electronics

MDPI

Article

A Lightweight, Efficient, and Physically Secure Key Agreement Authentication Protocol for Vehicular Networks

Shaoqiang Wang [1], Ziyao Fan [1], Yu Su [1], Baosen Zheng [1], Zhaoyuan Liu [1] and Yinfei Dai [2,*]

[1] College of Computer Science and Technology, Changchun University, Changchun 130022, China; wangsq@ccu.edu.cn (S.W.); 221501462@mails.ccu.edu.cn (Z.F.); 231502528@mails.ccu.edu.cn (Y.S.); 220701266@mails.ccu.edu.cn (B.Z.); 221501485@mails.ccu.edu.cn (Z.L.)
[2] College of Computer Science and Technology, Jilin University, Changchun 130022, China
* Correspondence: daiyf23@mails.jlu.edu.cn

Abstract: In the contemporary era, Vehicular Ad Hoc Networks (VANETs) have emerged as a vital technology in intelligent transportation systems, substantially enhancing the overall travel experience by providing advanced services to vehicles while ensuring driver safety. Despite the notable improvements, the inherent complexity of VANETs presents persistent security challenges, encompassing issues such as privacy preservation for vehicles, message authentication, and constraints in computational power and network bandwidth. Various authentication protocols have been designed for VANETs. However, many of these protocols exhibit significant vulnerabilities, rendering them insecure and unreliable in the face of diverse security threats, such as denial of service, replay, forgery, and impersonation attacks. Moreover, some existing schemes encounter limitations, including high computational complexity and the introduction of additional communication overhead and computational costs. To tackle these concerns, we designed a lightweight and secure identity authentication protocol based on elliptic curve cryptography with the objective of furnishing an effective and secure data transmission mechanism across a public communication channel for the Internet of Vehicles. In addition, we introduce Physically Unclonable Functions (PUFs) to ensure physical layer security during the communication process. A detailed security analysis demonstrates that the proposed protocol is resilient against various attacks. Through a comparative analysis with existing relevant protocols, in scenarios with a high density of vehicles, the algorithm demonstrates significantly lower computational costs and communication overhead than the related protocols, indicating that the proposed protocol is lightweight and efficient. Consequently, the empirical findings indicate that our protocol surpasses others in terms of reliability, user convenience, and practicality for ensuring secure data transmission within VANETs.

Keywords: authentication; privacy preserving; elliptic curve cryptography (ECC); security; vehicular ad hoc networks (VANETs)

Citation: Wang, S.; Fan, Z.; Su, Y.; Zheng, B.; Liu, Z.; Dai, Y. A Lightweight, Efficient, and Physically Secure Key Agreement Authentication Protocol for Vehicular Networks. *Electronics* **2024**, *13*, 1418. https://doi.org/10.3390/electronics13081418

Academic Editor: Dongkyun Kim

Received: 20 March 2024
Revised: 1 April 2024
Accepted: 6 April 2024
Published: 9 April 2024

1. Introduction

With the rapid development of technology, Vehicular Ad Hoc Network (VANET) technology has emerged as a revolutionary advancement in the modern automotive industry. By closely integrating vehicles with the internet, VANETs provide drivers with unparalleled experiences of intelligence, convenience, and safety. Obviously, with the increasing number of vehicles in urban areas [1,2], intelligent transportation systems have been playing a crucial role in urban traffic management, to the extent that support from VANETs has become a vital pillar in ensuring road safety [3]. Hence, VANETs have garnered significant attention from both industry and academia [4].

In Vehicular Ad Hoc Networks (VANETs), the On-Board Units (OBUs) serve as a tamper-resistant device installed in vehicles, capable of storing critical vehicle information such as identity and certain cryptographic computations. Additionally, the system involves

a Trusted Authority (TA) and numerous Road Side Units (RSUs). RSUs are positioned along the roadside, serving as communication bridges between the TA and vehicles. The TA is tasked with registering both RSUs and vehicles, as well as providing necessary communication assistance. Within VANETs, two communication modes exist: Vehicle-to-Vehicle (V2V), where vehicles in motion can communicate with each other, and Vehicle-to-Infrastructure (V2I), enabling communication between moving vehicles and roadside infrastructure. Both of these modes can utilize the Dedicated Short-Range Communication (DSRC) standard [5,6], operating over open wireless communication channels. Due to the fact that V2V and V2I communications take place over open wireless communication channels, they are vulnerable to a variety of attacks, including interference, eavesdropping, and spoofing [7]. This reality not only exposes potential threats to information exchange between vehicles but also underscores the urgency of identity authentication in VANETs. Additionally, by employing side-channel attacks [8], partial information stored in the On-Board Units can be obtained, leading to privacy leakage in vehicles.

In this era of information, vehicles are no longer standalone entities but are interconnected within the expansive realm of cyberspace. This integration renders VANET security highly susceptible to network threats like identity theft, unauthorized access, and malicious attacks, all of which can severely impact its safety. Therefore, ensuring the security of both vehicles and their user identities is of paramount importance. As a crucial component in ensuring the security of VANET systems, the identity authentication mechanism enables the straightforward identification of all authenticated vehicles [9,10]. Simultaneously, the identity authentication mechanism must strike a delicate balance between convenience and security to ensure the protection of users' privacy rights.

The central research contributions of this paper are delineated as follows:

- We propose an improved, lightweight identity authentication protocol with conditional privacy protection suitable for VANETs. Leveraging elliptic curve cryptography, the protocol ensures a balance between lightweight characteristics, security, and privacy through lightweight encryption operations such as hash functions, concatenation, XOR, and PUF technology.
- We conducted in-depth formal and informal analyses of the security attributes of the proposed protocol. Formal verification was achieved through Burrows-Abadi-Needham (BAN) logic proof and the Real-Or-Random (ROR) model to demonstrate the protocol's resistance to security threats. Additionally, we showcased the security resilience of the proposed protocol against relevant attacks.
- We conducted a performance analysis of existing authentication schemes [11–15], demonstrating that the proposed scheme outperforms others in various aspects, such as communication cost and computational cost, in most cases.
- We conducted simulation and emulation of the proposed protocol using discrete event simulators OMNeT++ 5.6.2 and Simulation of Urban Mobility 1.8.0 (SUMO), an open-source traffic simulation software, to illustrate its practical feasibility in real-world scenarios.

The remaining sections of this paper are structured as follows. Section 2 presents relevant research on VANET identity authentication. Section 3 introduces some fundamental knowledge related to the proposed protocol. The specific protocol process is outlined in Section 4. Section 5 showcases the security analysis and protective mechanisms of the proposed protocol, while Section 6 analyzes and verifies the performance of the scheme through simulation. Finally, conclusions are drawn in Section 7, along with prospects for future research in VANET security.

2. Related Studies

In this section, we will discuss the existing authentication schemes for VANETs. Each authentication approach utilizes distinct communication modes and cryptographic principles, resulting in varying degrees of security and performance. In 2008, Lu et al. [16] introduced the concept of conditional privacy security, aiming to protect the privacy of

OBUs from attackers while preventing malicious OBUs from interfering with normal communication. The general public cannot track OBUs, but the Trusted Authority (TA) has the capability to identify the real identities of exposed OBUs. In the same year, Zhang et al. [17] proposed an identity-based authentication method with conditional privacy, which eliminates the requirement for certificates between RSUs and vehicles. The following year, Zhang et al. [18] designed a novel key management protocol aimed at ensuring the security of VANET communications. Nevertheless, Lee et al. [19] later found that the scheme proposed by Zhang et al. [18] was vulnerable to threats like denial-of-service and replay attacks. Additionally, Lee et al. [19] proposed a more secure and scalable protocol based on bilinear pairing. In 2015, He et al. [20] proposed an identity-based authentication method for VANETs, eliminating the need for bilinear pairing and thereby reducing processing costs. Following He et al.'s approach [20], subsequent modifications [21,22] were proposed to further enhance performance. Lo and Tsai [23] introduced a pairing-free authentication method in 2016 to maintain computational complexity. Dua et al. [24] introduced a two-tier identity authentication protocol utilizing elliptic curve cryptography (ECC), aiming at safeguarding the security of vehicle communication in intelligent transportation systems. However, it is unable to defend against cluster head impersonation attacks, where any registered yet dishonest cluster head can manipulate regular vehicles. Li et al. [25] introduced an identity authentication scheme for UAV networks based on elliptic curve cryptography. Their design encompasses three stages: ECC certificate generation, identity authentication, and key compatibility verification. However, their scheme led to substantial computational costs. Bagga et al. [26] proposed a novel bidirectional identity authentication and key agreement protocol aimed at enhancing the security, anonymity, and resilience of VANETs within intelligent transportation systems. The proposed method achieves low communication and computational overhead, along with higher security. Additionally, due to its lower throughput, it is suitable for networks in sparsely populated areas. Yang et al. [27] devised a certificateless key establishment protocol based on elliptic curve cryptography to address the key escrow problem in traditional identity-based cryptography (IBC) protocols. However, their protocol is susceptible to physical/cloning attacks. In 2020, Li et al. [28] introduced a lightweight key agreement scheme based on hashing. However, Shamshad et al. [29] conducted an evaluation of their study, uncovering that the scheme [28] lacks guarantees of untraceability and anonymity and is vulnerable to threats like impersonation and RSU key leakage attacks. In the same year, Alshudukhi et al. [30] developed an identity verification technique that supports privacy factors, countering potential side-channel attacks by regularly updating the Tamper-proof Device (TPD). Similarly, Cui et al. [31] also opted for regularly updating information to resist side-channel attacks, ensuring vehicles complete identity authentication securely. Aman et al. [32] introduced a VANET authentication scheme based on physical unclonable functions to minimize costs and network traffic while protecting the network against clone attacks. In order to minimize authentication overhead and improve network throughput, the network is organized into three tiers: roadside units, roadside unit gateways, and trusted authorities. Simulation results demonstrate a significant reduction in MAC/PHY overhead and enhanced security against various attacks. While the scheme achieves lower throughput and bandwidth requirements, it may not be suitable for densely populated areas. Gope et al. [33] introduced a lightweight, privacy-preserving dual-factor authentication scheme for IoT devices utilizing physical unclonable functions. However, due to their oversight of message loss during transmission, their scheme is susceptible to desynchronization attacks [34]. Kudva et al. [35] introduced an approach to enhance VANET security during vehicle-to-vehicle and vehicle-to-infrastructure communication. They implemented a secure AODV protocol to safeguard the network against black hole attacks in the event of network failures. Additionally, the scheme employs cryptographic function-based encryption and decryption methods to achieve better performance. This approach has demonstrated improved performance in terms of packet delivery ratio, packet loss rate, latency, and overhead, but it has not achieved high throughput. Son et al. [36] proposed a blockchain-based authentication

framework considering handover for V2I communication. However, the paper lacks a clear explanation regarding the storage or calculation of certain parameters, and the method may be susceptible to smart contract capture and dictionary attacks if vehicle verification can be bypassed to initiate authentication. Feng et al. [37] introduced an efficient privacy-preserving authentication model leveraging blockchain technology. They extended its architecture to safeguard and streamline authentication processes within vehicular ad hoc networks. This model supports member identity verification and optimizes time utilization by circumventing verification through certificate revocation lists. Ahmed et al. [38] also proposed a blockchain-based authentication protocol for VANET. This protocol is adept at mitigating diverse attacks while concurrently reducing the computational overhead and storage footprint associated with authentication messages. Tandon et al. [39] introduced a decentralized architecture based on dual blockchains for vehicle authentication and secure, efficient communication within the network. This approach employs separate blockchains for identity verification, message sharing, and enhancing network efficiency, responsiveness, and security.

3. Preliminary

3.1. VANET Architecture

Vehicular Ad Hoc Network (VANET) is a special form of Mobile Ad Hoc Network (MANET), involving communication between vehicles and between vehicles and roadside infrastructure. The architecture of VANETs (as illustrated in Figure 1) typically consists of several key components:

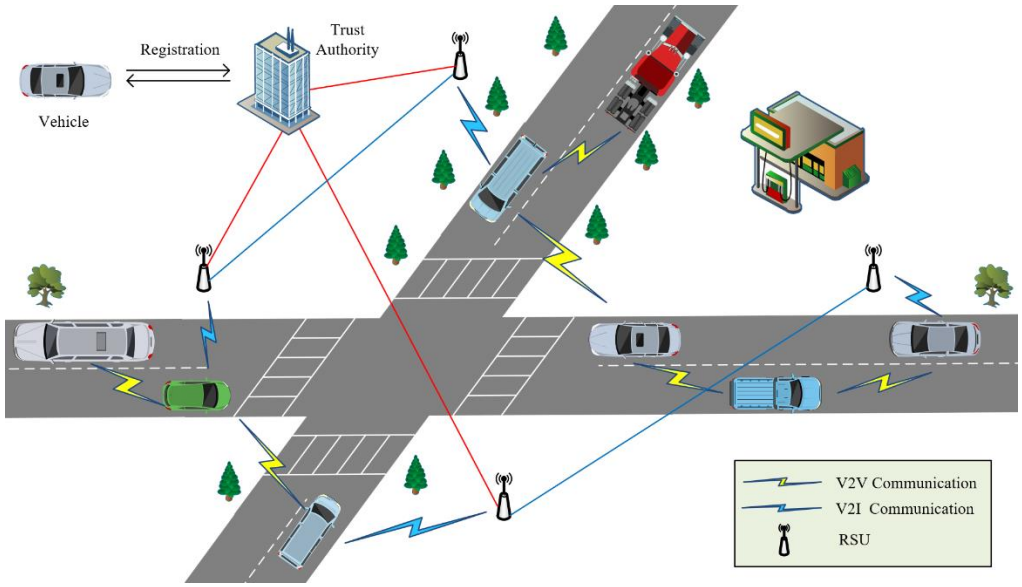

Figure 1. The system structure of the VANET.

On-Board Units (OBUs): On-Board Units are integral components of vehicular ad hoc networks (VANETs). They are dedicated communication devices installed in vehicles to facilitate communication between vehicles and between vehicles and roadside infrastructure. Numerous OBUs employ DSRC technology, functioning within the 5.9 GHz frequency band. Furthermore, certain OBUs may utilize cellular networks like 4G and 5G for communication. Typically, OBUs integrate sensors like GPS, accelerometers, and gyroscopes to furnish vehicle-related data. It is important to highlight that OBUs play a vital role in ensuring the security and privacy of communication within VANETs. They are responsible for implementing encryption and authentication mechanisms to prevent unauthorized access and malicious activities.

Road Side Units (RSUs): Roadside Units are infrastructure components within VANETs, typically strategically deployed along roadways, intersections, and other locations to provide optimal communication coverage. RSUs are outfitted with network equipment utilizing short-range wireless communication standards like IEEE 802.11p [40]. This enables them to establish wireless connections with OBUs installed in vehicles. RSUs efficiently gather and distribute real-time information regarding traffic conditions, road hazards, and other pertinent data to vehicles. This facilitates the enhancement of traffic signal timing, traffic flow management, and the alleviation of roadway congestion.

Trusted Authority (TA): In the context of vehicular ad hoc network communication systems, the Trusted Authority is the entity responsible for managing and implementing network security, often regarded as the highest authority within VANETs. Its role is vital in ensuring the authenticity, integrity, and confidentiality of communication between vehicles and between vehicles and infrastructure components. Furthermore, the TA can engage in partnerships with other stakeholders, such as government bodies, industry institutions, and network operators, to foster a secure and reliable environment for VANET communication. The TA is generally regarded as entirely trustworthy and impervious to attacks.

3.2. Threat Models

Threat modeling, as a crucial process for identifying and analyzing potential security risks and vulnerabilities, holds unparalleled significance in the development of open network protocols like VANETs. By conducting threat modeling, effective planning and implementation of corresponding security controls and strategies can be achieved, ensuring the resilience and reliability of VANET systems. In this paper, we will employ commonly used threat models, such as the Dolev-Yao (DY) threat model [41] and the Canetti-Krawczyk (CK) adversarial model [42], to describe the capabilities of adversaries. The DY model offers a simplified and abstract framework for assessing the security of encryption protocols, delineating adversaries' capabilities in accessing communication channels. The CK model introduces a more realistic and computationally feasible adversary model, taking into account attackers' polynomial-time computational constraints. This makes it more suitable for analyzing practical systems and key exchange protocols. Hence, we assume that adversary $\mathcal{A}$ possesses the following capabilities:

- Adversary $\mathcal{A}$ is capable of freely accessing any message transmitted over the public communication channel and can modify, delete, intercept, and replay messages at will.
- $\mathcal{A}$ is cognizant of the public identities of all protocol participants, and the identity of TA is publicly known.
- $\mathcal{A}$ can be either an insider or an outsider. Any registered or unregistered vehicle could potentially be adversary $\mathcal{A}$.
- During the session key establishment process, adversary $\mathcal{A}$ can steal and compromise session states for partial secret information stored in insecure storage within OBUs.
- $\mathcal{A}$ has sufficient computational power to conduct exhaustive guessing attacks within polynomial time.

3.3. System Network Model and Assumptions

In this section, we present the fundamental network model and assumptions of the proposed protocol. The VANET network model utilized in this paper is depicted in Figure 2. The Trusted Authority (TA) is deemed entirely reliable, boasting ample computational capabilities and storage capacity. Vehicles are outfitted with tamper-resistant On-Board Units (OBUs) designed to store sensitive data and conduct associated computations. However, compared to TA, their computational power and storage space are extremely limited. In this network model, the protocol operates at two communication levels: one at the server level and the other at the vehicle level. At the server level, which operates within a secure channel, the Trusted Authority (TA) resides. It stores detailed information about registered vehicles and partial credentials. Additionally, it performs initialization and registration operations for vehicles, allowing them to obtain relevant authentication pa-

rameters. The TA supports elements at the vehicle level and assists authenticated vehicles in identifying the legitimate identities of other vehicles during the authentication process. At the vehicle level, communication between vehicles occurs using DSRC for information exchange and authentication processes. This layer operates within a non-secure public channel. In the event of an OBU malfunction in a vehicle, rendering it unable to broadcast evacuation information, other vehicles can serve as relay nodes to ensure uninterrupted communication. This means that the malfunction or evacuation of a single vehicle does not disrupt communication across the entire network, thereby guaranteeing the stability of authentication communication at the vehicle level.

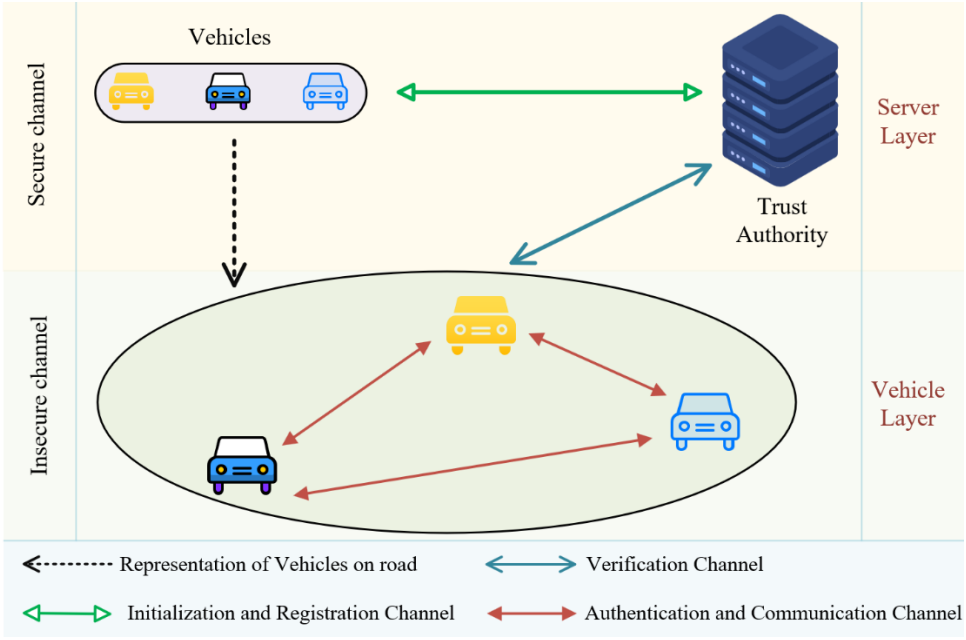

Figure 2. Network model.

3.4. Physical Unclonable Function

The Physical Unclonable Function (PUF) is a hardware-based security technology that relies on the microscopic irregularities and physical characteristics of hardware devices to generate unique identifiers. PUF generally functions using a challenge–response mechanism. When presented with a challenge C_x, the PUF generates a distinct response R_x based on its physical traits. This response serves as a unique identifier for the device. Due to the inherent irregularities in the hardware manufacturing process, even devices of the same model exhibit slight variations in their physical characteristics. This uniqueness makes PUF responses unclonable, meaning identical hardware models cannot generate the same response. As a result, the security of the system is enhanced. An ideal PUF would provide various features, such as reliability, unpredictability, and uniqueness, effectively safeguarding sensing devices against side-channel attacks [43], cloning attempts, and tampering threats [11]. PUF systems typically exhibit the ability to handle diversity in challenging situations. Even if the same challenge is issued multiple times, variations in environmental conditions or device noise cause the PUF-generated responses to differ. If the following conditions are met, a PUF can be considered $(d,\ n,\ l,\ \lambda,\ \varepsilon)$-secure [44]:

- For any two Physical Unclonable Functions, $PUF_1(\cdot)$ and $PUF_2(\cdot)$, and for any input $C_1 \in \{0,\ 1\}^k$, $PR[H_d(PUF_1(C_1),\ (PUF_2(C_1)) > d] \geq 1 - \varepsilon$ holds, where H_d represents the Hamming distance.
- For any $PUF_i(\cdot)$ and any input $C_1,\ C_2,\ C_3,\ \cdots,\ C_n \in \{0,\ 1\}^k$, $PR[H_d(PUF_i(C_1),\ (PUF_i(C_2)) > d] \geq 1 - \varepsilon$ holds.

- For any $PUF_i(\cdot)$ and any input $C_1, C_2, C_3, \cdots, C_n \in \{0, 1\}^k$, $PR[H_\infty(PUF_i(C_p), PUF_j(C_q))_{1 \le p, q \le n,\ i \ne j,\ p \ne q} > \lambda] \ge 1 - \varepsilon$ holds. This condition states that when multiple inputs are used to evaluate different PUFs, the minimum entropy of the PUF outputs must be greater than λ with high probability [45]. Here, ε represents the error rate, λ represents the message length, and C_p, C_q represents two different challenge messages.

3.5. Notation Table

The notations used in this paper and their corresponding explanations are shown in Notation table in Abbreviations section below.

4. Discussion

In this section, we will provide a detailed explanation of the proposed identity authentication protocol, which involves two entities: vehicles and the trusted authority. The protocol is divided into four main phases: initialization, registration, authentication, and communication. In the initialization and registration phases, communication between entities occurs via dedicated channels, while in the authentication phase, communication takes place over non-secure channels. Descriptions of each phase will be provided in subsequent sections.

4.1. Initialization Phase

During this phase, relevant parameters will be generated and sent to the vehicles, laying the foundation for subsequent authentication communications in the protocol. Communication during the initialization setup process will be carried out over a secure channel. The steps in this phase are as follows:

First, TA selects an elliptic curve E over a finite field F_p and determines a suitably sized prime number P and generator G. TA selects a random number $k_t (k_t \in F_p)$ over the chosen finite field F_p. This random number will serve as the server's private key. Then, TA performs scalar multiplication on the random number k_t and the generator point G over the elliptic curve E, denoting the result as PK_t, which serves as the server's public key, namely, $PK_t = k_t * G$. TA selects two one-way hash functions, denoted as $h_i(\cdot)\ (i = 1, 2)$, where $h_1(x) = \{m\}\ (x\ is\ value,\ m \in F_p)$ and $h_2(\cdot): \{1,0\}^* \to \{1,0\}^{\ln}$. Additionally, TA elects a secure symmetric encryption algorithm such as the AES algorithm. Finally, TA stores its own public–private key pair and distributes $\{E, F_p, PK_t, h_i(\cdot)\}$ to all participating vehicles in the protocol.

4.2. Registration Phase

During this phase, all vehicles participating in the protocol need to undergo initial registration at the TA. Over a secure channel, communication for the entire registration process will be conducted, as this phase involves handling sensitive information that will be utilized for authentication purposes in the future. The registration process details are depicted in Figure 3.

After receiving the challenge message C_x from the TA, vehicle V_x computes $R_x = PUF(C_x)$ to generate the response message, which is embedded in the OBU of vehicle V_x. Following this, vehicle V_x proceeds by selecting a random number $n_x \in Z_p^*$ and subsequently storing it within OBU. The vehicle's identity $ID_x = h_2(R_x \parallel n_x)$ is derived by calculating the hash value of the concatenation of the response and the random number. Afterward, the vehicle V_x transmits message $M_1 = \{ID_x, R_x\}$ to the TA. Upon reception of message M_1, the TA saves the challenge–response pair $< C_x, R_x >$ associated with vehicle V_x into the database and, subsequently, elects another random number $n_{tx} \in Z_p^*$ to function as a temporary key. Afterwards, computations are executed to derive $\alpha_x = h_2(ID_x \parallel k_t)$ and $SID_x = Enc_{k_t}(n_{tx} \parallel ID_x)$, which will be used for the subsequent authentication and serve as pseudo-identity for vehicle V_x, respectively. The pseudo-identity SID_x will be stored in the TA's database. Then, the TA will calculate $Y_{V_x} = n_{tx} * G$ and $Z_{V_x} = \alpha_x * k_t + n_{tx}$ for

constructing the session key. Ultimately, the pertinent information is encapsulated within message $M_2 = \{\alpha_x, SID_x, Y_{V_x}, Z_{V_x}\}$ and dispatched to vehicle V_x, whereupon it is stored after receipt.

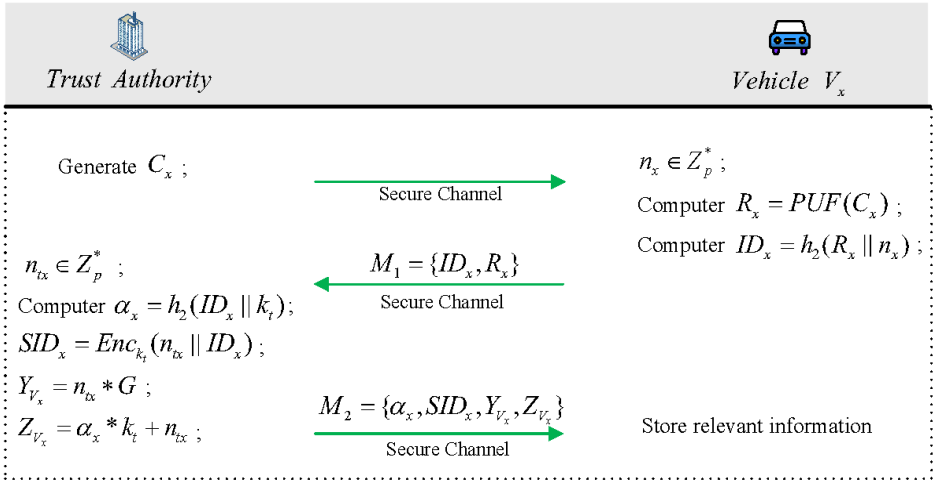

Figure 3. Registration phase.

4.3. Authentication Phase

During this phase, vehicles authenticate each other to ensure secure communication for subsequent exchanges. During the authentication phase, vehicles can verify each other's identities using both insecure and secure channels. Secure channel communication is exclusively utilized when vehicles verify each other's identities with the *TA*, while other communications can occur over insecure channels, enabling *V2V* communication by DSRC mode over the public channel. Figure 4 provides a detailed illustration of this phase.

1. The vehicle V_A selects a random integer $r_A \in Z_p^*$ and calculates the following values $Q_A = r_A * G$, $A_1 = ID_A \oplus r_A$, and $A_2 = h_2(ID_A \parallel SID_A \parallel \alpha_A \parallel r_A)$. Then obtain the current timestamp T_{IA}^1 and calculate $A_3 = (r_A \oplus T_{IA}^1) \parallel C_A$. Finally, obtain the current timestamp T_{OA}^1 again and send the messages $M_3 = \{A_1, A_2, A_3, SID_A, T_{OA}^1\}$ and $M_4 = \{SID_A, Q_A, Y_{V_A}, \alpha_A, T_{OA}^1\}$ to vehicle V_B.
2. Vehicle V_B, upon receiving messages M_3 and M_4, obtains the current timestamp T_{OB}^1 and retrieves the timestamp T_{OA}^1 from the messages. Then, it calculates and verifies if the inequality $T_{OB}^1 - T_{OA}^1 < \Delta T_1$ holds. If the inequality is not satisfied, V_B terminates the authentication process. Otherwise, if the inequality holds, V_B obtains the current timestamp T_{OB}^2 and sends message $M_5 = \{A_1, A_2, A_3, SID_A, T_{OB}^2\}$ to *TA*.
3. *TA* verifies the freshness of the message, after receiving message M_5, by selecting the current timestamp T_{OT}^1 and checking whether the inequality $T_{OT}^1 - T_{OB}^2 < \Delta T_2$ holds true. If the inequality does not hold true, the authentication process is terminated. Otherwise, the *TA* proceeds to compute $Dec(SID_A) = n_{tA} \parallel ID_A$ to get the value of ID_A. Compute $r_A = A_1 \oplus ID_A$ to get the value of r_A. Then, by calculating $T_{IA}^1 = r_A \oplus (r_A \oplus T_{IA}^1)$, we can get the T_{IA}^1. After that, check if the inequality $T_{OT}^1 - T_{IA}^1 < \Delta T_3'$ holds true. It is worth noting that the time threshold $\Delta T_3'$ is slightly different from the previously used threshold ΔT_2. The former is used to determine and ensure that messages from vehicle V_A have not been intercepted or spoofed. If vehicle V_B receives a message from vehicle V_A that is forged or replayed, the internally calculated time threshold will exceed the specified range. Since this timestamp cannot be known by a third party, forging this timestamp is impossible. If the inequality $T_{OT}^1 - T_{IA}^1 < \Delta T_3'$ is not satisfied, the authentication process is terminated. However, if the inequality holds, *TA* retrieves the challenge C_A of vehicle V_A from A_3, calculates its response $R_A = PUF(C_A)$, and verifies it against the corresponding challenge–response pair $<C_A, R_A>$ stored in the database. After successful validation, a confirmation message

W_1 is generated, and then a timestamp T_{OT}^2 is acquired. Subsequently, message $M_6 = \{T_{OT}^2, W_1\}$ is transmitted to vehicle V_B.

4. After receiving message M_6, vehicle V_B retrieves the current timestamp T_{OB}^3 and verifies whether the condition $T_{OB}^3 - T_{OT}^2 < \Delta T_4$ holds true. If the inequality holds true, V_B accepts W_1 and confirms that vehicle V_A is legitimate. Afterward, vehicle V_B selects a random integer r_B($r_B \in Z_p^*$) and calculates $Q_B = r_B * G$. Then, it computes the values $\beta_B = (Q_A + Y_{V_A} + \alpha_A * PK_t) * (r_B + Z_{V_B})$ and $\gamma_B = h_1(SID_A \parallel \beta_B)$ to generate the session key $SK_B = h_1(SID_A \parallel SID_B \parallel \beta_B)$. Afterward, similar to vehicle V_A, vehicle V_B computes B_1, B_2, B_3 for the verification from vehicle V_A. The values of B_1, B_2, B_3 are as follows: $B_1 = ID_B \oplus r_B$, $B_2 = h_2(ID_B \parallel SID_B \parallel \alpha_B \parallel r_B)$, $B_3 = (r_B \oplus T_{IB}^1) \parallel C_B$. In which, the T_{IB}^1 in B_3 is the current timestamp obtained by vehicle V_B after computing B_2. Finally, vehicle V_B obtains the current timestamp T_{OB}^4 and sends messages $M_7 = \{B_1, B_2, B_3, SID_B, T_{OB}^4\}$ and $M_8 = \{Q_B, Y_{V_B}, \alpha_B, T_{OB}^4, \gamma_B, SID_B\}$ to vehicle V_A.
5. Vehicle V_A, upon receiving messages M_7, M_8, selects the current timestamp T_{OA}^2 and retrieves the timestamp T_{OB}^4 from the received messages. Then, it evaluates whether the inequality $T_{OA}^2 - T_{OB}^4 < \Delta T_5$ holds true. If the inequality does not hold true, the authentication process is terminated. If the inequality holds true, vehicle V_A obtains the current timestamp T_{OA}^3 and sends the message $M_9 = \{T_{OA}^3, B_1, B_2, B_3, SID_B\}$ to *TA*.
6. Upon receiving the message M_9, *TA* first verifies its freshness by selecting the current timestamp T_{OT}^3 and calculating whether the inequality $T_{OT}^3 - T_{OA}^3 < \Delta T_6$ holds true. If the inequality does not hold true, the authentication process is terminated. If the inequality holds true, *TA* calculates $Dec(SID_B) = n_{tB} \parallel ID_B$ to obtain the value of ID_B. Calculate $r_B = B_1 \oplus ID_B$ to obtain the value of r_B, then calculate $T_{IB}^1 = (r_B \oplus T_{IB}^1) \oplus r_B$ and determine if the inequality $T_{OT}^3 - T_{IB}^1 < \Delta T_7'$ is satisfied. If the inequality does not hold true, the authentication process is terminated. If the inequality holds true, obtain the challenge C_B from B_3, compute response $R_B = PUF(C_B)$, and compare it with the corresponding challenge–response pair stored in the database, $< C_B, R_B >$, for validation. After successful validation, a confirmation message W_2 is generated, and then a timestamp T_{OT}^4 is acquired. Subsequently, message $M_{10} = \{T_{OT}^4, W_2\}$ is transmitted to vehicle V_A.
7. After receiving message M_{10}, vehicle V_A retrieves the current timestamp T_{OA}^4 and verifies whether the condition $T_{OA}^4 - T_{OT}^4 < \Delta T_8$ holds true. If the inequality holds true, V_A accepts W_2 and confirms that vehicle V_B is legitimate. Otherwise, terminate the authentication process. Then, vehicle V_A calculates the values of $\beta_A = (Q_B + Y_{V_B} + \alpha_B * PK_t) * (r_A + Z_{V_A})$ and $\gamma_A = h_1(SID_A \parallel \beta_A)$ and verifies $\gamma_A \stackrel{?}{=} \gamma_B$. If true, compute the session key $SK_A = h_1(SID_A \parallel SID_B \parallel \beta_A)$.

Considering that $\beta_B = (Q_A + Y_{V_A} + \alpha_A * PK_t) * (r_B + Z_{V_B})$, substituting the following equations $Q_A = r_A * G$, $Y_{V_A} = n_{tA} * G$, $PK_t = k_t * G$ into β_B yields $\beta_B = (r_A * G + n_{tA} * G + \alpha_A * k_t * G) * (r_B + Z_{V_B})$. Also, since the equation $Z_{V_A} = \alpha_A * k_t + n_{tA}$, β_B can be transformed into $\beta_B = (r_A * G + Z_{V_A} * G) * (r_B + Z_{V_B})$. At this point, it can be observed that by substituting the equation $Z_{V_B} = \alpha_B * k_t + n_{tB}$ and β_B simplifies to $\beta_B = (r_A + Z_{V_A}) * [r_B * G + (n_{tB} + \alpha_B * k_t) * G]$. At this moment, it is worth noting that by substituting $Q_B = r_B * G$, $Y_{V_B} = n_{tB} * G$, and $PK_t = k_t * G$, we obtain $\beta_B = \beta_A$, namely, $\beta_B = (Q_B + Y_{V_B} + \alpha_B * PK_t) * (r_A + Z_{V_A}) = \beta_A$. Now, we have $\beta_B = \beta_A$, it can be inferred that $\gamma_A = h_1(SID_A \parallel \beta_A)$ and $\gamma_B = h_1(SID_A \parallel \beta_B)$. Thus, $\gamma_A = \gamma_B$. Also, since $SK_A = h_1(SID_A \parallel SID_B \parallel \beta_A)$ and $SK_B = h_1(SID_A \parallel SID_B \parallel \beta_B)$, it follows that $SK_A = SK_B$.

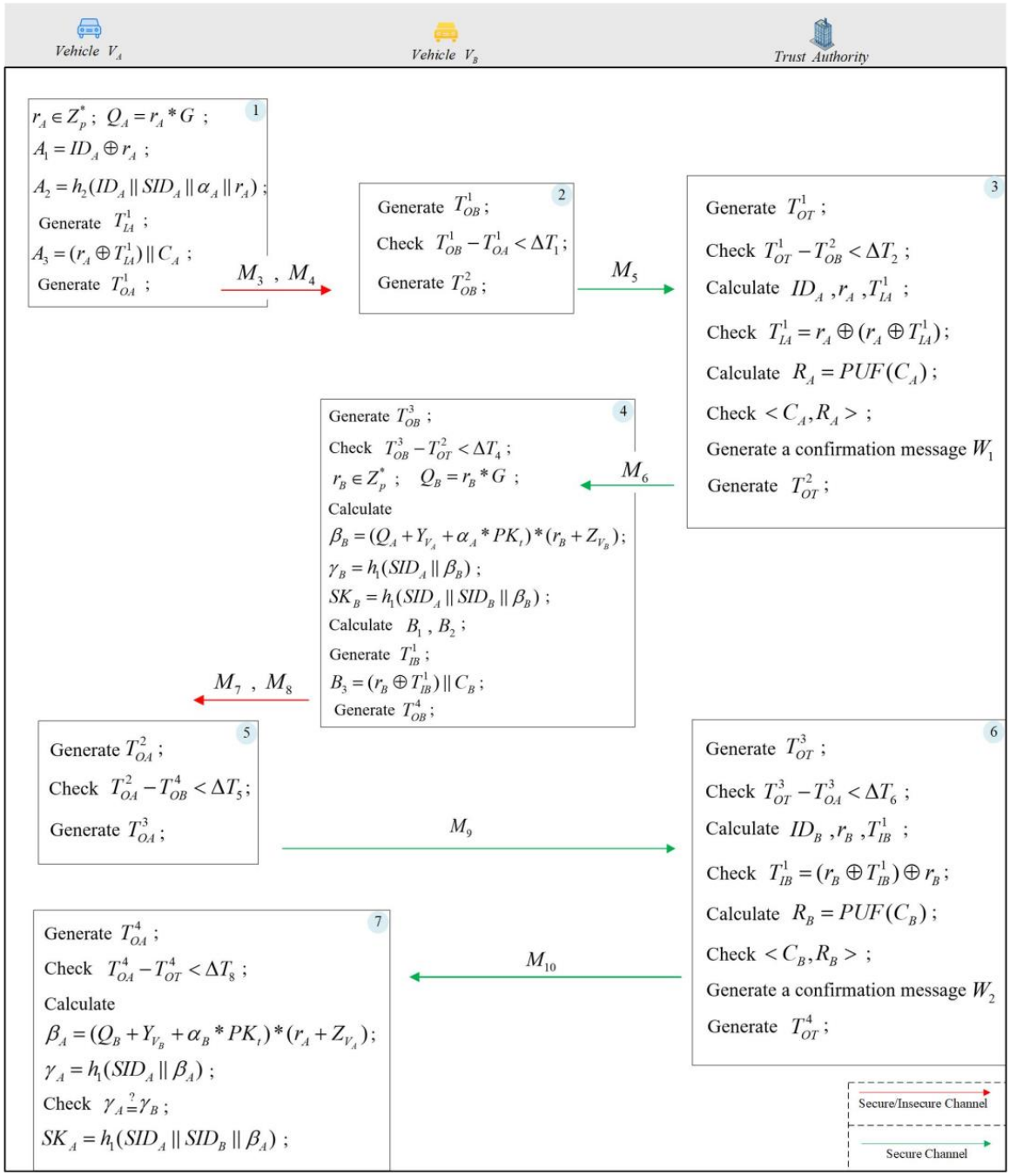

Figure 4. Authentication phase.

4.4. Communication Phase

In this phase, the vehicles have mutually authenticated each other and can communicate using the agreed-upon session key established earlier. An important point to highlight is that identity authentication among vehicles occurs solely during the initial communication exchange. Subsequent communication instances do not necessitate reauthentication. Moreover, it is noteworthy that information exchange between vehicles during the communication phase will transpire over an insecure communication channel. The detailed elucidation of the communication steps will be delineated in the subsequent section (Figure 5).

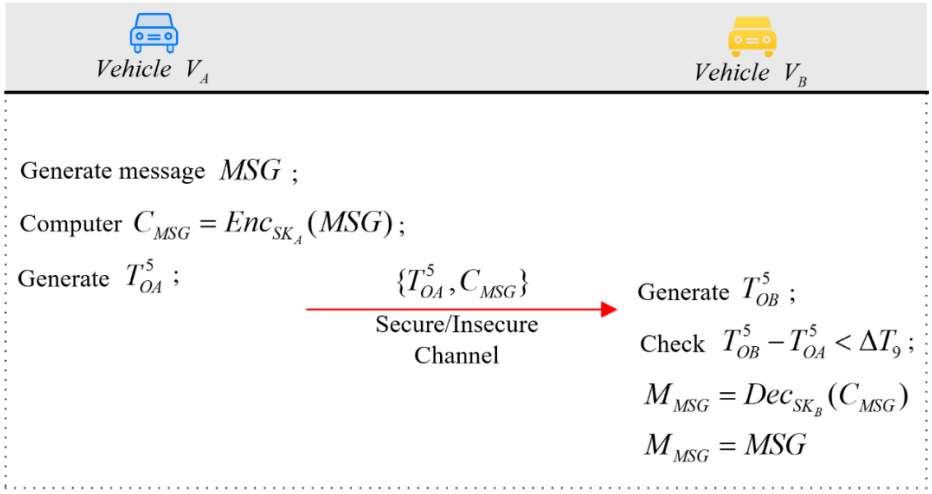

Figure 5. Communication phase.

Let MSG represent the message to be transmitted from vehicle V_A to vehicle V_B. Employing the session key SK_A, previously negotiated with vehicle V_B, vehicle V_A encrypts message MSG using symmetric encryption, yielding ciphertext $C_{MSG} = Enc_{SK_A}(MSG)$. Vehicle V_A selects the current timestamp T_{OA}^5 and combines it with the ciphertext, sending this amalgamation as the message to vehicle V_B. Upon receiving the message, vehicle V_B first generates the current timestamp T_{OB}^5 and checks if $T_{OB}^5 - T_{OA}^5 < \Delta T_9$ to ensure the legality of the message. Should the inequality prove valid, vehicle V_B proceeds to decrypt the ciphertext using SK_B to get $M_{MSG} = Dec_{SK_B}(C_{MSG})$, as the session key shared between vehicle V_B and vehicle V_A ensures mutual decryption capability, namely, $MSG = M_{MSG}$.

4.5. Information Update

The subsequent process allows vehicles to update their relevant information, such as identities, passwords, or characteristic data, due to various reasons. In this step, vehicles connect to the *TA* via a secure channel, and the values requiring updates are registered directly with the server. The detailed process (Figure 6) will be explained below.

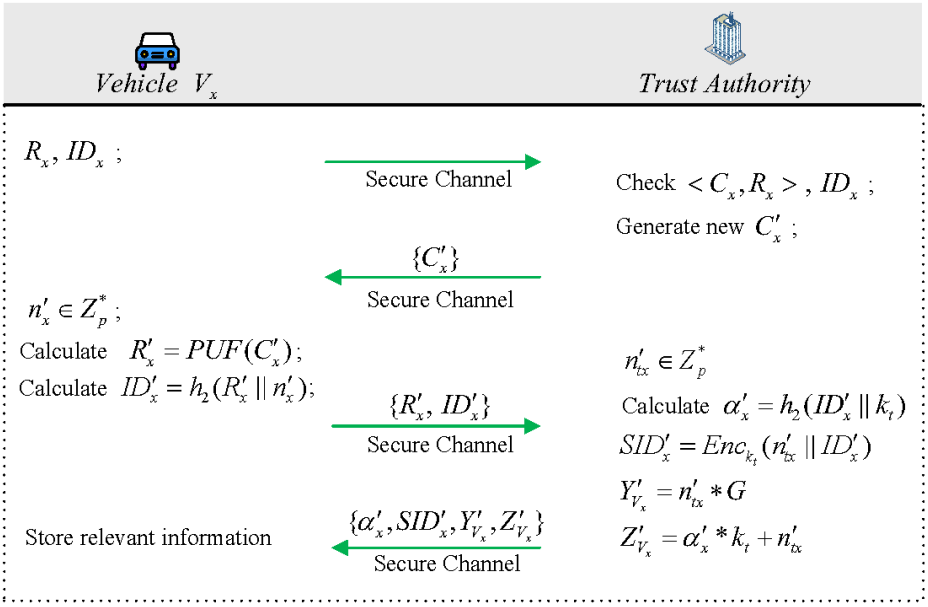

Figure 6. Vehicle password update phase.

Vehicle V_x sends its response R_x and identity ID_x to the *TA*. The *TA* compares the received challenge–response pair $< C_x, R_x >$ with its stored one and verifies the identity of the vehicle ID_x. Upon successful verification, it generates a new challenge C'_x and sends it to vehicle V_x. After receiving the challenge message, the vehicle recalculates the response $R'_x = PUF(C'_x)$, selects a new random number $n'_x \in Z^*_p$, and computes the $ID'_x = h_2(R'_x \parallel n'_x)$. Subsequently, it sends the new response and identity to the *TA*. Upon receiving the information from the vehicle, *TA* stores the new challenge–response pair and the vehicle's identity in the database. It then selects another new random number $n'_{tx} \in Z^*_p$ and recalculates the following values: $\alpha'_x = h_2(ID'_x \parallel k_t)$, $Y'_{V_x} = n'_{tx} * G$, and $Z'_{V_x} = \alpha'_x * k_t + n'_{tx}$. Afterwards, using the new random number and identity, the *TA* computes the new pseudonym $SID'_x = Enc_{k_t}(n'_{tx} \parallel ID'_x)$ for vehicle V_x. Finally, the calculated values α'_x, SID'_x, Y'_{V_x}, Z'_{V_x} are sent to vehicle V_x, which stores the new values after receiving the message.

5. Security Analysis

This section provides a detailed analysis of the security of the proposed protocol. Specific details will be elaborated on in the subsequent subsections.

5.1. Informal Security Analysis

In this section, we provide an informal security proof for the VANET authentication scheme, demonstrating its security and its ability to mitigate significant security threats as per the security objectives of the vehicular ad hoc network authentication scheme.

Vehicle Anonymity: During the authentication procedure, a vehicle V_x employs a pseudonymous identity SID_x on the public channel to obscure its actual identity ID_x. It should be emphasized that the pseudonymous identity SID_x of the vehicle, denoted as $SID_x = Enc_{k_t}(n_{tx} \parallel ID_x)$, is produced by *TA* through encryption using its private key k_t. Furthermore, apart from *TA*, no third party will know the value of k_t. Therefore, besides the vehicle V_x itself, only *TA* can access the true identity of the vehicle, while only *TA* can determine the pseudonymous identity of vehicle V_x. Additionally, the pseudonymous identity SID_x used by a vehicle may vary for the same vehicle under different circumstances. As a result, attacker $\mathcal{A}$ cannot identify or track vehicle V_x by intercepting the information transmitted by V_x on the public channel, ensuring the anonymity of the vehicle.

Resistance to Replay Attack: In this protocol, timestamps are employed in communications between entities to ensure the freshness and integrity of messages. As each message is received, a check is performed against the current timestamp, for example, $T^1_{OB} - T^1_{OA} < \Delta T_1$. If an adversary $\mathcal{A}$ attempts to eavesdrop on and impersonate any message in transit, it will fail to meet the time constraints specified in equations similar to the one above. Consequently, this protocol is resilient against replay attacks.

Mutual Authentication: The authentication between vehicles V_A and V_B is accomplished by computing a session key SK_x through negotiation. In the protocol, each communicating party computes their corresponding β_x value using self-selected random numbers and various parameters obtained during the registration stage. It is important to highlight that V_A and V_B never exchange temporary keys throughout this process. Instead, they calculate their respective β_x values using known parameters and parameters extracted from messages $M_4 = \{SID_A, Q_A, Y_{V_A}, \alpha_A, T^1_{OA}\}$ and $M_8 = \{Q_B, Y_{V_B}, \alpha_B, T^4_{OB}, \gamma_B, SID_B\}$. Subsequently, one of the entities involved in communication, vehicle V_B, needs to calculate the value of $\gamma_B = h(SID_A \parallel \beta_B)$ and send it to V_A. On the other hand, V_A also needs to compute its own value of γ_A and verify $\gamma_A \stackrel{?}{=} \gamma_B$ to ensure the security of the mutual authentication process.

Resistance to Physical Attack: Ensuring the security of the *OBU* is crucial for the entire authentication protocol, considering it is a device highly susceptible to access and tampering by attackers like $\mathcal{A}$. In this protocol, every *OBU* is equipped with a *PUF* to enhance the physical layer security of the authentication process. As this paper focuses on the design of

authentication protocols, it does not impose constraints on PUFs. To resist side-channel attacks, improvements to PUFs can be made, such as adopting low-power RO PUFs [46] or Subthreshold Current Array (SCA) PUFs [47]. (Interested readers can refer to [46,47] for more information.) Besides, any attempt to tamper with the OBU during the authentication process will cause fluctuations in the PUF, rendering it unable to generate accurate outputs. Additionally, the TA can easily identify such tampering attempts. Since the attacker $\mathcal{A}$ cannot reconstruct the PUF in subsequent attacks, the protocol can resist physical layer attacks such as OBU cloning/tampering during the authentication process.

Vehicle Traceability: Traceability is essential for the TA to detect any unusual activities by vehicles and to enable authorized vehicles to reclaim their true identities. This protocol ensures that attacker $\mathcal{A}$ cannot obtain the true identity of vehicle V_x, thereby preserving the anonymity of the vehicles. However, the true identity of vehicle V_x is only accessible to TA through the calculation of $\mathrm{Dec}(SID_A) = n_{tA} \parallel ID_A$ during the authentication process, aside from the vehicle itself. Thus, this protocol only allows TA to trace vehicle V_x.

Resistance to Vehicle Impersonation Attack: If attacker $\mathcal{A}$ intends to conduct a vehicle masquerading attack on this protocol, they must forge relevant request information, such as $M_3 = \{A_1, A_2, A_3, SID_A, T_{OA}^1\}$ and $M_4 = \{SID_A, Q_A, Y_{V_A}, \alpha_A, T_{OA}^1\}$. However, for $\mathcal{A}$ to successfully forge the corresponding data, they would need to know some secret credentials of V_x, such as ID_x , r_x , C_x, which are not accessible to attacker $\mathcal{A}$. Meanwhile, during vehicle authentication, V_x submits the verification of the counterpart vehicle to TA. At this point, since the database of TA does not contain any forged messages by attacker $\mathcal{A}$, this will directly expose the deception attempted by $\mathcal{A}$. Therefore, due to the absence of relevant parameters and TA's verification mechanism, it is impractical for attacker $\mathcal{A}$ to disguise as a vehicle.

Forward Secrecy: Using the CK adversarial model, forward secrecy can be achieved when attacker $\mathcal{A}$ has complete access to communication information and knowledge of secret credentials. Even if the session state and secret credentials are compromised, attacker $\mathcal{A}$ remains unable to access/generate the temporary key r_x for vehicle V_x, thus rendering them incapable of computing the secret key β_x. Hence, in the CK adversarial model, this protocol guarantees forward secrecy.

5.2. Formal Security Proof Based on the ROR Model

In this section, we will provide a security proof of the proposed scheme using the ROR model [48]. In the ROR model, all legitimate participants involved in session key negotiation share a dictionary of size N. The ROR model enables participants to transform low-entropy passwords, randomly chosen from the dictionary, into high-entropy shared session keys through negotiation among themselves. Here are the different terms and definitions in the ROR model.

Participants: Vehicles V_A, V_B, and the Trusted Authority TA are three distinct independent participants in the protocol, with $U_{V_A}^a$, $U_{V_B}^b$, U_{TA}^c representing instances a, b, c of participants V_A, V_B, TA, respectively. These instances are referred to as random oracle machines, and the random oracle machines will be involved in the execution of the 3PAKE protocol.

Partnering: Partnering is based on session identifier (SID) and partner identification (PID). Here, SID can be viewed as the variable of all protocol messages exchanged by instances U^{i_1} and U^{i_2}, while PID is an instance used to establish shared keys. Two instances are considered to be partnering when they satisfy the following conditions:

- Both instances U^{i_1} and U^{i_2} accept.
- Instances U^{i_1} and U^{i_2} share the same SID.
- The PID of both U^{i_1} and U^{i_2} is the same.
- No instance except for U^{i_1} and U^{i_2} will accept a PID equal to that of U^{i_1} and U^{i_2}.

Freshess: When the adversary A fails to discover the session key SK_X between V_A and V_B by Reveal (U^a), then $U_{V_A}^a$ or $U_{V_B}^b$ is considered fresh.

Random oracle: Both participant ($U^a_{V_A}$, $U^b_{V_B}$, U^c_{TA}) and adversary $\mathcal{A}$ have access to a one-way hash function h, also known as a hash oracle.

Adversary: The adversary $\mathcal{A}$ has the capability to eavesdrop on and control the entire communication network, employing a polynomial number of oracle queries to simulate realistic attacks, thereby intercepting all communication messages between the participants. The queries are formulated as follows:

Execute query $EX(U^a, U^c)$: The adversary A executes this query to intercept/eavesdrop on all instances of communication exchanged between U^a and U^c.

Send query $SE(U^a, m)$: The adversary A executes this query to conduct an active attack, sending a message m to the instance U^a. Upon receiving m, U^a will compute some relevant information of the proposed protocol and send them back to adversary A.

Reveal query $RE(U^a)$: Adversary A can obtain the current session key between U^a and its partner through this query. If adversary A requests to send a reveal query to U^a, then U^a will output as follows:

- U^a and its partner mutually authenticate, enter an accept state, and compute the session key SK. Then U^a sends the session key SK to adversary $\mathcal{A}$.
- Otherwise, U^a returns an empty value $\perp$ as output.

Test query $TE(U^a)$: This query is used to demonstrate the semantic security of the session key SK. If U^a and its partner have computed the session key, it returns SK; otherwise, it returns a null value. So, A is allowed to perform the Test query to U^a only once. When U^a receives $TE(U^a)$, it tosses an unbiased coin c, and if the result is 1, it outputs the session key SK; if the result is 0, it returns a randomly generated key of the same length as the session key; otherwise, it returns a null value ($\perp$).

Now, we can define Adv_p as the advantage of adversary A breaking the semantic security of the proposed protocol p, and W as the event of A breaking the semantic security of the proposed protocol p. Thus, $Adv_p = |2P[W] - 1|$ holds. This means that if $Adv_p \leq \eta$, then p is secure, where η is an arbitrarily small positive value.

Theorem 1. *Suppose that the adversary $\mathcal{A}$ attempts to break the semantic security of protocol p between $U^a_{V_A}$ and $U^b_{V_B}$ within polynomial time t.*

Then, the advantage of $\mathcal{A}$ in breaking the semantic security of p is denoted by:

$$Adv_p^{AKE}(t) \leq \frac{q^2_{hash}}{|Hash|} + 2Adv^{\Pi}(t) \tag{1}$$

where q_{hash}, $|Hash|$, Adv^{Π} represents the number of hash queries, the range space of the hash function, and the advantage of $\mathcal{A}$ in breaking the proposed protocol Π, respectively.

Proof. The proof process is based on the following four games, denoted as *Game* G_i $(0 \leq i \leq 3)$. Where G_0 simulates a real attack on protocol p, and G_3 illustrates the minimum advantage of $\mathcal{A}$ in breaking SK_X in the protocol. For each G_i, we define an event W_i $(0 \leq i \leq 3)$ as the event where $\mathcal{A}$ succeeds in guessing c in G_i. Considering $W_1 \wedge \neg W_3 \Leftrightarrow W_2 \wedge \neg W_3$, then we have:

$$|P[W_1] - P[W_2]| \leq P[W_3] \tag{2}$$

Game G_0: In this game, $\mathcal{A}$ selects c and starts attacking p. This attack models the hash function as a random oracle, yielding:

$$Adv_p^{AKE}(t) = |P[W_0] - \frac{1}{2}| \tag{3}$$

Game G_1: In this game, $\mathcal{A}$ obtains all the information exchanged between $U^a_{V_A}$, $U^b_{V_B}$ during the authentication and communication phases through the *Execute query*. Upon re-

ceiving the messages, $\mathcal{A}$ can execute the *Test query* to verify whether the output is the session key or a random key. Since $SK_A = h(SID_A||SID_B||\beta_A)$ and $SK_B = h(SID_A||SID_B||\beta_B)$ are the session keys for V_A and V_B, respectively, and $SK_A = SK_B$, and we cannot obtain the values of β_A and β_B through eavesdropping, the chances of $\mathcal{A}$ winning the game are not increased in this case. Therefore, we have:

$$P[W_0] = P[W_1] \tag{4}$$

Game G_2: In this game, $\mathcal{A}$ attacks by using hash queries to distinguish between the session key and the random key. $\mathcal{A}$ can utilize the previously eavesdropped information, M_4 and M_8 , to perform hash queries. But $\mathcal{A}$ requires relevant information to compute the session key, which cannot be obtained through eavesdropping or querying. Because the hash digest ensures that messages do not collide, $\mathcal{A}$ must find a hash collision in polynomial time to win the game, as inferred from the birthday paradox [49]:

$$P[W_1] - P[W_2] \leq \frac{q_{hash}^2}{|Hash|} \tag{5}$$

Game G_3: In this game, $\mathcal{A}$ attempts to eavesdrop to obtain the real session key SK_X. However, $\mathcal{A}$ cannot obtain the key to compute β_X, nor can $\mathcal{A}$ obtain r_X from Q_X. Therefore, we have:

$$P[W_2] - P[W_3] \leq 2Adv^{\Pi}(t) \tag{6}$$

At this point, if $\mathcal{A}$ guesses correctly for c, $\mathcal{A}$ can win the game. So:

$$P[W_3] = \frac{1}{2} \tag{7}$$

From (3), (4), and (7) we get:

$$Adv_p^{AKE} = |P[W_0] - \frac{1}{2}| = |P[W_1 - \frac{1}{2}]| = |P[W_1] - P[W_3]| \tag{8}$$

From (5)–(7), and the triangle inequality, we get:

$$\begin{aligned} |P[W_1] - P[W_3]| &= |P[W_1] - P[W_2] + P[W_2] - P[W_3]| \\ &\leq |P[W_1] - P[W_3]| + |P[W_2] - P[W_3]| \\ &\leq \tfrac{q_{hash}^2}{|Hash|} + 2Adv^{\Pi}(t) \end{aligned} \tag{9}$$

From (8) and (9), we obtain the desired result, namely (1):

$$Adv_p^{AKE}(t) \leq \frac{q_{hash}^2}{|Hash|} + 2Adv^{\Pi}(t) \quad \square$$

5.3. Formal Security Proof Based on BAN Logic

BAN Logic [50] is a logical system used for analyzing the security of protocols, commonly employed to prove or analyze the correctness and security of cryptographic protocols. BAN Logic typically involves a set of formal rules and inference mechanisms used to prove the goals of authentication protocols. By employing BAN Logic, users can ultimately ascertain the reliability of transmitted data and prevent eavesdropping and tampering. Here is the security analysis of the proposed protocol using BAN Logic.

The logical assumptions or rules of BAN Logic that will be used in the analysis process are as follows:

The message meaning rule R_1: $\frac{U|\equiv U \xleftrightarrow{k} V,\ U \triangleleft \{M\}_N}{U|\equiv V|\sim M}$.

The freshness rule R_2: $\frac{U|\equiv \#(M)}{U|\equiv \#(M,\ N)}$.

The nonce-verification rule R_3: $\frac{U|\equiv \#(M),\ U|\equiv V|\sim M}{U|\equiv V|\equiv M}$

The jurisdiction rule R_4: $\frac{U|\equiv V \Rightarrow M,\ U|\equiv V|\equiv M}{U|\equiv M}$

The corresponding objectives to be proven for the proposed protocol are as follows:

Goal G_1: $V_A| \equiv (V_A \xleftrightarrow{\beta_x} V_B)$ Goal G_2: $V_A| \equiv V_B| \equiv (V_A \xleftrightarrow{\beta_x} V_B)$

Goal G_3: $V_B| \equiv (V_A \xleftrightarrow{\beta_x} V_B)$ Goal G_4: $V_B| \equiv V_A| \equiv (V_A \xleftrightarrow{\beta_x} V_B)$

Goal G_5: $TA| \equiv (V_x \xleftrightarrow{r_x} TA)$ Goal G_6: $TA| \equiv V_x| \equiv (V_x \xleftrightarrow{r_x} TA)$

The idealized form of the messages transmitted between vehicles V_A, V_B, and between V_x and TA in the proposed protocol is as follows:

Message M_1: $V_A \rightarrow V_B : \{V_A \xleftrightarrow{\beta_x} V_B,\ T^1_{OA}\}_{k_t}$

Message M_2: $V_B \rightarrow V_A : \{V_B \xleftrightarrow{\beta_x} V_A,\ T^4_{OB}\}_{k_t}$

Message M_3: $V_x \rightarrow TA : \{V_x \xleftrightarrow{r_x} TA,\ X_2,\ X_3,\ SID_x,\ T^i_{OX}\}$

According to the proposed protocol, the following basic assumptions are made:

Assumption A_1: $V_A| \equiv \#(T^1_{OA})$

Assumption A_2: $V_A| \equiv \#(T^4_{OB})$

Assumption A_3: $V_B| \equiv \#(T^1_{OA})$

Assumption A_4: $V_x| \equiv \#(T^i_{OX})$

Assumption A_5: $V_A| \equiv V_A \xleftrightarrow{\{\beta_x\}_{k_t}} V_B$

Assumption A_6: $V_A| \equiv V_B \Rightarrow V_A \xleftrightarrow{\beta_x} V_B$

Assumption A_7: $V_B| \equiv V_A \xleftrightarrow{\{\beta_x\}_{k_t}} V_B$

Assumption A_8: $V_B| \equiv V_A \Rightarrow V_A \xleftrightarrow{\beta_x} V_B$

Assumption A_9: $TA| \equiv TA \xleftrightarrow{r_x} V_x$

Assumption A_{10}: $TA| \equiv V_x \Rightarrow V_x \xleftrightarrow{r_x} TA$

The proposed protocol aims to demonstrate its objectives based on rules, idealizations, and assumptions. The specific proofs are as follows:

From Message M_3, get S_1: $V_B \lhd \{T^1_{OA},\ V_A \xleftrightarrow{\beta_x} V_B\}_{k_t}$

From S_1, A_7 and rule R_1, get S_2: $V_B| \equiv V_A| \sim (T^1_{OA},\ V_A \xleftrightarrow{\beta_x} V_B)$

From S_2, A_3 and rules R_2, R_3, get S_3: $V_B| \equiv V_A| \equiv (V_A \xleftrightarrow{\beta_x} V_B)$ [G_4 proved]

From S_3, A_8 and rule R_4, get S_4: $V_A| \equiv V_B| \equiv (V_A \xleftrightarrow{\beta_x} V_B)$ [G_2 proved]

From Message M_2, get S_5: $V_A \lhd \{T^1_{OB},\ V_A \xleftrightarrow{\beta_x} V_B\}_{k_t}$

From S_5, A_5 and rule R_1, get S_6: $V_A| \equiv V_B| \sim (T^4_{OB},\ V_A \xleftrightarrow{\beta_x} V_B)$

From S_6, A_2 and rules R_2, R_3, get S_7: $V_B| \equiv (V_A \xleftrightarrow{\beta_x} V_B)$ [G_3 proved]

From S_7, A_6 and rule R_4, get S_8: $V_A| \equiv (V_A \xleftrightarrow{\beta_x} V_B)$ [G_1 proved]

From Message M_3, get S_9: $TA \lhd \{V_x \xleftrightarrow{r_x} TA,\ X_2,\ X_3,\ SID_x,\ T^i_{OX}\}$

From S_9, A_9 and rule R_1, get S_{10}: $TA| \equiv V_x| \sim (T^i_{OX},\ V_x \xleftrightarrow{r_x} TA)$

From S_{10}, A_4 and rules R_2, R_3, get S_{11}: $TA| \equiv V_x| \equiv (V_x \xleftrightarrow{r_x} TA)$ [G_6 Proved]

From S_{11}, A_{10} and rule R_4, get S_{12}: $TA| \equiv (V_x \xleftrightarrow{r_x} TA)$ [G_5 Proved]

6. Performance Analysis

This section will delve into the performance evaluation of the proposed protocol, juxtaposed with comparative analyses against other protocols [11–15]. This comparison is based on two key metrics: computational expenditure and communication overhead. Considering that initialization setup and registration phases occur only once, performance analysis primarily focuses on the authentication and communication phases. The experiments were executed on a 64-bit Ubuntu (18.04.6) system, powered by a 12th Gen Intel(R) Core(TM) i5 3.5 GHz processor and 32 GB of memory. To enhance the accuracy of the experimental

findings, each operation underwent rigorous testing 50 times, and the resultant average value was considered the definitive outcome. Detailed analysis will be elaborated in the subsequent sections.

6.1. Computation Cost

The computational expense of the authentication algorithm is contingent upon the computation method utilized. Table 1 provides a breakdown of the computational time required for each computational method. In the proposed phase, *PUF* is embedded into the *OBU* of the vehicle, and the BCH code offset mechanism [51] is utilized to minimize the impact of environmental factors on the output. Table 2 delineates the computational costs associated with accessing individual and multiple devices in both the existing solutions and our proposed approach. In the proposed protocol, the authentication and communication stages involve a total of six hash operations. Additionally, symmetric encryption and decryption operations occur twice in both the authentication and communication stages. Furthermore, there are four elliptic curve point addition operations, four elliptic curve scalar multiplication operations, and two *PUF* operations. Therefore, the overall computational expenditure amounts to:

$$T_{total} = T_{au} + T_{com} = (6T_h + 2T_{enc/dec} + 4T_{ecca} + 4T_{eccsm} + 2T_p) + 2T_{enc/dec} \approx 0.8686 \ \ ms.$$

Table 1. Running time of the cryptographic operations.

Symbol	Operation	Time Cost/ms
T_h	Hash	0.0017
$T_{enc/dec}$	Symmetric en(de)cryption	0.0449
T_{ecca}	Addition operation of an elliptic curve	0.0031
T_{eccsm}	Scalar multiplication operation of an elliptic curve	0.1038
T_{mm}	modular multiplication	0.1561
T_p	The operation of the PUF	0.1256
T_{po}	Pairing operation	1.2871
T_{bpsm}	Scalar multiplication operation of bilinear pairing	0.1732
T_{bpa}	Addition operation of bilinear pairing	0.1203
T_{feg}	Fuzzy extractor generation	0.1172
T_{fer}	Fuzzy extractor reproduction	0.3284

Table 2. Computation cost in the mathematical equation.

Scheme	Authentication	Communication	Time Cost for a Single Communication	Time Cost for Multiple Communication (n)
Saleem et al. [11]	$16T_h + 3T_{enc/dec} + 2T_p + 3T_{fer}$	Combined with authentication	$16T_h + 3T_{enc/dec} + 2T_p + 3T_{fer}$	$(16T_h + 3T_{enc/dec} + 2T_p + 3T_{fer})n$
Yang et al. [12]	$22T_h + 2T_{ecca} + 14T_{eccsm}$	Combined with authentication	$22T_h + 2T_{ecca} + 14T_{eccsm}$	$(22T_h + 2T_{ecca} + 14T_{eccsm})n$
Wu et al. [13]	$18T_h$	$16T_h + 2T_{eccsm}$	$34T_h + 2T_{eccsm}$	$18T_h + (16T_h + 2T_{eccsm})n$
Vinoth et al. [14]	$9T_h + 2T_{enc/dec} + T_{fer}$	$10T_h + 4T_{enc/dec} + 2T_{mm}$	$19T_h + 6T_{enc/dec} + 2T_{mm} + T_{fer}$	$9T_h + 2T_{enc/dec} + T_{fer} + (10T_h + 4T_{enc/dec} + 2T_{mm})n$
Umar et al. [15]	$13T_h + 2T_{enc/dec} + T_p$	Combined with authentication	$13T_h + 2T_{enc/dec} + T_p$	$(13T_h + 2T_{enc/dec} + T_p)n$
Proposed	$6T_h + 2T_{enc/dec} + 4T_{ecca} + 4T_{eccsm} + 2T_p$	$2T_{enc/dec}$	$6T_h + 4T_{enc/dec} + 4T_{ecca} + 4T_{eccsm} + 2T_p$	$6T_h + 2T_{enc/dec} + 4T_{ecca} + 4T_{eccsm} + 2T_p + (2T_{enc/dec})n$

Other relevant protocols [11–15] can also employ the same methodology to obtain their computational costs, as depicted in Figure 7. In terms of computational costs, there is little difference between the proposed protocol and the protocols by Wu et al. [13] and Umar et al. [15] when the number of vehicles is small or even exceeds them in some cases. As the number of participating vehicles increases, the proposed protocol exhibits a slower growth rate in computational costs compared to other relevant protocols, thereby making it better suited for scenarios involving a larger number of vehicles.

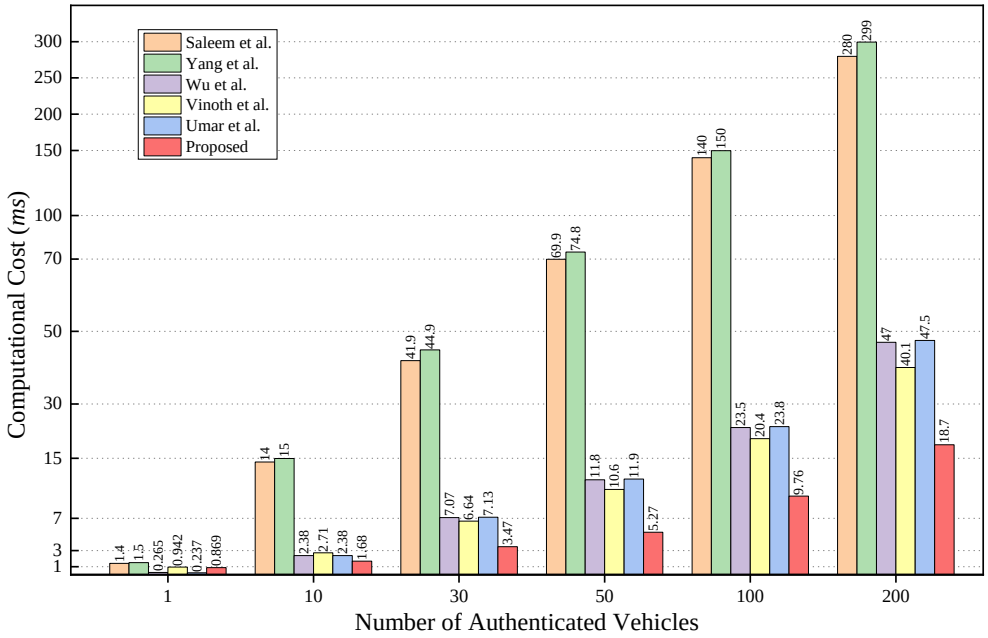

Figure 7. Computation cost comparison [11–15].

6.2. Communication Cost

Communication overhead refers to the number of bits required to transmit messages between participants in the authentication protocol. This section presents a quantitative analysis of the communication costs of the proposed protocol compared to previous relevant protocols. Table 3 presents the communication costs of the proposed protocol and related protocols in scenarios involving single and multiple participants.

Table 3. Comparison of the communication costs.

Scheme	Access Single Device Overhead (*bits*)	Access Multiple Devices Overhead (*bits*)
Saleem et al. [11]	3072	3072n
Yang et al. [12]	3456	3456n
Wu et al. [13]	4384	2464 + 1920n
Vinoth et al. [14]	3040	1248 + 1792n
Umar et al. [15]	2976	2976n
Proposed	7568	7184 + 384n

During the identity authentication phase, vehicle V_A sends information packet $\{A_1, A_2, A_3, SID_A, T_{OA}^1, Q_A, Y_{V_A}, \alpha_A\}$ to vehicle V_B, resulting in a total cost of 256 + 256 + 384 + 128 + 256 + 192 + 192 + 256 = 1920 *bits* within the proposed protocol. Subsequently, vehicle V_A requests authentication from TA, and upon receiving the verification message, both operations incur costs, denoted as 256 + 256 + 384 + 128 + 256 = 1280 *bits* and 256 + 8 = 264 *bits*, respectively. After receiving the verification feedback message,

vehicle V_B promptly sends a message to vehicle V_A, which includes the following content: $\{B_1, B_2, B_3, SID_B, T_{OB}^4, Q_B, Y_{V_B}, \alpha_B, \gamma_B\}$.

The total cost of this part is 256 + 256 + 384 + 128 + 256 + 192 + 192 + 256 + 256 = 2176 *bits*. Vehicle V_A, similar to vehicle V_B's action, requests authentication from *TA*. The communication overhead for this operation is 1280 bits, while the feedback message returned is 264 *bits*. The overall cost incurred during communication between vehicles is denoted as 128 + 256 = 384 *bits*. The total overhead for authentication and communication processes is represented by 1920 + 1280 + 264 + 2176 + 1280 + 264 + 384n = 7184 + 384n. In a similar manner, the communication expenses for related protocols [11–15] can be calculated, as shown in Figure 8. It can be observed from the figure that, the proposed protocol does not demonstrate significant superiority over other related protocols and, in some cases, even incurs higher costs when the number of vehicles is small. However, with the growth in the number of vehicles, the overall overhead increases at a noticeably slower rate compared to other relevant schemes, indicating superior adaptability for multivehicle scenarios. In summary, the proposed protocol stands out as lightweight and highly efficient compared to related protocols.

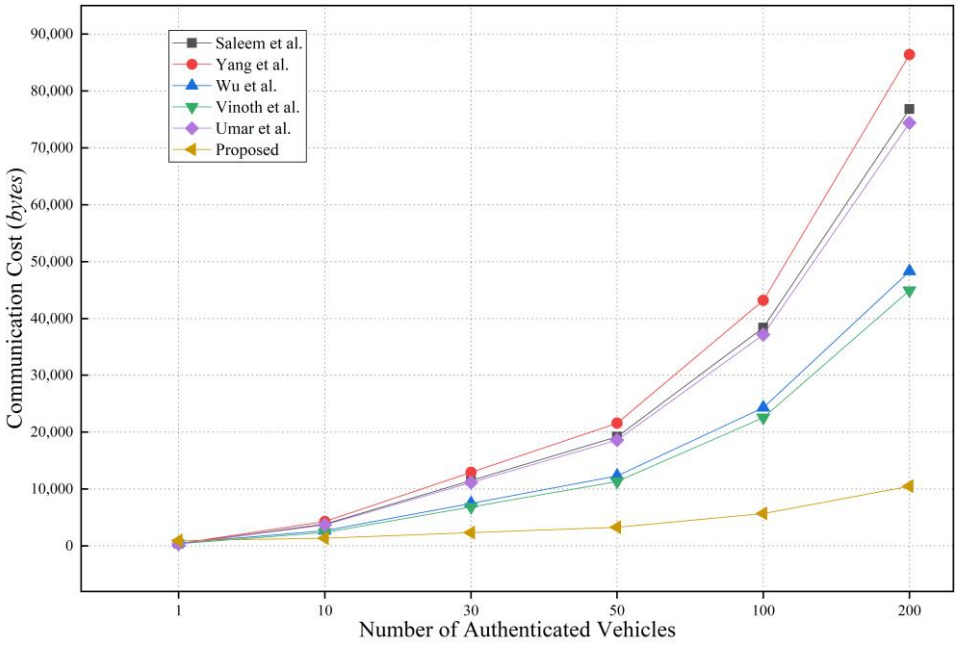

Figure 8. Communication cost comparison.

6.3. Simulation

To test the feasibility of the proposed protocol, simulations were conducted using the network simulation systems OMNeT++ 5.6.2 and SUMO 1.8.0. OMNeT++ is responsible for detailed packet-level simulation of source, destination, data traffic transmission, reception, background load, routing, links, and channels. SUMO is used to create traffic simulations, generate the required road networks for the simulation, and represent traffic demand. The specifications of the simulation experiment environment are shown in Table 4. We selected a 1600 m^2 area from the OpenStreetMap as the simulation area and included different types of vehicles, such as cars, buses, and trucks. Since SUMO requires the road network to be in its own format, the first step is to configure the desired road network on the OpenStreetMap webpage and export it as a .osm file. After that, the .osm file needs to be converted into a .net.xml file format that SUMO can accept. Using the randomTrips.py tool provided in SUMO, a route file .rou.xml can be generated, and then the simulation is configured using the .sumocfg file (as shown in Figure 9b). Finally, the simulation is conducted in OMNeT++, where vehicle movement and information exchange are simulated. Figure 9a illustrates the

transmission of messages during the simulation process, validating the practicality of the proposed protocol.

Table 4. Simulation parameters.

Parameters	Value
Simulation area	1800×1800 (m^2)
Routing protocol	AODV
Types of vehicles	Bus, car, and truck
Communication protocol	IEEE 802.11 p
Simulation time	200 s
Speed of the vehicles	50 km/h to 80 km/h
Channel bandwidth	5.9 GHz
Mobility model	Random way point

Figure 9. (**a**) A glimpse of message transfer. (**b**) SUMO configuration file.

7. Conclusions

In this paper, we propose an efficient, lightweight identity authentication protocol tailored for VANETs, based on elliptic curve cryptography with conditional privacy protection. Additionally, the proposed protocol effectively balances security with lightweight characteristics. Formal and informal evaluations of the protocol's security reveal its effectiveness in defending against physical attacks on vehicles, as well as thwarting vehicle impersonation and replay attacks. Additionally, the protocol ensures vehicle anonymity and untraceability while satisfying forward secrecy requirements. Performance evaluations focusing on computational costs and communication overhead demonstrate that our protocol outperforms recent relevant protocols, particularly in scenarios with a higher number of vehicles. Given that the authentication process of this protocol still involves communication between vehicles and *TA*, it is more suitable for urban areas with a higher density of vehicles and well-established infrastructure. However, for environments lacking infrastructure, such as rural areas, there are still certain challenges to overcome. Our future study will focus on addressing the issue of vehicles' excessive dependence on infrastructure to ensure applicability in different network environments, such as urban and rural areas. Additionally, we can choose to integrate blockchain technology, leveraging its distributed framework, to store and transmit application data information between vehicles more efficiently and securely. At this point, introducing an efficient and scalable consensus mechanism would be an open research challenge. Our next research focus will be on efficiently achieving vehicle-to-vehicle authentication and malicious node exclusion through rapid and lightweight consensus methods.

Author Contributions: Methodology, Z.F. and S.W.; software, Z.F., B.Z. and Z.L.; validation, S.W., Z.F. and Y.D.; analysis, Z.F., B.Z. and Y.D.; investigation, Z.F. and Y.S.; writing—original draft, Z.F. and Y.S.; writing—review and editing, Z.F., S.W. and Y.D.; supervision, S.W. and Y.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Natural Science Foundation of Jilin Province (20240101343JC), Department of Science and Technology of Jilin Province (20220201154GX).

Data Availability Statement: Data is contained within the article.

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

Abbreviations

Notation Table.

Symbol	Description
TA	Trusted Authority
PUF	Physical Unclonable Function
E	Elliptic Curve
F_p	Finite Field
G	Generator
V_x, V_A, V_B	Vehicle
k_t	TA's private key
PK_t	TA's public key
$< C_x, R_x >$	Challenge–response pair
ID_x	Vehicle identity
SID_x	Pseudonym of the vehicle
$T^i_{OX}, T^i_{IX}\ \ (i = 1, 2, 3, \cdots;\ X = A, B)$	Timestamp
$X_i\ \ (i = 1, 2, 3, \cdots;\ X = A, B)$	Data involved in the authentication process
SK_x	Vehicle session key
$\oplus$	XOR operation
$\|\|$	Concatenation operation
$h(\cdot)$	One-way hash function
$\Delta T_i\ \ (i = 1, 2, 3, \cdots)$	Prescribed time threshold

References

1. Tang, Q.; Xie, M.; Yang, K.; Luo, Y.; Zhou, D.; Song, Y. A decision function based smart charging and discharging strategy for electric vehicle in smart grid. *Mob. Netw. Appl.* **2019**, *24*, 1722–1731. [CrossRef]
2. Xia, Z.; Hu, Z.; Luo, J. UPTP vehicle trajectory prediction based on user preference under complexity environment. *Wirel. Pers. Commun.* **2017**, *97*, 4651–4665. [CrossRef]
3. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. VANet security challenges and solutions: A survey. *Veh. Commun.* **2017**, *7*, 7–20. [CrossRef]
4. Qu, F.; Wu, Z.; Wang, F.Y.; Cho, W. A security and privacy review of VANETs. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 2985–2996. [CrossRef]
5. Sun, X.; Lin, X.; Ho, P.H. Secure vehicular communications based on group signature and ID-based signature scheme. In Proceedings of the 2007 IEEE International Conference on Communications, Glasgow, UK, 24–28 June 2007; pp. 1539–1545.
6. Cheng, X.; Yang, L.; Shen, X. D2D for intelligent transportation systems: A feasibility study. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 1784–1793. [CrossRef]
7. Dak, A.Y.; Yahya, S.; Kassim, M. A literature survey on security challenges in VANETs. *Int. J. Comput. Theory Eng.* **2012**, *4*, 1007. [CrossRef]
8. Standaert, F.X. Introduction to side-channel attacks. *Secur. Integr. Circuits Syst.* **2010**, 27–42. [CrossRef]
9. Huang, J.L.; Yeh, L.Y.; Chien, H.Y. ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* **2010**, *60*, 248–262. [CrossRef]
10. Hao, Y.; Cheng, Y.; Zhou, C.; Song, W. A distributed key management framework with cooperative message authentication in VANETs. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 616–629. [CrossRef]
11. Saleem, M.A.; Li, X.; Ayub, M.F.; Shamshad, S.; Wu, F.; Abbas, H. An Efficient and Physically Secure Privacy-Preserving Key-Agreement Protocol for Vehicular Ad-Hoc Network. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 9940–9951. [CrossRef]
12. Yang, Q.; Zhu, X.; Wang, X.; Fu, J.; Zheng, J.; Liu, Y. A novel authentication and key agreement scheme for Internet of Vehicles. *Future Gener. Comput. Syst.* **2023**, *145*, 415–428. [CrossRef]

13. Wu, L.; Sun, Q.; Wang, X.; Wang, J.; Yu, S.; Zou, Y.; Zhu, Z. An efficient privacy-preserving mutual authentication scheme for secure V2V communication in vehicular ad hoc network. *IEEE Access* **2019**, *7*, 55050–55063. [CrossRef]
14. Vinoth, R.; Deborah, L.J.; Vijayakumar, P.; Kumar, N. Secure multifactor authenticated key agreement scheme for industrial IoT. *IEEE Internet Things J.* **2020**, *8*, 3801–3811. [CrossRef]
15. Umar, M.; Islam, S.H.; Mahmood, K.; Ahmed, S.; Ghaffar, Z.; Saleem, M.A. Provable secure identity-based anonymous and privacy-preserving inter-vehicular authentication protocol for VANETS using PUF. *IEEE Trans. Veh. Technol.* **2021**, *70*, 12158–12167. [CrossRef]
16. Lu, R.; Lin, X.; Zhu, H.; Ho, P.H.; Shen, X. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In Proceedings of the IEEE INFOCOM 2008—The 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 1229–1237.
17. Zhang, C.; Lu, R.; Lin, X.; Ho, P.H.; Shen, X. An efficient identity-based batch verification scheme for vehicular sensor networks. In Proceedings of the IEEE INFOCOM 2008—The 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 246–250.
18. Zhang, L.; Wu, Q.; Solanas, A.; Domingo-Ferrer, J. A scalable robust authentication protocol for secure vehicular communications. *IEEE Trans. Veh. Technol.* **2009**, *59*, 1606–1617. [CrossRef]
19. Lee, C.C.; Lai, Y.M. Toward a secure batch verification with group testing for VANET. *Wirel. Netw.* **2013**, *19*, 1441–1449. [CrossRef]
20. 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]
21. Zhong, H.; Wen, J.; Cui, J.; Zhang, S. Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET. *Tsinghua Sci. Technol.* **2016**, *21*, 620–629. [CrossRef]
22. Gayathri, N.B.; Thumbur, G.; Reddy, P.V.; Rahman MZ, U. Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks. *IEEE Access* **2018**, *6*, 31808–31819. [CrossRef]
23. Lo, N.W.; Tsai, J.L. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. *IEEE Trans. Intell. Transp. Syst.* **2015**, *17*, 1319–1328. [CrossRef]
24. Dua, A.; Kumar, N.; Das, A.K.; Susilo, W. Secure message communication protocol among vehicles in smart city. *IEEE Trans. Veh. Technol.* **2017**, *67*, 4359–4373. [CrossRef]
25. Teng, L.; Jianfeng, M.; Pengbin, F.; Yue, M.; Xindi, M.; Jiawei, Z.; Gao, C.; Di, L. Lightweight security authentication mechanism towards UAV networks. In Proceedings of the 2019 International Conference on Networking and Network Applications (NaNA), Daegu City, Republic of Korea, 10–13 October 2019; pp. 379–384.
26. Bagga, P.; Das, A.K.; Wazid, M.; Rodrigues, J.J.; Choo, K.K.R.; Park, Y. On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system. *IEEE Trans. Veh. Technol.* **2021**, *70*, 1736–1751. [CrossRef]
27. Ming, Y.; Cheng, H. Efficient certificateless conditional privacy-preserving authentication scheme in VANETs. *Mob. Inf. Syst.* **2019**, *2019*, 7593138. [CrossRef]
28. Li, X.; Liu, T.; Obaidat, M.S.; Wu, F.; Vijayakumar, P.; Kumar, N. A lightweight privacy-preserving authentication protocol for VANETs. *IEEE Syst. J.* **2020**, *14*, 3547–3557. [CrossRef]
29. Shamshad, S.; Saleem, M.A.; Obaidat, M.S.; Shamshad, U.; Mahmood, K.; Ayub, M.F. On the security of a lightweight privacy-preserving authentication protocol for VANETs. In Proceedings of the 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India, 25–27 March 2021; pp. 1766–1770.
30. Alshudukhi, J.S.; Mohammed, B.A.; Al-Mekhlafi, Z.G. An efficient conditional privacy-preserving authentication scheme for the prevention of side-channel attacks in vehicular ad hoc networks. *IEEE Access* **2020**, *8*, 226624–226636. [CrossRef]
31. Cui, J.; Xu, W.; Han, Y.; Zhang, J.; Zhong, H. Secure mutual authentication with privacy preservation in vehicular ad hoc networks. *Veh. Commun.* **2020**, *21*, 100200. [CrossRef]
32. Aman, M.N.; Javaid, U.; Sikdar, B. A privacy-preserving and scalable authentication protocol for the internet of vehicles. *IEEE Internet Things J.* **2020**, *8*, 1123–1139. [CrossRef]
33. Gope, P.; Sikdar, B. Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. *IEEE Internet Things J.* **2018**, *6*, 580–589. [CrossRef]
34. Jiang, Q.; Zhang, X.; Zhang, N.; Tian, Y.; Ma, X.; Ma, J. Two-factor authentication protocol using physical unclonable function for IoV. In Proceedings of the 2019 IEEE/CIC International Conference on Communications in China (ICCC), Changchun, China, 11–13 August 2019; pp. 195–200.
35. Kudva, S.; Badsha, S.; Sengupta, S.; La, H.; Khalil, I.; Atiquzzaman, M. A scalable blockchain based trust management in VANET routing protocol. *J. Parallel Distrib. Comput.* **2021**, *152*, 144–156. [CrossRef]
36. Son, S.; Lee, J.; Park, Y.; Park, Y.; Das, A.K. Design of blockchain-based lightweight V2I handover authentication protocol for VANET. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 1346–1358. [CrossRef]
37. Feng, X.; Shi, Q.; Xie, Q.; Liu, L. An efficient privacy-preserving authentication model based on blockchain for VANETs. *J. Syst. Archit.* **2021**, *117*, 102158. [CrossRef]
38. Ahmed, M.; Moustafa, N.; Akhter, A.S.; Razzak, I.; Surid, E.; Anwar, A.; Zengin, A. A blockchain-based emergency message transmission protocol for cooperative VANET. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 19624–19633. [CrossRef]
39. Tandon, R.; Verma, A.; Gupta, P.K. D-BLAC: A dual blockchain-based decentralized architecture for authentication and communication in VANET. *Expert Syst. Appl.* **2024**, *237*, 121461. [CrossRef]

40. Jiang, D.; Delgrossi, L. IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments. In Proceedings of the VTC Spring 2008-IEEE Vehicular Technology Conference, Marina Bay, Singapore, 11-14 May 2008; pp. 2036–2040.
41. Dolev, D.; Yao, A. On the security of public key protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 198–208. [CrossRef]
42. Canetti, R.; Krawczyk, H. Analysis of key-exchange protocols and their use for building secure channels. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Innsbruck, Austria, 6–10 May 2001; Springer: Berlin/Heidelberg, Germany, 2001; pp. 453–474.
43. Crocetti, L.; Baldanzi, L.; Bertolucci, M.; Sarti, L.; Carnevale, B.; Fanucci, L. A simulated approach to evaluate side-channel attack countermeasures for the Advanced Encryption Standard. *Integration* **2019**, *68*, 80–86. [CrossRef]
44. Gope, P.; Lee, J.; Quek, T.Q. Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2831–2843. [CrossRef]
45. Armknecht, F.; Moriyama, D.; Sadeghi, A.R.; Yung, M. Towards a unified security model for physically unclonable functions. In *Topics in Cryptology-CT-RSA 2016: The Cryptographers' Track at the RSA Conference 2016, San Francisco, CA, USA, 29 February–4 March 2016, Proceedings*; Springer International Publishing: Berlin/Heidelberg, Germany, 2016; pp. 271–287.
46. Cao, Y.; Zhao, X.; Ye, W.; Han, Q.; Pan, X. A compact and low power RO PUF with high resilience to the EM side-channel attack and the SVM modelling attack of wireless sensor networks. *Sensors* **2018**, *18*, 322. [CrossRef] [PubMed]
47. Xi, X.; Aysu, A.; Orshansky, M. Fresh re-keying with strong PUFs: A new approach to side-channel security. In Proceedings of the 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, USA, 30 April–4 May 2018; pp. 118–125.
48. Abdalla, M.; Fouque, P.A.; Pointcheval, D. Password-based authenticated key exchange in the three-party setting. In *Public Key Cryptography-PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, 23–26 January 2005*; Proceedings 8; Springer: Berlin/Heidelberg, Germany, 2005; pp. 65–84.
49. Boyko, V.; MacKenzie, P.; Patel, S. Provably secure password-authenticated key exchange using Diffie-Hellman. In *Advances in Cryptology—EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, 14–18 May 2000*; Proceedings 19; Springer: Berlin/Heidelberg, Germany, 2000; pp. 156–171.
50. Burrows, M.; Abadi, M.; Needham, R. A logic of authentication. *ACM Trans. Comput. Syst. (TOCS)* **1990**, *8*, 18–36. [CrossRef]
51. Dodis, Y.; Reyzin, L.; Smith, A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2–6 May 2004*; Proceedings 23; Springer: Berlin/Heidelberg, Germany, 2004; pp. 523–540.