, once the system's master key of any TPD is compromised, the whole system is exposed and insecure. In contrast, the scheme proposed by Cui et al. [39] uses several scalar multiplication operations associated with ECC to verify a massive number of messages in a short period.

We propose a password-guessing attack-aware authentication scheme based on CRT to secure inter-vehicle communication for 5G-enabled vehicular networks to overcome the issues that plague the above-stated schemes. In the proposed scheme, TA utilizes CRT to compute domain keys for vehicles in its domain. As a result, both pseudonym ID and domain keys are updated after a vehicle joins or leaves the 5G-enabled vehicular networks to preserve user privacy and to prevent adversaries from linking multiple messages to the same sender. Furthermore, the proposed scheme utilizes multiplication inverse in the message signing process, which mitigates the recipient's verification cost. Furthermore, drivers can change their passwords without involving TA, allowing them to change passwords anytime at their convenience.

3. Preliminaries

This section first describes the three components of the proposed authentication scheme for 5G-enabled vehicular networks, followed by identifying the security objectives. Finally, mathematical tools utilized in the proposed scheme are demonstrated. Table 1 lists the notations used by the proposed scheme.

3.1. Network Model

The network model of the proposed scheme in 5G-enabled vehicular networks comprises a trusted authority (TA), some fixed 5G base stations (5G-BS), and mobile vehicles equipped with OBUs, as illustrated in Figure 1. The details of the components are described below.

Table 1. Notations.

Notations	Definitions
P	The generator of the cycle additive group G
P_{pub}, s	The key pairs of the system
sk_i, r_i	The random values from the group of multiplicative Z_q^*
H_1, H_2, H_3	The three secure one-way hash functions
PW_i	The login password for a driver
DID_i, ID_i	The real identity of driver and vehicle
A_i, B_i	The two secret authentication parameters
V_i	The i-th vehicle
s_d, P_{pub}^d	The key pairs of an updated domain
ET_i	The valid period of this domain key s_d
M_i	The safety message
T_i	The current timestamp
$\frac{1}{P}$	The multiplication inverse
σ_i	The message signature
AID_i	The pseudonym ID for each vehicle V_i
vbs_i	The variables
$\|\|, \oplus$	The concatenation operation and exclusive OR
$\equiv$	The congruent modulo

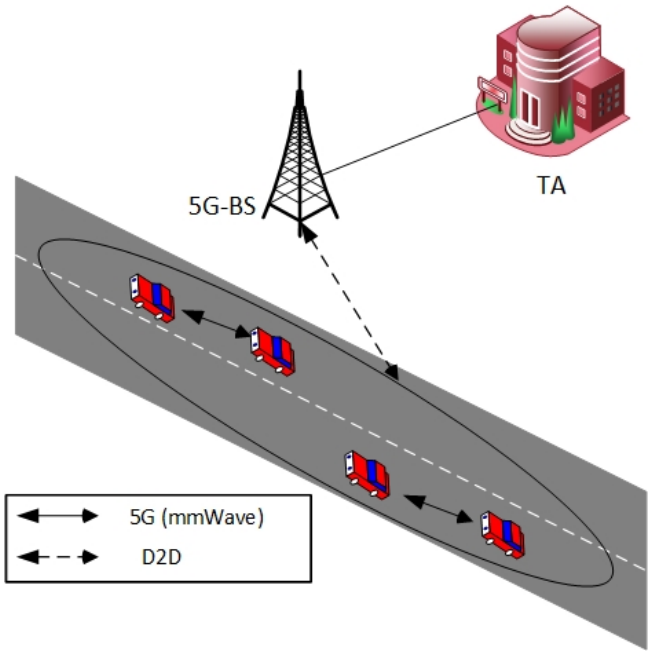

Figure 1. The network model of 5G-enabled vehicular networks.

- Trusted authority (TA): the TA has a large storage capacity and computing power. TA is in charge of issuing system parameters and secret keys for each corresponding vehicle in 5G-enabled vehicular networks. In addition, the TA is responsible for generating sensitive data for each domain. Each network has a group of duplicate TAs to avert bottlenecks and a single point of failure. Therefore, the entire 5G-enabled vehicular networks are segmented into many geographical areas, and each area has a TA in the proposed scheme [40].
- 5G base station (5G-BS): The 5G-BS is a wireless communication device located at intersections or hotspots. The 5G-BS is a transceiver with wide-area coverage and super-fast transmission and is usually security-hardened to prevent compromise. However, it is only an intermediary transmission medium between TA and vehicles; therefore, it does not have any storage and does not execute any verification process.

- Vehicles: Vehicles in the proposed scheme are the terminal nodes in 5G-enabled vehicular networks that enjoy all types of applications. A realistic TPD is usually fitted on the vehicle's OBU. Vehicles can exchange data with each other or local TAs using the 5G protocol.

3.2. Security and Privacy Requirements

Both security and privacy are critical to securing communications for 5G-enabled vehicular networks. Therefore, the proposed scheme should satisfy the following security requirements:

- Message Integrity and Authentication: The receiver must check the integrity and legitimacy of all received messages to ensure secure communication. It must also check messages for tampering during transit.
- Identity Privacy Preservation: The message sent from a registered vehicle should be anonymous and should not use the actual sender's identity to preserve the user's privacy and to prevent privacy breaches.
- Traceability and Revocability: Only the TA can disclose the identity of a vehicle to prevent attackers from forging broadcast messages to avoid accountability and liability for road accidents. Furthermore, TA should have the ability to revoke any malicious vehicle's certificate from future use.
- Unlinkability: To ensure user's privacy, third parties, including adversaries, should not be able to link multiple messages to the same sender.
- Resistance to Security Attacks: The proposed scheme must withstand various known attacks such as modify, replay, impersonation, and password-guessing attacks.

3.3. Mathematical Tools

The following sections introduce the Chinese Remainder Theorem and elliptic curve cryptography.

3.3.1. Chinese Remainder Theorem

The Chinese remainder theorem (CRT) is widely used in authentication schemes for VANETs [41]. In addition, CRT is an essential tool for proving theorems in number theory, which shows that, once the Euclidean division remainders of an integer n are known, then the remainder of n is uniquely determined under pairwise coprime divisors [42,43].

Consider $k_1, k_2, k_3, \ldots, k_n$ to be the positive integers pairwise prime, and consider K_i^- to be the modular multiplicative inverse of K_i mod k_i. Hence, it satisfies Equation (1) as follows, where $i = 1, 2, 3 \ldots n$.

$$K_i K_i^- \equiv 1 (mod\ k_i) \tag{1}$$

Consider $a_1, a_2, a_3, ..., a_n$ to be a specified n positive integers. Hence, CRT shows that the congruence pair has a unique solution mod ζ_g=k_1 k_2..k_i = $\prod_{i=1}^{n}(sk_i)$, as the following equation.

$$\begin{aligned} &X \equiv a_1\ mod\ k_1 \\ &X \equiv a_2\ mod\ k_2 \\ &,\ldots\ldots\ldots.., \\ &X \equiv a_n\ mod\ k_n \end{aligned} \tag{2}$$

The solution is obtained by the key server using the following equation, where $\beta_i = \frac{\zeta_g}{k_i}$ and $\beta_i \gamma_i \equiv 1$ mod k_i.

$$X = a_1 + a_2 + \ldots + a_n (mod\ \zeta_g) = \sum_{i=1}^{n} a_i \beta_i \gamma_i (mod\ \zeta_g) \tag{3}$$

3.3.2. Elliptic Curve Cryptography

Miller [44] introduced elliptic curve cryptography (ECC) in 1985. Since its introduction, ECC has been widely employed in many authentication mechanisms. Some mechanisms documented their implementation steps in detail. For example, assume that the symbol E/F_p indicates an elliptic curve. Then, E is determined using the following equation.

$$y^2 = x^3 + ax + b(mod\ p) \quad (4)$$

where p is a large prime number; a, b $\in F_p$, Z_p is a prime finite field; and $(4a^3 + 27b^2)\ mod\ p \neq 0$. The primary hard problems of ECC are as follows:

- Elliptic Curve Discrete Logarithm (ECDL) Problem: P and $Q = a\mathrm{P} \in Z_q^*$ are two random points on ECC. The core idea of this problem is to calculate the secret value a from point $Q = a\mathrm{P} \in Z_q^*$. However, it is difficult to calculate the points $Q = a\mathrm{P}$ with negligible probability based on the supposition.
- Elliptic Curve Computational Diffie–Hellman (ECCDH) Problem: $R = b\mathrm{P}$ and $Q = a\mathrm{P} \in Z_q^*$ are two random points on ECC. The core idea of this problem is to calculate the secret values a and b from points $R = b\mathrm{P}$ and $Q = a\mathrm{P} \in Z_q^*$. However, based on the supposition, it is difficult to compute the points $R = b\mathrm{P}$ and $Q = a\mathrm{P}$ with negligible probability.

4. Proposed Scheme

This section explains the proposed scheme to secure communication in 5G-enabled vehicular networks, as shown in Figure 2. The proposed scheme has seven phases: system setup, registration, login, secure domain key calculation, message signing and verification, pseudonym ID and domain key updating, and password-changing phases.

Unlike the scheme by Zhang et al. [36], the proposed scheme utilizes multiplication inverse $\frac{1}{P}$ in the message signing process (refer to Section 4.5.1), which mitigates the receiver's verification costs. Moreover, in the pseudonym ID and domain key updating phase of the proposed scheme (refer to Section 4.6), the pseudonym ID is periodically updated after a vehicle joins or leaves the 5G-enabled vehicular networks to preserve user's privacy and to prevent attackers from linking multiple messages to the same sender. In addition, even without the TA's assistance, drivers are provided with a convenient password-changing procedure that allows drivers to change their passwords anytime (refer to Section 4.7).

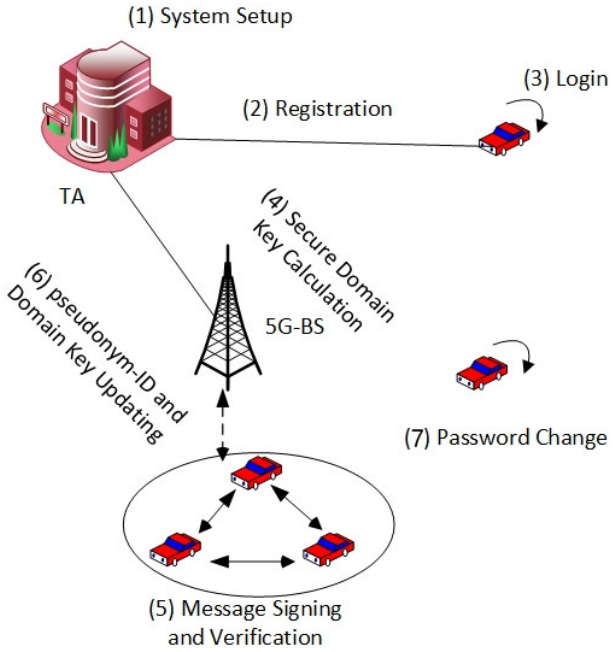

Figure 2. Flow diagram of the proposed scheme.

4.1. System Setup Phase

In the system setup phase, the TA executes the following processes.

- TA uses a randomly chosen value $s \in Z_q^*$ as its secret key and then calculates its relevant public key $P_{pub} = sP$;
- TA selects two large prime values q and p, where $q \leq [p/4]$ and $p > q$, p is utilized for identifying a group of multiplicative Z_q^*, and q is utilized for selecting the domain key;
- TA utilizes the randomly selected value sk_i from the group of multiplicative Z_q^* for 'n' number of vehicles, which is given to the users during the offline registration time;
- TA computes x_i= $\frac{\zeta_g}{sk_i}$, where ζ_g=$\prod_{i=1}^{n}(sk_i)$ and $i = 1, 2, 3, \ldots, n$;
- TA computes y_i such that $x_i \times y_i \equiv 1 \bmod sk_i$;
- TA multiplies all users x_i and y_i numbers, saves them in the variables $vbs_i = x_i \times y_i$, and computes the number $\mu = \sum_n^i(vbs_i)$;
- TA utilizes three selected secure one-way hash functions $H_i : \{0,1\}^* \rightarrow Z_q^*$ $(i = 1, 2, 3)$;

4.2. Registration Phase

In the domain of 5G-enabled vehicular networks, vehicle Vi begins the registration process with the local TA by following these steps:

- After the login password PW_i is chosen, the driver submits the identity of driver DID_i and the identity of vehicle ID_i to the local TA.
- TA computes two secret authentication parameters $A_i = H_1(DID_i||ID_i||s)$ and $B_i = H_1(PW_i) \oplus A_i$.
- TA randomly picks a value $r_i \in Z_q^*$ and computes the corresponding $R_i = r_iP$ for V_i. It then computes a pseudonym ID $AID_i = ID_i \oplus H_1(s||R_i)$ for each vehicle V_i.
- TA preloads $\{p, q, P, E, G, R_i, Z_q^*, DID_i, ID_i, PW_i, A_i, B_i, P_{pub}, H_1, H_2, H_3\}$ to the vehicle V_i.
- Finally, TA stores $\{ID_i\}$ locally.

The adversary cannot launch a successful stolen-verified attack because the TA does not store the vehicle's login password.

4.3. Login Phase

Vehicle V_i should validate the driver before accepting the secure domain key calculation in 5G-enabled vehicular networks. The login phase follows these steps:

- Driver inputs (PW_i, DID_i, ID_i) to vehicle V_i.
- Vehicle V_i checks whether the equation $B_i = H_1(PW_i) \oplus A_i$ holds a given PW_i, where TA preloads A_i.
- If the driver inputs match the login password PW_i, then vehicle V_i permits this login request; otherwise, vehicle V_i rejects this request.

4.4. Secure Domain Key Calculation Phase

Once TA calculates the domain key for 5G-enabled vehicular networks, TA multicasts it to the domain of the vehicles via 5G-BS in the following steps.

- TA sets the randomly selected value $s_d \in Z_q^*$ as an updated domain key and then calculates its corresponding public key $\gamma_d = s_d \times \mu$;
- TA assigns γ_d and ET_i utilizing its private key sk_{TA} as $SIG_{sk_{TA}}(\gamma_d||ET_i)$, where ET_i denotes the valid period of this domain key s_d;
- TA calculates $P_{pub}^d = s_dP$ and broadcasts the tuple $\{\gamma_d, P_{pub}^d, SIG_{sk_{TA}}(\gamma_d||ET_i)\}$ to all 5G-BS and vehicles in D_y;
- Once the authorized vehicle receives γ_d from the TA side, it can obtain an updated domain key s_d via a one modulo division operation $gamma_d \bmod sk_i = s_d$.

Due to $s_d < q < sk_i < p$ and $\mu \bmod sk_i = 1$, s_d obtained via the above steps should equal the number of s_d computed in the first step of this phase. Once "i" holds to n, TA

performs the system setup process to calculate ζ_g, vbs_i and μ for "m" users value, where $m = n \times \zeta$, where ζ is a constant that fulfills $\zeta < 5$.

4.5. Message Signing and Verification Phase

After completing the login phase, vehicle V_i first computes signing keys. Then, vehicle V_i sends its pseudonym ID, the message, and the respective message signature to its neighboring vehicles. Upon receiving the message-signature tuple, the receiver must check its message signature before accepting the messages. The message signing and verification processes are explained separately in subsequent subsections.

4.5.1. Message Signing

When vehicle V_i wants to assign a message, it has to execute the steps below, where tt_i is the latest timestamp and M_i is infotainment information or safety-related messages.

- Vehicle V_i obtains an updated domain key s_d via a one modulo division operation γ_d mod $sk_i = s_d$.
- Vehicle V_i calculates $\alpha_i = H_2\,(AID_i||R_i||M_i||T_i)$ and then computes $\beta_i = H_3(AID_i||R_i||T_i)$, where M_i is safety-related-message and T_i is the current timestamp.
- By using multiplication inverse $\frac{1}{P}$, vehicle V_i sets the message signature $\sigma_i = s_d.\alpha_i + \frac{1}{P}\beta_i$ mod q, which $\frac{1}{P}$ is utilized to mitigate the receiver's verification cost.
- Vehicle V_i sends the message-signature tuple $\{AID_i, R_i, M_i, T_i, \sigma_i\}$ to the neighboring vehicles.

4.5.2. Message Verification

The proposed scheme offers two modes of message verification processes: single message verification and batch message verification.

Single Message Verification

Upon receiving the message signature, the receiving vehicle must check the message and signature authenticity and integrity before accepting it to prevent malicious vehicles from impersonating authentic vehicles and from transmitting false messages. Therefore, each receiver must verify the message signature σ_i of the signed message by utilizing this verification process, as follows:

- Upon receiving the message-signature tuple $\{AID_i, R_i, M_i, T_i, \sigma_i\}$, the verifier initially verifies the timestamp of the message. The receiver can accept the message if it is fresh; otherwise, it rejects the tuple.
- The verifier checks whether Equation (5) holds with $\sigma_i.P$.

$$\sigma_i.P = H_2(AID_i||R_i||M_i||T_i)P^d_{pub} + H_3(AID_i||R_i||T_i) \tag{5}$$

The following step proves Equation (5).

$$\begin{aligned} L.H.S &= \sigma_i.P \\ &= \left(s_d.\alpha_i + \frac{1}{P}\beta_i\right).P \\ &= \left(s_d.H_2(AID_i||R_i||M_i||T_i) + \frac{1}{P}H_3(AID_i||R_i||T_i)\right).P \\ &= H_2(AID_i||R_i||M_i||T_i)s_d.P + H_3(AID_i||R_i||T_i)\frac{1}{P}.P \\ &= H_2(AID_i||R_i||M_i||T_i)P^d_{pub} + H_3(AID_i||R_i||T_i \\ &= R.H.S. \end{aligned}$$

Hence, it is verified that Equation (5) is true.

Batch Message Verification

Upon receiving a large number of message-signature tuples $\{AID_i^1, R_i^1, M_i^1, T_i^1, \sigma_i^1\}$, $\{AID_i^2, R_i^2, M_i^2, T_i^2, \sigma_i^2\}$,…,$\{AID_i^n, R_i^n, M_i^n, T_i^n, \sigma_i^n\}$ from other vehicles, the verifier can simultaneously verify n messages. The verifier checks whether Equation (6) holds given $\sum_{i=1}^{n}(a_i.\sigma_i).P$.

$$\sum_{i=1}^{n}\left(a_i.\sigma_{v_i}\right)P = \sum_{i=1}^{n}\left(a_i.H_2(AID_i||R_i||M_i||T_i)\right)P_{pub}^{d} + \sum_{i=1}^{n}\left(a_i.H_3(AID_i||R_i||T_i)\right) \quad (6)$$

4.6. Pseudonym ID and Domain Key Updating Phase

The pseudonym ID and domain key updating phase begins immediately once a vehicle joins or leaves the network. The TA is responsible for securely disseminating the updated domain key to domain members every time a vehicle joins a 5G-enabled vehicular network domain. Since newly joined vehicles cannot listen to the above communication, backward secrecy is preserved. Similarly, once a vehicle leaves a domain, TA updates the domain key to prevent the key from being reused on the old vehicle, thus ensuring forward secrecy. When the domain membership changes, the proposed scheme provides a pseudonym ID update to prevent adversaries from tracing authorized vehicles by linking multiple messages to the same sender. In this phase, the TA has to execute the batch leave or batch join process depending on the vehicle's action.

4.6.1. Batch Leave

Once a vehicle leaves domain D_y, the nearest TA will update the pseudonym ID and domain key. For example, if four vehicles v_2, v_4, v_6, and v_8 leave domain D_y, the TA executes the following steps:

- Subtract vbs_2, vbs_4, vbs_6, and vbs_8 from μ as follow

$$\mu^{-} = \mu - (vbs_2 + vbs_4 + vbs_6 + vbs_8) \quad (7)$$

- TA should select an updated domain key s_d^{-}, and it must be multiplied by μ^{-} to form the message from rekeying.

$$\gamma_d^{-} = s_d^{-} \times \mu^{-} \quad (8)$$

- TA randomly picks a value $r_i^{-} \in Z_q^*$ and computes the corresponding $R_i^{-} = r_i^{-}P$ for each existing vehicle in the domain. It then computes a pseudonym ID $AID_i^{-} = ID_i \oplus H_1(s||R_i^{-})$ for each vehicle V_i^{-} in the domain.
- TA deliveries the pseudonym ID and updated domain key as a broadcast message. Once existing vehicles in the domain receive an updated domain key, s_d^{-} is obtained by performing the modulo operation once. Vehicle V_i cannot disclose the newly updated domain key s_d^{-} since its secret key is not in μ. Hence, once "n" vehicles want to leave the domain, TA updates the domain key by executing (n-1) additions and one subtraction operation.

Hence, once "n" vehicles want to leave the domain, $(n-1)$ additions and one subtraction operation are executed by the TA to update the domain key.

4.6.2. Batch Join

Once some vehicles want to join the domain D_y, the TA executes additional operations to update the pseudonym ID and domain key. For example, when the vehicles v_2, v_4, v_6, and v_8 are ready to enter the domain D_y, the TA executes the following steps:

- Rather than calculating x_i and y_i for these vehicles, the TA takes the multiplied numbers of x_i and y_i from vbs_2, vbs_4, vbs_6, and vbs_8, which has been pre-calculated in the system setup phase.

$$\mu^{-} = \mu + (vbs_2 + vbs_4 + vbs_6 + vbs_8) \quad (9)$$

- TA should select an updated domain key s_d^{-} and multiply it by μ^{-} to form a rekeying message, as per Equation (8).
- TA randomly picks a value $r_i^{-} \in Z_q^*$ and computes the corresponding $R_i^{-} = r_i^{-}P$ vehicle V_i the domain. It then computes a pseudonym ID $AID_i^{-} = ID_i \oplus H_1(s||R_i^{-})$ for each vehicle V_i^{-} in the domain, where $i = 2, 4, 6, 8$.
- TA deliveries the pseudonym ID and updated domain key as a broadcast message. Vehicle V_i obtains newly updated domain key s_d^{-} because vbs_i (i.e., vbs_2, vbs_4, vbs_6, and vbs_8) are contained in μ.

Therefore, if "n" vehicles want to join the vehicle's multicast domain, the TA executes "n" addition operations to update the domain key, which translates to big-oh of 1 (O(1)) calculation complexity. Furthermore, TA only sends one message to the vehicles in the multicast domain.

4.7. Password Changing Phase

The proposed scheme provides drivers with an appropriate password-changing operation without TA assistance. To execute this phase, the drivers must follow the following steps:

- The driver keys in PW_i, DID_i, ID_i, and PW_i^{-}
- Vehicle V_i verifies whether Equation $B_i = H_1(PW_i) \oplus A_i$ hold with driver's inputs.
- If the equation holds, vehicle V_i then executes $B_i^{-} = B_i \oplus H_1(PW_i) \oplus H_1(PW_i^{-})$ to change PW_i to PW_i^{-}.

5. Security Analysis

This section presents the security analysis of the proposed scheme.

5.1. Security Proof

Since the 5G-enabled vehicular network relies on wireless communication channels for inter-vehicle communication, adversaries always have opportunities to exploit them. To this end, the following game-based security model analysis proves that the proposed scheme is secure against adaptive selection message attacks.

Game: The adversary's ability to compromise the proposed scheme is determined by a game between challenger B and adversary A. Note that B maintains three hash lists, L_{H_1}, L_{H_2}, and L_{H_3}.

Proof: Suppose that A can fabricate a valid message-signature tuple {AID_i, R_i, M_i, T_i, and σ_i} of the safety-related message Mi. Challenger B has been established depending on A. Challenger B is responsible for distinguishing whether the attacker can solve the ECDL problem by running for A as a subroutine with a non-ignorable probability.

Setup: This process obtains sensitive data k as input. B picks the randomly chosen value s_d as its secret key and then calculates public key P_{pub}, where $P_{pub} = s_d$P. Afterward, B sends $P, P_{pub}, q, H_1, H_2, H_3$ to adversary A.

H_1-hash query: When A invokes an H_1 query utilizing the tuple (θ), B tests whether the tuple (θ) already exists in L_{H_1}, under the tuple of (θ, h_1). If so, B outputs h_1 to A; otherwise, B chooses a random value h_1 and then adds the new tuple (θ, h_1) into the hash list L_{H_1}. Afterward, B transmits the value of $h_1 = H_1(\theta)$ to A.

H_2-hash query: When A invokes an H_2 query utilizing the tuple (AID_i, R_i, M_i, T_i), B tests whether the tuple (AID_i, R_i, M_i, T_i) already exists in hash list L_{H_2}, under the tuple of $(AID_i, R_i, M_i, T_i, h_2)$. If so, B outputs h_2 to A; otherwise, B picks a random value h_2 and then inserts the new tuple $(AID_i, R_i, M_i, T_i, h_2)$ into the hash list L_{H_2}. Afterwards, B transmits the value of $h_2 = H_2(AID_i||R_i||M_i||T_i)$ to A.

H_3-hash query: When A invokes an H_3 query utilizing the tuple (AID_i, R_i, T_i), B tests whether the tuple (AID_i, R_i, T_i) already exists in hash list L_{H_3}, under the tuple of (AID_i, R_i, T_i, h_3). If so, B outputs h_3 to A; otherwise, B picks a random value h_3 then inserts

the new tuple (AID_i, R_i, T_i, h_3) into the hash list L_{H_3}. Afterwards, B transmits the value of $h_3 = H_3(AID_i||R_i||T_i)$ to A.

Sign query: If adversary A made a signing query on message M_i, B adds $(AID_i, R_i, M_i, T_i, h_2)$ and (AID_i, R_i, T_i, h_3) into the hash lists L_{H_2} and L_{H_3}, respectively. Finally, B sends message-signature tuple $\{AID_i, R_i, M_i, T_i, \sigma_i\}$ to A. The outcome of this phase is a valid signature once the message satisfies Equation (10).

$$\begin{aligned} &\sigma_i.P = h_{i,2}P^d_{pub} + h_{i,3} \\ &h_{i,3} = \sigma_i.P - h_{i,2}P^d_{pub} \\ &= h_{i,2}P^d_{pub} + (\sigma_i.P - h_{i,2}P^d_{pub}) \\ &= h_{i,2}P^d_{pub} + (\sigma_i.P - h_{i,2}P^d_{pub}) = \sigma_i.P \end{aligned} \tag{10}$$

Output: At last, A outputs message-signature tuple $\{AID_i, R_i, M_i, T_i, \sigma_i\}$. B checks this tuple utilizing Equation (11).

$$\sigma_i.P = h_{i,2}P^d_{pub} + h_{i,3} \tag{11}$$

If not, B finishes the game. By utilizing the forgery lemma [45], A could result in another legitimate tuple $\{AID_i, R_i, M_i, T_i, \sigma^*_i\}$ if it selects another H_2, where $H^*_2 \neq H_2$ that fulfills the following equation.

$$\sigma^*_i.P = h^*_{i,2}P^d_{pub} + h_{i,3} \tag{12}$$

According to Equations (11) and (12), the following is deduced.

$$\begin{aligned} &(\sigma^*_i - \sigma^*_i).P = \sigma^*_i.P - \sigma^*_i.P \\ &= \left(h^*_{i,2}P^d_{pub} + h_{i,3}\right) - \left(h_{i,2}P^d_{pub} + h_{i,3}\right) \\ &= h^*_{i,2}P^d_{pub} - h_{i,2}P^d_{pub} \\ &= \left(h^*_{i,2} - h_{i,2}\right).P^d_{pub} \\ &= \left(h^*_{i,2} - h_{i,2}\right).s_d.P \end{aligned} \tag{13}$$

Now, B outputs $\left(h^*_{i,2}\text{ - }h_{i,2}\right)^{-1}\left(h^*_{i,2}\text{ - }h_{i,2}\right)$ as a solution to the given ECDL problem instance. Nevertheless, it contradicts the hardness of solving the ECCDL problem. Therefore, the proposed scheme is secure against adaptive selection message attacks under the random oracle model. Figure 3 illustrates an example of the game played between challenger B and adversary A.

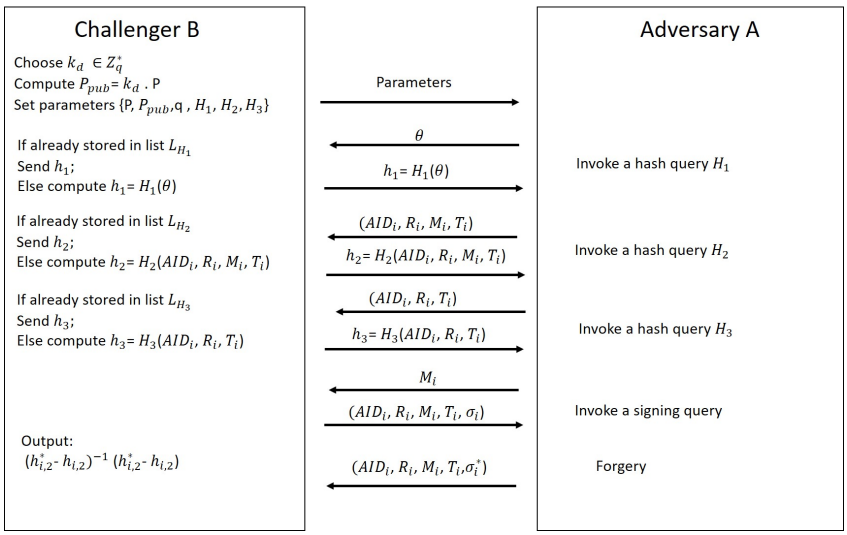

Figure 3. Example of the game played between a challenger B and an adversary A.

5.2. Security Analysis

This subsection presents the analysis of the proposed scheme security under the above-stated security proof.

- Message integrity and authentication: Consistent with the above security proof, no attacker can forge a valid signature in polynomial time because the ECDL problem is hard. Thus, the recipient can verify the validity of messages received from other vehicles using Equation (5).
- Identity privacy-preserving: The real identity of the vehicle ID_i is hidden in the pseudonym ID such as $AID_i = ID_i \oplus H_1(s||R_i)$, where $R_i = r_iP$ and $r_i \in Z_q$. Since the system's private key is secret and $r_i \in Z_q$ is random, others cannot obtain the vehicle's original identity.
- Traceability and Revocability: Once illegal information or error messages are sent by a vehicle using a pseudonym ID AID_i, the TA can disclose the identity of the vehicle ID_i utilizing $ID_i = AID_i \oplus H_1(s||R_i)$. In addition, after revoking the malicious vehicle's certificate, the TA saves it on the certificate revocation list (CRL). Once the vehicles group wants to update their pseudonym ID and domain key while joining or leaving, the TA only updates them to non-revoked vehicles. After the expiry of the old domain key, the revoked vehicle's certificate will no longer be usable in the future.
- Unlinkability: Since all registered participating vehicles dynamically update their pseudonym ID when joining or leaving a domain, no adversary can link multiple messages to the same vehicle during its travel.
- Resistance to security attacks: The proposed scheme could resist the following known attacks:
  - Resistance to modify attack: In the proposed scheme, a registered participating vehicle broadcasts message-signature tuple $\{AID_i, R_i, M_i, T_i, \sigma_i\}$ wirelessly to others. Since the signature σ_i of each message includes a hidden domain private key s_d, there is no disclosure of the key, preventing adversaries from modifying the message undetected. The receiver detects modifications to the message since the signature verification fails. Hence, the proposed system is resistant to modify attacks.
  - Resistance to replay attack: In the proposed scheme, a timestamp T_i is included in the signature σ_i of each message-signature tuple $\{AID_i, R_i, M_i, T_i, \sigma_i\}$, where $\sigma_i = s_d.\alpha_i + \frac{1}{p}\beta_i \bmod q$, $\alpha_i = H_2\ (AID_i||R_i||M_i||T_i)$ and $\beta_i = H_3(AID_i||R_i||T_i)$, making it impossible to tamper with the signature. By validating the signature, the recipient can detect any replay attacks. Hence, the proposed system is resistant to replay attacks.
  - Resistance to impersonation attack: Consistent with the above security proof, no adversary can forge a valid signature message without the domain private key s_d. Hence, the proposed system is resistant to impersonation attacks.
  - Resistance to password-guessing attack: Once the driver's real identity DID_i, the vehicle's identity ID_i, and the login password PW_i are submitted to the local TA, there will no longer be a threat of disclosure. The driver holds two secret authentication parameters A_i and B_i that TA computed. After the login phase, only a legitimate driver can control the registered participating vehicle, thus preventing adversaries from taking control of the vehicle. Hence, the proposed system is resistant to password-guessing attacks.

5.3. Security Comparison

Table 2 compares the properties of the proposed scheme with the recant eight existing authentication schemes of Zhong et al. [25], Azees et al. [26], Bayat et al. [29], Asaar et al. [31], Li et al. [32], Zhang et al. [36], Cui et al. [39], and Cui et al. [38]. From this table, the schemes of Zhong et al. [25], Azees et al. [26], Bayat et al. [29], Asaar et al. [31], Li et al. [32], and Zhang et al. [36] are vulnerable to password-guessing attacks and requires RSUs for operation. In addition, a dedicated TPD is requirement for the schemes of Zhong et al. [25], Azees et al. [26], Bayat et al. [29], Asaar et al. [31], Li et al. [32],

Cui et al. [39], and Cui et al. [38]. Therefore, the proposed scheme satisfies all stated security and privacy requirements compared with other schemes, as presented in Table 2.

Table 2. Security comparison.

Scheme	Zhong et al. [25]	Azees et al. [26]	Bayat et al. [29]	Asaar et al. [31]	Li et al. [32]	Zhang et al. [36]	Cui et al. [39]	Cui et al. [38]	Proposed Scheme
Traceability and Revocability	✓	✓	✓	✓	✓	✓	✓	✓	✓
Identity privacy-preserving	✓	✓	✓	✓	✓	✓	✓	✓	✓
Message integrity and authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓
Unlinkability	✓	✓	✓	✓	✓	✓	✓	✓	✓
No RSU aided	✗	✗	✗	✗	✗	✗	✓	✓	✓
No TPD aided	✗	✗	✗	✗	✗	✓	✗	✗	✓
Resistance to impersonation attack	✓	✓	✓	✓	✓	✓	✓	✓	✓
Resistance to modify attack	✓	✓	✓	✓	✓	✓	✓	✓	✓
Resistance to password-guessing attack	✗	✗	✗	✗	✗	✗	✓	✓	✓
Resistance to replay attack	✓	✓	✓	✓	✓	✓	✓	✓	✓

6. Performance Evaluation

This section presents the evaluation and comparison of the proposed scheme with eight existing authentication schemes for vehicular networks. The schemes by Zhong et al. [25], Azees et al. [26], Bayat et al. [29], and Asaar et al. [31] use bilinear pairing-based cryptographic operations, whereas the schemes by Li et al. [32], Zhang et al. [36], Cui et al. [39], and Cui et al. [38] as well as the proposed scheme use ECC-based cryptographic operations. Table 3 lists the notations and run times of several cryptographic operations from the simulation experiments.

Table 3. The run times of cryptographic operations.

Cryptographic Operation	Notation	Run Time (Milliseconds)
The bilinear pairing operation	T_{bp}	5.811
The scalar multiplication operation of the bilinear pairing	T_{bp-pm}	1.5654
The point addition operation of the bilinear pairing	T_{bp-pa}	0.0106
The MapToPoint hash function operation	$T_{M.T.P}$	4.1724
The scalar multiplication operation operation of ECC	T_{ecc-pm}	0.6718
The point addition operation	T_{ecc-pa}	0.0031
The secure cryptographic hash function operation	T_h	0.001

This paper uses MIRACL [46], a cryptography library code, to perform cryptographic operations. The hardware platform is a PC with Intel® Core™ i7-2670QM 2.20 GHz processor and 16.0 GB RAM running on 64-bit Microsoft® Windows™ 10 operating system.

6.1. Computation Cost Analysis and Comparison

This section discusses Zhong et al.'s scheme [25] and the proposed scheme, whereas the schemes of Azees et al. [26], Bayat et al. [29], Asaar et al. [31], Li et al. [32], Zhang et al. [36], Cui et al. [39], and Cui et al. [38] are analyzed using the same method. Table 4 presents the computation cost of each process.

Table 4. Computation cost comparison.

Scheme	Single Message Singing	Single Message Verification	Batch Messages Verification
Zhong et al. [25]	$3T_{bp-pm} + 2T_{bp-pa} + 1T_{M.T.P} + 1T_h \approx 23.192$ ms	$3T_{bp} + 2T_{bp-pm} + 1T_{bp-pa} + 2T_{M.T.P} + 1T_h 27.3644 \approx 27.3644$ ms	$3T_{bp} + (2n)T_{bp-pm} + (4n-3)T_{bp-pa} + (n+1)T_{M.T.P} + (2n)T_h \approx 21.5736 + 7.3476n$ ms
Azees et al. [26]	$4T_{bp-pm} + 2T_h \approx 6.2636$ ms	$2T_{bp} + 5T_{bp-pm} + 2T_{bp-pa} \approx 19.4702$	$(n+1)T_{bp} + (5n)T_{bp-pm} + (2n)T_{bp-pa} \approx 5.811 + 13.6592n$
Bayat et al. [29]	$6T_{bp-pm} + 1T_{bp-pa} + 1T_h \approx 9.404$	$3T_{bp} + 2T_{bp-pm} \approx 20.5638$	-
Asaar et al. [31]	$7T_{ecc-pm} + 6T_h \approx 4.7086$ ms	$12T_{ecc-pm} + 8T_{ecc-pa} + 8T_h \approx 8.0884$ ms	$(4n+10)T_{ecc-pm} + (6n+2)T_{ecc-pa} + (6n+2)T_h \approx 6.7262 + 2.7118n$ ms
Li et al. [32]	$1T_{ecc-pm} + 2T_h \approx 0.6729$ ms	$4T_{ecc-pm} + 1T_{ecc-pa} + 2T_h \approx 2.6923$ ms	$(2n+2)T_{ecc-pm} + (n)T_{ecc-pa} + (2n)T_h \approx 1.3436 + 1.3487n$ ms
Zhang et al. [36]	$2T_{ecc-pm} + 2T_h \approx 1.3456$ ms	$3T_{ecc-pm} + 2T_{ecc-pa} + 2T_h \approx 2.0236$ ms	$(n+2)T_{ecc-pm} + (n)T_{ecc-pa} + (2n)T_h \approx 1.3436 + 1.3487n$ ms
Cui et al. [39]	$1T_{ecc-pm} + 1T_h \approx 0.6728$ ms	$3T_{ecc-pm} + 2T_{ecc-pa} + 2T_h \approx 2.0236$ ms	$(n+2)T_{ecc-pm} + (2n+2)T_{ecc-pa} + (2n)T_h \approx 1.3436 + 1.3487n$ ms
Cui et al. [38]	$3T_{ecc-pm} + 3T_h \approx 2.0184$ ms	$3T_{ecc-pm} + 1T_{ecc-pa} + 2T_h \approx 2.0205$ ms	$(n+2)T_{ecc-pm} + (n-1)T_{ecc-pa} + (2n)T_h \approx 1.3405 + 0.6769n$ ms
Proposed scheme	$1T_{ecc-pm} + 2T_h \approx 0.0051$ ms	$2T_{ecc-pm} + 1T_{ecc-pa} + 2T_h \approx 1.3487$ ms	$2T_{ecc-pm} + (n+1)T_{ecc-pa} + (2n)T_h \approx 1.3467 + 0.0051n$ ms

The scheme of Zhong et al. [25] relies on bilinear pairing operations. A single message signing process in Zhong et al.'s scheme [25] requires a registered participating vehicle to run three operations of scalar multiplication $3T_{bp-pm}$, two operations of point addition $2T_{bp-pa}$, one MapToPoint hash function operation $1T_{M.T.P}$, and one operation of hash function $1T_h$. Consequently, the whole run time is $3T_{bp-pm} + 2T_{bp-pa} + 1T_{M.T.P} + 1T_h \approx$ ms. A single message-verification process in Zhong et al.'s scheme [25] requires the verifying recipient to perform three operations of bilinear pairing $3T_{bp}$, two operations of scalar multiplication $2T_{bp-pm}$, one operation of point addition $1T_{bp-pa}$, two operations of MapToPoint hash function $2T_{M.T.P}$, and one operation of hash function $1T_h$. Consequently, the total run time is $3T_{bp} + 2T_{bp-pm} + 1T_{bp-pa} + 2T_{M.T.P} + 1T_h \approx$ ms. The process of verifying multiple messages in Zhong et al.'s scheme [25] requires the verifying recipient to run three bilinear pairing operations $3T_{bp}$, $(2n)$ scalar multiplication operations $(2n)T_{bp-pm}$, $(4n-3)$ point addition operations $(4n-3)T_{bp-pa}$, $(n+1)$ MapToPoint hash function operations $(n+1)T_{M.T.P}$, and $(2n)$ hash function operations $(2n)T_h$. Consequently, the total run time is $3T_{bp} + (2n)T_{bp-pm} + (4n-3)T_{bp-pa} + (n+1)T_{M.T.P} + (2n)T_h \approx$ ms.

As for the ECC adopted in the proposed scheme, the single message signing process requires registered participating vehicle to run one operation of point addition $1T_{ecc-pa}$, and two operations of hash function $2T_h$. Consequently, the total run time is $1T_{ecc-pm} + 2T_h \approx$ ms. For a single message verification, the verifying recipient must perform two operations of scalar multiplication $2T_{ecc-pm}$, one operation of point addition $1T_{ecc-pa}$, and two operations of hash function $2T_h$. Consequently, the total run time is $2T_{ecc-pm} + 1T_{ecc-pa} + 2T_h \approx$ ms. To verify multiple messages in the proposed scheme, the verifying recipient needs to carry out two scalar multiplication operations $2T_{ecc-pm}$, $(n+1)$ point addition operations $(n+1)T_{ecc-pa}$, and $(2n)$ hash function operations $(2n)T_h$. Consequently, the total run time is $2T_{ecc-pm} + (n+1)T_{ecc-pa} + (2n)T_h \approx$ ms.

As presented in Figure 4, the proposed scheme achieved a much lower computation cost for signing and verifying a single message than the existing schemes. Furthermore, Figure 5 shows that the proposed scheme has a significant advantage in batch verifi-

cation of multiple messages compared with the eight other authentication schemes of Zhong et al. [25], Azees et al. [26], Bayat et al. [29], Asaar et al. [31], Li et al. [32], Zhang et al. [36], Cui et al. [39], and Cui et al. [38]. The proposed scheme achieves the best performance among the schemes compared.

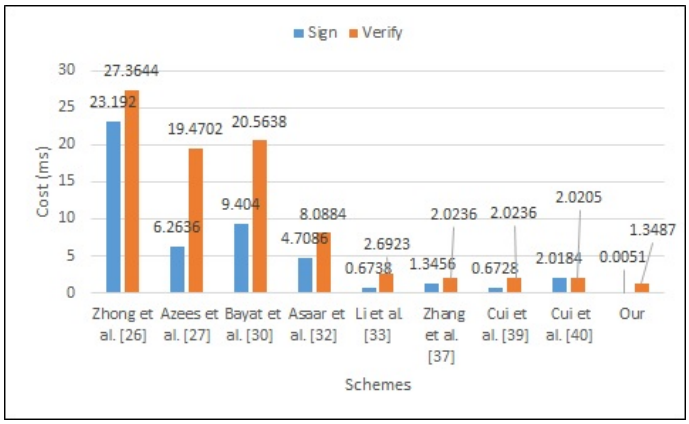

Figure 4. Computation cost for signing and verifying messages.

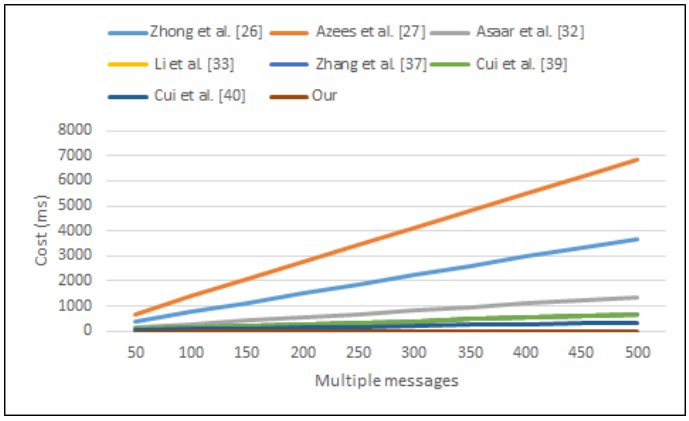

Figure 5. Computation cost in the batch verification of multiple messages.

6.2. Communication Cost Analysis and Comparison

In ECC, the length of cyclic group $G(p)$ is 40 bytes and the size of p is 20 bytes. In bilinear pairing, the length of cyclic group $G_1(p^-)$ is 128 bytes and the p size is 64 bytes. In addition, the timestamp and the size of integer item Z_q^* are 4 bytes and 20 bytes, respectively.

In the proposed scheme, registered participating vehicles broadcast $\{AID_i, R_i, M_i, T_i, \sigma_i\}$ to others, where $(R_i \in G)$, $(AID_i, \sigma_i \in Z_q^*)$ and T_i is the timestamp. Consequently, the total size of the message signature is (40 + 20 * 2 + 4) = 84 bytes. The same method is also used in the analysis of other related schemes.

Table 5 shows that the communication cost of the proposed scheme is lower than the related schemes of Zhong et al. [25], Azees et al. [26], Bayat et al. [29], Asaar et al. [31], Li et al. [32], Cui et al. [39], and Cui et al. [38].

Table 5. Communication cost comparison.

Scheme	Message Format	Size
Zhong et al. [25]	$\{PID_i, m_i, upk_i, t_i, \sigma_i\}$	644 bytes
Azees et al. [26]	$\{sig, Y_k, Cert_k\}$	848 bytes
Bayat et al. [29]	$\{V, m, r, T_{i1}, T_{i2}, T_{i3}, PID_i, ts_i\}$	772 bytes
Asaar et al. [31]	$\{PID_i, T_i, m_i, R_i, W_i, s_{i,1}, s_{i,2}\}$	184 bytes
Li et al. [32]	$\{M_i, PID_{i,l}, PK_{i,l}, R_i, T_i, sig_i\}$	144 bytes
Zhang et al. [36]	$\{ID_{i,1}, ID_{i,2}, M, T, \sigma\}$	84 bytes
Cui et al. [39]	$\{AID_i, R_i, M_1, M_2, tt_i, \sigma_{vi}\}$	104 bytes
Cui et al. [38]	$\{PID_j^1, PID_j^2, DT_{ij}, \sigma_j, D_j, T_j\}$	124 bytes
Proposed scheme	$\{AID_i, R_i, M_i, T_i, \sigma_i\}$	84 bytes

7. Conclusions

This paper proposed a password-guessing attack-aware authentication scheme based on CRT to secure inter-vehicle communication in 5G-enabled vehicular networks. The proposed scheme does not preload the system's master key into any TPD, making it impossible for adversaries to compromise the system. In addition, once a vehicle leaves or joins a domain, the TA dynamically updates the pseudonym IDs and domain keys for all domain vehicles to achieve high privacy preservation in 5G-enabled vehicular networks. In addition, during the login phase of the proposed scheme, the driver holds two secret authentication parameters to prevent adversaries from taking control of the registered vehicle. Furthermore, the security analysis showed that the proposed scheme is secure against adaptive chosen-message attacks under the random oracle model. Moreover, the proposed scheme not only satisfies the security requirements in terms of message integrity and authentication, identity privacy preservation, traceability and revocability, and unlinkability but also resists the security attacks such as modify, replay, impersonation, and password-guessing attacks for 5G-enabled vehicular networks. Finally, the evaluation proved that the proposed scheme achieved better performance in terms of computation cost and communication cost than existing schemes.

Our future work will include the design of an authentication scheme based on a fog computing that does not use ECC in 5G-enabled vehicular networks.

Author Contributions: Conceptualization, M.A.A.-S., M.A. and S.M.; methodology, M.A.A.-S., M.A. and S.M.; software, M.A.A.-S. and M.A.; validation, M.A.A.-S., M.A. and S.M.; formal analysis, M.A.A., M.A. and S.M.; investigation, M.A.A.-S., M.A. and S.M.; resources, I.H.H.; data curation, M.A.A.-S., M.A. and S.M.; writing—original draft preparation, M.A.A.-S., M.A. and S.M.; writing—review and editing, M.A.A.-S., M.A., I.H.H. and S.M.; visualization, M.A.A.-S., M.A. and S.M.; supervision, M.A. and S.M.; project administration, M.A.A.-S.; funding acquisition, I.H.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research is funded by Universiti Sains Malaysia (USM) via external grant (number 304/PNAV/650958/U154).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lai, C.; Lu, R.; Zheng, D.; Shen, X. Security and privacy challenges in 5G-enabled vehicular networks. *IEEE Netw.* **2020**, *34*, 37–45. [CrossRef]
2. Al-Shareeda, M.A.; Anbar, M.; Hasbullah, I.H.; Manickam, S. Survey of authentication and privacy schemes in vehicular ad hoc networks. *IEEE Sens. J.* **2020**, *21*, 2422–2433. [CrossRef]
3. Andrews, J.G.; Buzzi, S.; Choi, W.; Hanly, S.V.; Lozano, A.; Soong, A.C.; Zhang, J.C. What will 5G be? *IEEE J. Sel. Areas Commun.* **2014**, *32*, 1065–1082. [CrossRef]

4. Huang, X.; Yu, R.; Kang, J.; He, Y.; Zhang, Y. Exploring mobile edge computing for 5G-enabled software defined vehicular networks. *IEEE Wirel. Commun.* **2017**, *24*, 55–63. [CrossRef]
5. Shah, S.A.A.; Ahmed, E.; Imran, M.; Zeadally, S. 5G for vehicular communications. *IEEE Commun. Mag.* **2018**, *56*, 111–117. [CrossRef]
6. Sheikh, M.S.; Liang, J.; Wang, W. A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets). *Sensors* **2019**, *19*, 3589. [CrossRef]
7. Eiza, M.H.; Ni, Q.; Shi, Q. Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks. *IEEE Trans. Veh. Technol.* **2016**, *65*, 7868–7881. [CrossRef]
8. Bellalta, B.; Belyaev, E.; Jonsson, M.; Vinel, A. Performance evaluation of IEEE 802.11 p-enabled vehicular video surveillance system. *IEEE Commun. Lett.* **2014**, *18*, 708–711. [CrossRef]
9. Vijayakumar, P.; Azees, M.; Chang, V.; Deborah, J.; Balusamy, B. Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks. *Clust. Comput.* **2017**, *20*, 2439–2450. [CrossRef]
10. Tehrani, M.N.; Uysal, M.; Yanikomeroglu, H. Device-to-device communication in 5G cellular networks: Challenges, solutions, and future directions. *IEEE Commun. Mag.* **2014**, *52*, 86–92. [CrossRef]
11. Shen, X. Device-to-device communication in 5G cellular networks. *IEEE Netw.* **2015**, *29*, 2–3. [CrossRef]
12. Cincilla, P.; Hicham, O.; Charles, B. Vehicular PKI Scalability-consistency Trade-offs in Large Scale Distributed Scenarios. In Proceedings of the 2016 IEEE Vehicular Networking Conference (VNC), Columbus, OH, USA, 8–10 December 2016; pp. 1–8.
13. Huang, D.; Misra, S.; Verma, M.; Xue, G. PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs. *IEEE Trans. Intell. Transp. Syst.* **2011**, *12*, 736–746. [CrossRef]
14. Joshi, A.; Gaonkar, P.; Bapat, J. A Reliable and Secure Approach for Efficient Car-to-Car Communication in Intelligent Transportation Systems. In Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 22–24 March 2017; pp. 1617–1620.
15. Lu, R.; Lin, X.; Luan, T.H.; Liang, X.; Shen, X. Pseudonym changing at social spots: An effective strategy for location privacy in vanets. *IEEE Trans. Veh. Technol.* **2011**, *61*, 86–96. [CrossRef]
16. Thenmozhi, T.; Somasundaram, R. Pseudonyms based blind signature approach for an improved secured communication at social spots in VANETs. *Wirel. Pers. Commun.* **2015**, *82*, 643–658. [CrossRef]
17. Rajput, U.; Abbas, F.; Oh, H. A hierarchical privacy preserving pseudonymous authentication protocol for VANET. *IEEE Access* **2016**, *4*, 7770–7784. [CrossRef]
18. Asghar, M.; Doss, R.R.M.; Pan, L. A Scalable and Efficient PKI based Authentication Protocol for VANETs. In Proceedings of the 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), Sydney, NSW, Australia, 21–23 November 2018; pp. 1–3.
19. Förster, D.; Kargl, F.; Löhr, H. PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET). In Proceedings of the 2014 IEEE Vehicular Networking Conference (VNC), Paderborn, Germany, 3–5 December 2014; pp. 25–32.
20. Sun, Y.; Zhang, B.; Zhao, B.; Su, X.; Su, J. Mix-zones optimal deployment for protecting location privacy in VANET. *Peer-to-Peer Netw. Appl.* **2015**, *8*, 1108–1121. [CrossRef]
21. Shao, J.; Lin, X.; Lu, R.; Zuo, C. A Threshold Anonymous Authentication Protocol for VANETs. *IEEE Trans. Veh. Technol.* **2015**, *65*, 1711–1720. [CrossRef]
22. Alimohammadi, M.; Pouyan, A.A. Sybil attack detection using a low cost short group signature in VANET. In Proceedings of the 2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC), Rasht, Iran, 8–10 Septembe 2015; pp. 23–28.
23. Zhang, L.; Wu, Q.; Qin, B.; Domingo-Ferrer, J.; Liu, B. Practical secure and privacy-preserving scheme for value-added applications in VANETs. *Comput. Commun.* **2015**, *71*, 50–60. [CrossRef]
24. Lim, K.; Tuladhar, K.M.; Wang, X.; Liu, W. A scalable and secure key distribution scheme for group signature based authentication in VANET. In Proceedings of the 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, USA, 19–21 October 2017; pp. 478–483.
25. Zhong, H.; Han, S.; Cui, J.; Zhang, J.; Xu, Y. Privacy-preserving authentication scheme with full aggregation in VANET. *Inf. Sci.* **2019**, *476*, 211–221. [CrossRef]
26. Azees, M.; Vijayakumar, P.; Deboarh, L.J. EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2467–2476. [CrossRef]
27. Zhang, L.; Wu, Q.; Domingo-Ferrer, J.; Qin, B.; Hu, C. Distributed aggregate privacy-preserving authentication in VANETs. *IEEE Trans. Intell. Transp. Syst.* **2016**, *18*, 516–526. [CrossRef]
28. Pournaghi, S.M.; Zahednejad, B.; Bayat, M.; Farjami, Y. NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET. *Comput. Netw.* **2018**, *134*, 78–92. [CrossRef]
29. Bayat, M.; Barmshoory, M.; Pournaghi, S.M.; Rahimi, M.; Farjami, Y.; Aref, M.R. A new and efficient authentication scheme for vehicular ad hoc networks. *J. Intell. Transp. Syst.* **2020**, *24*, 171–183. [CrossRef]
30. Bayat, M.; Pournaghi, M.; Rahimi, M.; Barmshoory, M. NERA: A New and Efficient RSU based Authentication Scheme for VANETs. *Wirel. Netw.* **2019**, *26*, 3083–3098. [CrossRef]
31. Asaar, M.R.; Salmasizadeh, M.; Susilo, W.; Majidi, A. A secure and efficient authentication technique for vehicular ad-hoc networks. *IEEE Trans. Veh. Technol.* **2018**, *67*, 5409–5423. [CrossRef]

32. Li, J.; Choo, K.K.R.; Zhang, W.; Kumari, S.; Rodrigues, J.J.; Khan, M.K.; Hogrefe, D. EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *Veh. Commun.* **2018**, *13*, 104–113. [CrossRef]
33. He, D.; Zeadally, S.; Xu, B.; Huang, X. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2681–2691. [CrossRef]
34. Alshudukhi, J.S.; Mohammed, B.A.; Al-Mekhlafi, Z.G. Conditional Privacy-Preserving Authentication Scheme Without Using Point Multiplication Operations Based on Elliptic Curve Cryptography (ECC). *IEEE Access* **2020**, *8*, 222032–222040. [CrossRef]
35. Alazzawi, M.; Lu, H.; Yassin, A.; Chen, K. Efficient Conditional Anonymity with Message Integrity and Authentication in a Vehicular Ad hoc Network. *IEEE Access* **2019**, *7*, 71424–71435. [CrossRef]
36. Zhang, J.; Cui, J.; Zhong, H.; Chen, Z.; Liu, L. PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 722–735. [CrossRef]
37. Alshudukhi, J.S.; Al-Mekhlafi, Z.G.; Mohammed, B.A. A Lightweight Authentication With Privacy-Preserving Scheme for Vehicular Ad Hoc Networks Based on Elliptic Curve Cryptography. *IEEE Access* **2021**, *9*, 15633–15642. [CrossRef]
38. Cui, J.; Chen, J.; Zhong, H.; Zhang, J.; Liu, L. Reliable and Efficient Content Sharing for 5G-Enabled Vehicular Networks. *IEEE Trans. Intell. Transp. Syst.* **2020**, 1–13. [CrossRef]
39. Cui, J.; Zhang, X.; Zhong, H.; Ying, Z.; Liu, L. RSMA: Reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks. *IEEE Internet Things J.* **2019**, *6*, 6417–6428. [CrossRef]
40. Al-Shareeda, M.A.; Anbar, M.; Hasbullah, I.H.; Manickam, S.; Hanshi, S.M. Efficient conditional privacy preservation with mutual authentication in vehicular ad hoc networks. *IEEE Access* **2020**, *8*, 144957–144968. [CrossRef]
41. Alazzawi, M.A.; Chen, K.; Yassin, A.A.; Lu, H.; Abedi, F. Authentication and revocation scheme for VANETs based on Chinese remainder theorem. In Proceedings of the 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Zhangjiajie, China, 10–12 August 2019; pp. 1541–1547.
42. Vijayakumar, P.; Bose, S.; Kannan, A. Chinese remainder theorem based centralised group key management for secure multicast communication. *IET Inf. Secur.* **2014**, *8*, 179–187. [CrossRef]
43. Zheng, X.; Huang, C.T.; Matthews, M. Chinese remainder theorem based group key management. In Proceedings of the 45th Annual Southeast Regional Conference, Winston-Salem, NC, USA, 23–24 March 2007; pp. 266–271.
44. Miller, V. Use of Elliptic Curves in Cryptography. In Proceedings of the Conference on the Theory and Application of Cryptographic Techniques, Santa Barbara, CA, USA, 18–22 August 1985; pp. 417–426.
45. Pointcheval, D.; Stern, J. Security arguments for digital signatures and blind signatures. *J. Cryptol.* **2000**, *13*, 361–396. [CrossRef]
46. Raya, M.; Hubaux, J.P. Securing vehicular ad hoc networks. *J. Comput. Secur.* **2007**, *15*, 39–68. [CrossRef]