electronics

MDPI

Article

A Seamless Authentication Scheme for Edge-Assisted Internet of Vehicles Environments Using Chaotic Maps

Seunghwan Son, DeokKyu Kwon and Youngho Park *

School of Electronic and Electrical Engineering, Kyungpook National University, Daegu 41566, Republic of Korea; sonshawn@knu.ac.kr (S.S.); kdk145@knu.ac.kr (D.K.)
* Correspondence: parkyh@knu.ac.kr

Abstract: Internet of Vehicles (IoV) is a concept that combines IoT and vehicular ad hoc networks. In IoV environments, vehicles constantly move and communicate with other roadside units (edge servers). Due to the vehicles' insufficient computing power, repetitive authentication procedures can be burdensome for automobiles. In recent years, numerous authentication protocols for IoV environments have been proposed. However, there is no study that considers both re-authentication and handover authentication situations, which are essential for seamless communication in vehicular networks. In this study, we propose a chaotic map-based seamless authentication scheme for edge-assisted IoV environments. We propose authentication protocols for initial, handover, and re-authentication situations and analyze the security of our scheme using informal methods, the real-or-random (RoR) model, and the Scyther tool. We also compare the proposed scheme with existing schemes and show that our scheme has superior performance and provides more security features. To our knowledge, This paper is the first attempt to design an authentication scheme considering both handover and re-authentication in the IoV environment.

Keywords: chaotic map; internet of vehicles; mutual authentication; seamless authentication; Scyther tool

check for updates

Academic Editor: Yolanda Blanco Fernández

Received: 11 December 2024
Revised: 31 January 2025
Accepted: 4 February 2025
Published: 9 February 2025

Citation: Son, S.; Kwon, D.; Park, Y. A Seamless Authentication Scheme for Edge-Assisted Internet of Vehicles Environments Using Chaotic Maps. *Electronics* **2025**, *14*, 672. https://doi.org/10.3390/electronics14040672

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Internet of Vehicles (IoV) is a new paradigm that applies Internet of Things (IoT) to vehicular networks [1,2]. IoV can be combined with cloud computing and edge computing to reduce the computational burden on network entities. IoV is considered a key technology to realize high-definition mapping, autonomous driving, and other convenient services. In IoV environments, vehicle-to-infrastructure (V2I), vehicle-to-person (V2P), and vehicle-to-vehicle (V2V) interactions occur continuously to provide services to drivers. Among these interactions, V2I is the most important and fundamental communication because edge nodes maintain a connection with mobile vehicles and transmit necessary information in real-time.

However, various security attacks can occur in V2I communications. When an adversary is in the network, the adversary can masquerade as a legitimate vehicle or edge node and try to transmit false information to the other party [3–5]. Furthermore, an adversary can capture messages transmitted over a wireless channel and try to track the location of a particular vehicle, which can be an invasion of privacy. To prevent these potential threats, designing a mutual authentication protocol for V2I communication is essential to provide reliable autonomous driving services.

In recent years, many authentication schemes have been proposed for secure and efficient communications in edge-assisted IoV networks [6–9]. Vehicles have much higher

mobility than general IoT devices, and handover situations in other regions occur frequently. Moreover, a vehicle is often parked or stopped, and it should re-authenticate with the same edge server (ES) again. If a vehicle repeats the authentication process again, it is inefficient and generates unnecessary computational costs on the ES. Many existing authentication schemes take into account handover, yet they do not handle re-authentication. We are confident that if we can design an authentication protocol by considering the re-authentication situation, the network efficiency would considerably improve. Furthermore, most existing schemes utilize an elliptic curve cryptosystem (ECC), which generates intensive computational costs. Since vehicles perform numerous authentications, the computational costs incurred in authentication needs to be minimized. In this paper, we propose a chaotic map-based seamless authentication scheme for edge-assisted IoV considering both handover and re-authentication situations. The main contributions of this paper are as follows:

- We propose a chaotic map-based [10] initial authentication scheme for V2I communications. The Chebyshev chaotic map has a lower computational cost than elliptic curve-based authentication. Thus, it can ensure efficient authentication for IoV environments.
- We propose re-authentication and handover authentication schemes to ensure seamless communication in IoV environments. After the initial authentication, the ES stores the pseudo identity of the authenticated vehicle and sets the expiration time. It can lead to authenticating the vehicle quickly during the re-authentication process. In a handover situation, the ES transmits information about the vehicle in advance to the other ES and enables the performance of a quick handover authentication.
- We analyzed the security of our scheme using the Scyther tool and RoR model to show that our scheme can guarantee mutual authentication and session key security. We also compared the proposed scheme with previous schemes in terms of computational costs, communication cost, and security features. We show that the proposed scheme has better security and has lower computational cost than other schemes.

Paper Organization

In Section 2, we introduce the previous research studies and describe their strengths and limitations. In Section 3, we explain the preliminaries of our scheme. In Section 4, we demonstrate the proposed mutual authentication protocols for various situations. In Section 5, we prove the security of our scheme using informal and formal methods. In Section 6, we provide the performance comparison result of the proposed scheme and related schemes. Finally, we provide the conclusions of this paper in Section 7.

2. Related Work

We introduce state-of-the-art authentication schemes proposed in IoV environments.

Wang et al. [11] proposed a V2I initial authentication and handover authentication schemes based on bilinear pairing. Their scheme succeeded in significantly lightening the computational load of handover authentication compared to the load of initial authentication. However, in both authentication situations, vehicles should perform bilinear pairing opearations, which require considerable computational cost.

Bojjagani et al. [12] proposed a secure authentication protocol for fog-based IoV networks. Their scheme considers various situations, including V2V, V2I, and V2R, and proposes an authentication protocol for each scenario. They also analyzed their scheme using the RoR model, Scyther, and Tamarin tools. However, their scheme utilized the elliptic curve cryptosystem (ECC), which requires high computational cost, and they did not consider repeated authentication situations.

Shen et al. [13] proposed a blockchain-assisted authentication scheme for edge computing-based IoV environments. In their scheme, the vehicle's information is stored in the blockchain after a vehicle is authenticated to an edge node. Then, when the vehicle moves to the region of another edge node, the edge node can authenticate the vehicle quickly by querying the blockchain. However, blockchain can burden the edge server because it has to perform a high degree of computing in addition to vehicle authentication.

Wang et al. [14] proposed an authentication protocol using a chaotic map for electric vehicle charging systems. In their scheme, an electric vehicle authenticates to an aggregator to be provided charging services. They utilized chaotic map for fast authentication. However, there is a vulnerability in that the aggregator authenticates without knowing the pseudo identity of the vehicle; additionally, their scheme struggles to ensure mutual authentication.

Xi et al. [15] proposed a zero-knowledge proof (ZKP)-based anonymous authentication scheme for IoV environments considering fast reconnect situations. In their scheme, a vehicle can authenticate to an authentication server anonymously, and therefore, it can guarantee the privacy of the vehicle. Furthermore, they considered a fast reconnection phase, allowing for seamless communication in IoV environments. However, they used ECC encryption and decryption during the reconnection, and their scheme suffers from high computational cost.

Yang et al. [16] proposed a novel initial authentication and subsequent authentication schemes for IoV. They designed an initial authentication scheme using ECC and designed the subsequent authentication efficiently based on the initial authentication. However, they utilized ECC operations in a subsequent authentication phase, and it did not show a significant advantage in relation to computational costs compared to the initial authentication.

Dwivedi et al. [17] proposed a blockchain-assisted V2I handover scheme. They proposed a novel VANET system model using two blockchains. In their scheme, vehicle location information is stored in the auxiliary blockchain, and an RSU that keeps the auxiliary blockchain can authenticate the vehicle promptly. When a vehicle moves to the other region, the V2I authentication process requires more computational load. However, this approach is not suitable for the VANET environment because vehicles generally have high mobility.

Wang et al. [18] proposed physically unclonable function (PUF)-based authentication and a key agreement scheme for vehicular networks. They utilized various cryptosystems, including ECC, exclusive-OR, PUF, and hash operation, to guarantee privacy of vehicles. However, they did not consider handover and re-authentication situations, and their method could result in network inefficiency.

Rani and Tripathi [19] proposed a blockchain-based authentication scheme for VANET. They utilized consortium blockchain and ECC for secure V2I communication. They integrated a two-level blockchain storage method for reducing the computational cost. Therefore, their scheme prevents re-registration and re-authentication of vehicles in VANET. However, in their scheme, it is inevitable that additional costs arise due to the use of blockchain.

The contributions and limitations of cutting-edge schemes are summarized in Table 1. Overall, the existing schemes have limitations when applied to real IoV environments. In this paper, we propose a secure and seamless authentication protocol compared with existing schemes.

Table 1. Strengths and limitations of the existing schemes.

Ref.	Year	Technique	Strengths	Limitations
Wang et al. [11]	2021	ECC, bilinear pairing	Consider both initial and handover authentications	High computational cost because of using bilinear pairing
Bojjagani et al. [12]	2022	ECC	Consider various situations including V2V, V2I, and V2R	Lack of considerations about repeated authentications, high computational cost because of using ECC
Shen et al. [13]	2022	ECC, blockchain	Store vehicle's identity on blockchain for handover situation	High storage cost because of using blockchain
Wang et al. [14]	2022	Chaotic map	Design fast and efficient authentication and re-authentication protocols	Do not consider repeated authentications; RSU cannot retrieve vehicle's pseudo identity
Xi et al. [15]	2022	ECC, ZKP	Propose a ZKP-based authentication scheme considering a fast reconnection	High computational cost because of using ECC
Yang et al. [16]	2023	ECC	Consider subsequent authentication situations for IoV	High computational cost beacuse of using ECC
Dwivedi et al. [17]	2023	ECC, blockchain	Design blockchain-based IoV system model and propose various authentication schemes	Generate computational load when a vehicle moves to the other region
Wang et al. [18]	2024	ECC, PUF	Utilize various cryptosystems to guarantee privacy of vehicles	Do not consider handover and re-authentication situations
Rani and Tripathi [19]	2024	ECC, blockchain	Integrate a blockchain storage for reducing the computational cost in re-authentication	Additional costs arise due to the use of blockchain

3. Preliminary

We introduce the preliminaries of the proposed scheme.

3.1. Chaotic Map

We describe the basic definition of Chebyshev chaotic map and its hardness assumptions [10].

3.1.1. Definition

For a degree n and $x \in [-1, 1]$, Chebyshev polynomial $T_n(x) : [-1, 1] \rightarrow [-1, 1]$ can be defined as the following equation:

$$T_n(x) = \begin{cases} T_0(x) = 1 & (n = 0) \\ T_1(x) = x & (n = 1) \\ T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) & (n \leq 2) \end{cases} \quad (1)$$

Then, Chebyshev polynomial defined in $x \in (-\infty, +\infty)$ can satisfy the semigroup properties for $n \geq 2$, a large prime number p, and large numbers a and b as follows:

$$T_n(x) \equiv (2xT_{n-1}(x) - T_{n-2}(x)) \ mod \ p, \tag{2}$$

$$T_{ab}(x) = T_a(T_b(x)) = T_b(T_a(x)) \ mod \ p. \tag{3}$$

3.1.2. Hardness Assumptions

Based on Equation (2), the following three hardness assumptions hold for $x \in (-\infty, +\infty)$ and a large prime p due to the Chebyshev polynomial: "Extended chaotic map-based discrete logarithm problem (CMDL)", "extended chaotic map-based computational Diffie–Hellman problem (ECMCDH)", and "extended chaotic map-based decisional Diffie–Hellman problem (ECMDDH)". They are defined as follows:

1. ECMDL problem: When a big integer $y \geq p$ is given, there is no efficient algorithm to find s which satisfies $(T_s(x) \ mod \ p) \equiv y$ in polynomial time.
2. ECMCDH problem: When $T_y(x) \ mod \ p$ and $T_z(x) \ mod \ p$ for big integers y and z are given, there is no efficient algorithm to calculate $T_{yz}(x) \ mod \ p$ in polynomial time.
3. ECMDDH problem: When $T_y(x) \ mod \ p$, $T_z(x) \ mod \ p$, and $T_r(x) \ mod$ for big integers y, z, and r are given, it is hard to determine whether $T_{yz}(x) \stackrel{?}{=} T_r(x)$.

3.2. Threat Model

We adopt both Dolev–Yao (DY) [20] and Canetti–Krawczyk (CK) [21] adversary models to analyze the proposed scheme. The adversary has the following capabilities [22,23]:

- The adversary has complete control over the wireless communication channels, and can eavesdrop, modify, and delete the messages transmitted in wireless channels.
- The adversary can act as a middleman between communication entities, performing replay attacks and man-in-the-middle attacks.
- The adversary can try to trace an identity or location of a vehicle using obtained messages from wireless channels.
- The adversary can obtain long-term or short-term keys of the network and try to reveal the session key.

In the informal analysis section, we demonstrate the security of the proposed scheme based on the adversary's capabilities.

3.3. Design Goal

We designed the proposed scheme to meet the following security goals.

1. Mutual authentication: A vehicle and an edge server must verify each other's legitimacy before agreeing to a session key. The communication should be rejected if the other party cannot be authenticated during the authentication phase.
2. Vehicle privacy: A vehicle's identity, location, and transmitted data must be hidden in wireless channels. If traceable messages are continuously sent from a vehicle, an adversary may be able to guess the vehicle's location or personal information.
3. Perfect forward secrecy: Even if the network is compromised and long-term keys are leaked, previously agreed-upon session keys must not be calculated. This includes session keys in all situations of initial authentication, handover authentication, and re-authentication.
4. Resistance to ephemeral secret leakage attack: Even if random numbers generated in a session are leaked to an adversary, the adversary cannot calculate the session key.
5. Seamless authentication: Considering the characteristics of IoV environments, it is necessary to lower the computational cost in repeated authentication situations.

Furthermore, security must be guaranteed during the re-authentication and handover authentication processes.

3.4. System Model

There are three entities in the proposed model: the cloud server (CS), edge server (ES), and vehicle. Figure 1 shows the system model.

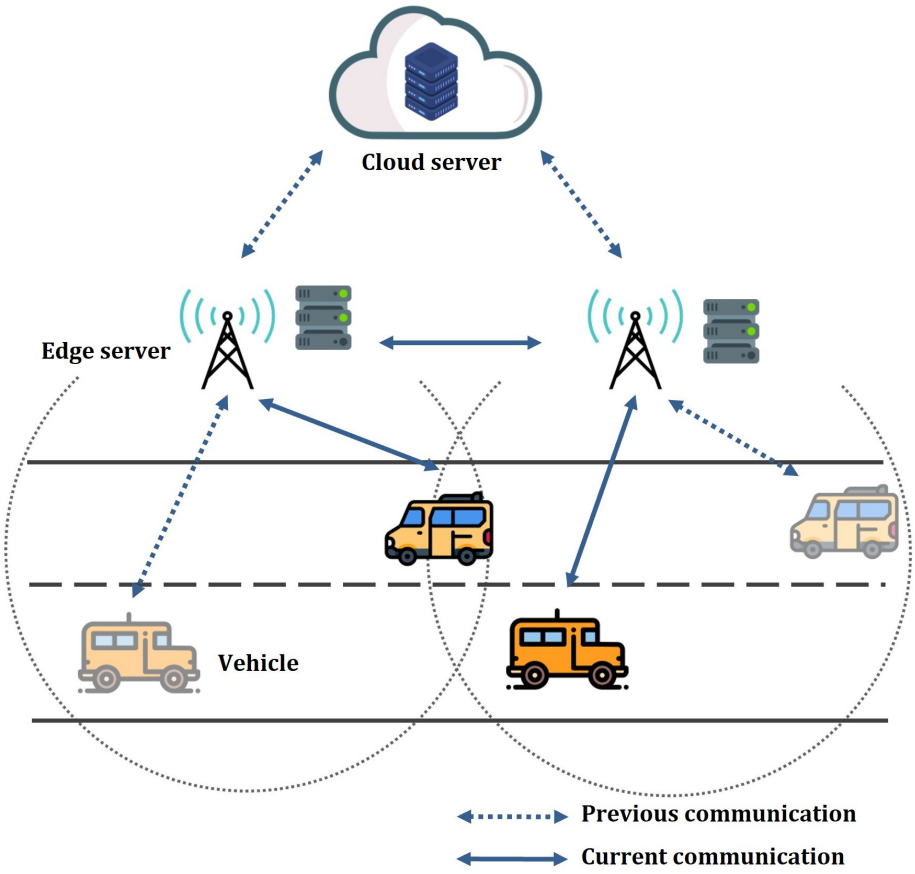


Figure 1. The edge-assisted IoV network model.

- CS: CS is a fully trusted entity that initializes the network, distributes secret keys for edge servers, and registers vehicles.
- ES: ESs communicate with vehicles in real-time and provide services. The transmitted data between an ES and a vehicle may contain sensitive and private data of the vehicle, and the transmission should be carried out after being mutually authenticated. In addition, when vehicles' handover or re-authentication occurs, ESs should be able to verify vehicles quickly to ensure real-time communication.
- Vehicle: A vehicle with a user registers with CS and participates in the network. Vehicles initially authenticate with a nearby ES, and perform re-authentication and handover authentication with ESs frequently. An adversary may attempt to masquerade as a legitimate vehicle and steal private information.

4. Proposed Scheme

We demonstrate the proposed authentication schemes for IoV environments. The proposed scheme includes system initialization, registration, login and initial authentication, re-authentication, and handover authentication phase. Before providing detailed descriptions for each phase, notations and their meanings are summarized in Table 2, and the flowchart of the proposed scheme is presented in Figure 2.

Table 2. Notations and meanings.

Notation	Meaning
V_i	i-th vehicle
ES_j	j-th edge server
s	secret key of CS
T_k (k = 1, 2, ...)	timestamps
ET_i	expiration time of V_i
RID_i	pseudo identity of V_i
SID_i	secret identity of V_i
$Auth_i$	V_i authentication value for login
r_i, r_j, r_{CS}	random nonce
$h(.)$	one-way hash function
H_i, H_j, H_{CS}	message digest
M_i, M_j, M_{CS}	message from V_i, ES_j, and CS
AID_i^j	pseudo identity of V_i agreed upon between ES_j and V_i
BID_i^j	secret identity of V_i agreed upon between ES_j and V_i

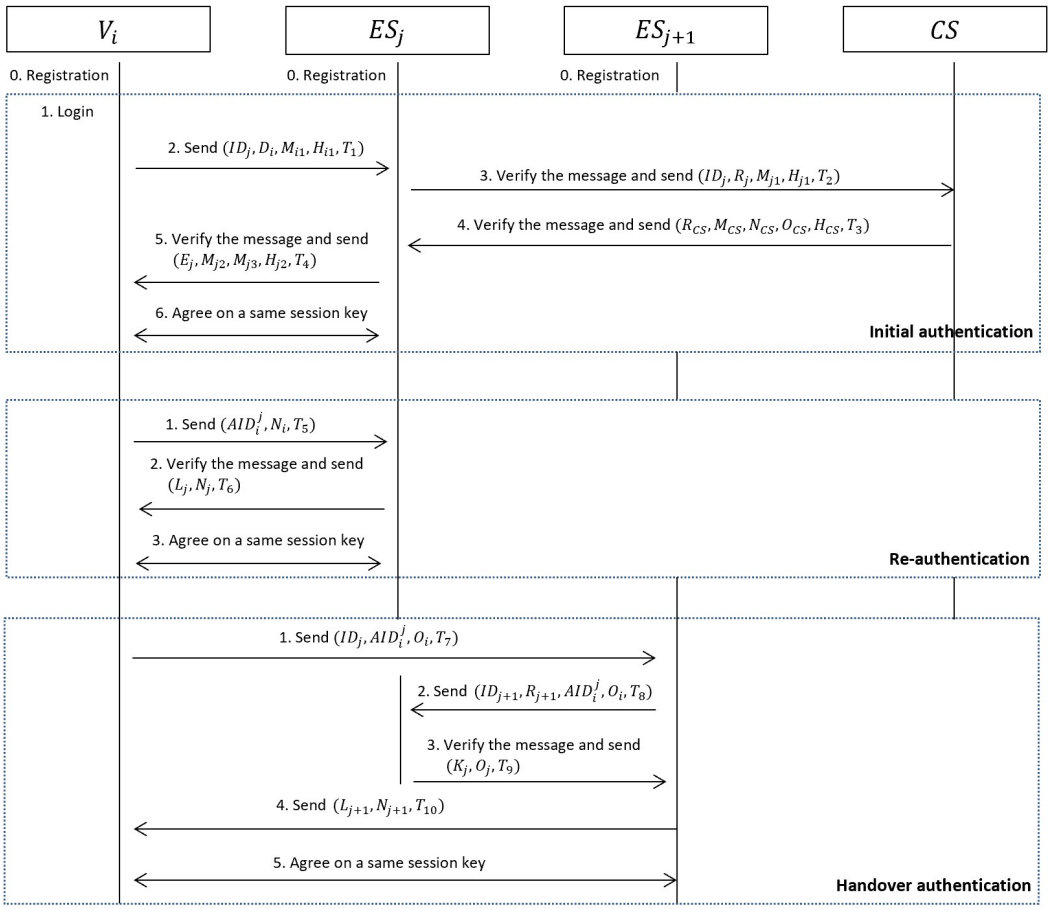


Figure 2. The flowchart of the proposed scheme.

4.1. System Initialization

The system is initiated by CS. CS chooses a Chebyshev polynomial function $T_n(x)$ with $x \in (-\infty, +\infty)$, a large prime number p, cryptographic one-way hash function $h(.)$, and a time threshold $\triangle T$. Then, CS chooses a random number $s < n$, computes $P = T_s(x)$ *mod* p, publishes $\{x, T_n(x), p, h(.), P, \triangle T\}$, and keeps s as a secret. Afterwards, CS chooses ID_j and s_j, computes $SID_j = h(ID_j||s)$, and sends (ID_j, SID_j, s_j) to ES_j. ES_j computes $P_j = T_{s_j}(x)$, publishes (ID_j, P_j), and stores (SID_j, s_j) securely.

4.2. Vehicle Registration

A user chooses ID_i and PW_i and inputs them to V_i. Then, V_i computes $HIP_i = h(ID_i||PW_i)$, $R_{i-TA} = T_{HIP_i}(x)$, and $HID_i = ID_i \oplus h(R_{i-TA})$, and sends $(HID_i, T_{HIP_i}(x))$ to CS. Then, CS computes $R_{i-TA} = T_s(T_{HIP_i}(x))$ and $ID_i = HID_i \oplus h(R_{i-TA})$ and checks whether ID_i is registered. CS chooses a random number a_{CS} and computes $RID_i = h(ID_i||a_{CS})$, $SID_i = h(RID_i||s)$, and $M_i = (RID_i||SID_i) \oplus h(R_{i-TA}||HID_i)$. Then, CS sends M_i to V_i and transmits RID_i to ES_j, which is the closest edge server to V_i. V_i computes $(RID_i||SID_i) = M_i \oplus h(R_{i-TA}||HID_i)$, chooses a random number a_i, computes $X_i = a_i \oplus HIP_i$, $Y_i = (RID_i||SID_i) \oplus h(ID_i||PW_i||a_i)$, and $Auth_i = h(ID_i||PW_i||RID_i||SID_i)$, and stores X_i, Y_i , $Auth_i$ in the memory.

4.3. Login and Initial Authentication

After registration, a user logs in to V_i and authenticates with the nearest ES_j to be provided services. First, the user inputs ID_i and PW_i to V_i, and V_i computes $a_i = X_i \oplus h(ID_i||PW_i)$ and $(RID_i||SID_i) = Y_i \oplus h(ID_i||PW_i||a_i)$, and checks $Auth_i \stackrel{?}{=} h(ID_i||PW_i||RID_i||SID_i)$. If it is equal, V_i generates a timestamp T_1 and a random number r_i, computes $D_i = T_{r_i}(x)$, $D_{ij} = T_{r_i}(P_j)$, $M_{i1} = RID_i \oplus h(D_{ij}||T_1)$, and $H_{i1} = h(SID_i||RID_i)$, and sends $(ID_j, D_i, M_{i1}, H_{i1}, T_1)$ to ES_j. After ES_j receives the message, ES_j computes $RID_i = M_{i1} \oplus h(D_{ij}||T_1)$, checks whether RID_i is registered and $|T_1^{'} - T_1| \leq \triangle T$. If it satisfies, ES_j generates a random number r_j and a timestamp T_2, $R_j = T_{r_j}(x)$, $M_{j1} = RID_i \oplus h(T_{r_j}(P)||T_2)$, $H_{j1} = h(H_{i1}||SID_j||T_2)$, and sends $(ID_j, R_j, M_{j1}, H_{j1}, T_2)$ to CS. CS first checks whether $|T_2^{'} - T_2| \leq \triangle T$, computes $RID_i = M_{j1} \oplus h(T_s(R_j)||T_2)$, $SID_i = h(RID_i||s)$, $H_{i1} = h(SID_i||RID_i)$, and $SID_j = h(ID_j||s)$, and checks $H_{j1} \stackrel{?}{=} h(H_{i1}||SID_j||T_2)$. Then, CS generates a timestamp T_3 and random numbers a_{cs}^{new} and r_{cs}, computes $RID_i^{new} = h(RID_i||a_{cs}^{new})$, $SID_i^{new} = h(RID_i^{new}||s)$, $R_{CS} = T_{r_{CS}}(x)$, $M_{CS} = RID_i^{new} \oplus h(T_{r_{CS}}(R_j)||T_s(P_j))$, $N_{CS} = SID_i \oplus h(T_{r_{CS}}(R_j)||T_s(P_j)||RID_i^{new})$, $O_{CS} = SID_i^{new} \oplus h(SID_i||RID_i^{new})$, and $H_{CS} = h(SID_i^{new}||\ RID_i^{new})$, and sends $(R_{CS}, M_{CS}, N_{CS}, O_{CS}, H_{CS}, T_3)$ to ES_j. After ES_j receives the message, the user checks whether $|T_3^{'} - T_3| \leq \triangle T$, and generates a timestamp T_4, random number a_j and AID_i^j, and expiration time ET_i^j. Then, ES_j computes $RID_i^{new} = M_{CS} \oplus h(T_{r_j}(R_{CS})||T_{s_j}(P))$, $SID_i = N_{CS} \oplus h(T_{r_{CS}}(R_j)||T_s(P_j)||RID_i^{new})$, $E_j = T_{a_j}(x)$, $M_{j2} = RID_i^{new} \oplus h(T_{a_j}(D_i)||T_4)$, $BID_i^j = h(AID_i^j||s_j)$, $M_{j3} = (O_{CS}||AID_i^j||BID_i^j) \oplus h(RID_i||RID_i^{new})$, $SK = h(AID_i^j\ ||BID_i^j||\ SID_i||RID_i^{new}||T_{a_j}(D_i))$, and $H_{j2} = h(H_{CS}||\ SK||T_4)$, sends $(E_j, M_{j2}, M_{j3}, H_{j2}, T_4)$ to V_i, and stores $(AID_i^j, RID_i^{new}, ET_i^j)$ in a secure memory. V_i receives the message, checks whether $|T_4^{'} - T_4| \leq \triangle T$, computes $RID_i^{new} = M_{j2} \oplus h(T_{r_i}(E_j)||T_4)$, $(O_{CS}||AID_i^j||BID_i^j) = M_{j3} \oplus h(RID_i||RID_i^{new})$, $SID_i^{new} = O_{CS} \oplus h(SID_i||\ RID_i^{new})$, $H_{CS} = h(SID_i^{new}||RID_i^{new})$, and $SK = h(AID_i^j||BID_i^j||SID_i||RID_i^{new}||T_{r_i}(E_j))$, and checks $H_{j2} \stackrel{?}{=} h(H_{CS}||SK||T_4)$. If it is equal, V_i computes $Y_i^{new} = (RID_i^{new}||SID_i^{new}) \oplus h(ID_i||PW_i||a_i)$, $Z_i^j = (AID_i^j||\ BID_i^j) \oplus h(RID_i^{new}||SID_i^{new}||a_i)$, and $Auth_i^{new} = h\ (RID_i^{new}||SID_i^{new}||AID_i^j||BID_i^j)$. Then, V_i updates Y_i and $Auth_i$ to Y_i^{new} and $Auth_i^{new}$ and adds Z_i^j in a memory. Figure 3 presents the proposed initial authentication phase.

V_i	ES_j	CS
A user inputs ID_i^* and PW_i^* to V_i Compute $a_i = X_i \oplus h(ID_i\|\|PW_i)$ $(RID_i\|\|SID_i) = Y_i \oplus h(ID_i\|\|PW_i\|\|a_i)$ Check $Auth_i \stackrel{?}{=} h(ID_i\|\|PW_i\|\|RID_i\|\|SID_i)$ Generate a timestamp T_1 and a random number r_i Compute $D_i = T_{r_i}(x)$, $D_{ij} = T_{r_i}(P_j)$ $M_{i1} = RID_i \oplus h(D_{ij}\|\|T_1)$ $H_{i1} = h(SID_i\|\|RID_i)$		
$\xrightarrow{(ID_j, D_i, M_{i1}, H_{i1}, T_1)}$		
	Compute $RID_i = M_{i1} \oplus h(D_{ij}\|\|T_1)$ Check whether RID_i is registered	
	$\|T_1' - T_1\| \leq \triangle T$ Generate a r_j and T_2 Compute $R_j = T_{r_j}(x)$ $M_{j1} = RID_i \oplus h(T_{r_j}(P)\|\|T_2)$ $H_{j1} = h(H_{i1}\|\|SID_j\|\|T_2)$	Check whether $\|T_2' - T_2\| \leq \triangle T$ Compute $RID_i = M_{j1} \oplus h(T_s(R_j)\|\|T_2)$ $SID_i = h(RID_i\|\|s)$, $H_{i1} = h(SID_i\|\|RID_i)$ $SID_j = h(ID_j\|\|s)$ Check $H_{j1} \stackrel{?}{=} h(H_{i1}\|\|SID_j\|\|T_2)$
	$\xrightarrow{(ID_j, R_j, M_{j1}, H_{j1}, T_2)}$	Generate T_3 and random a_{cs}^{new} and r_{cs} Compute $RID_i^{new} = h(RID_i\|\|a_{cs}^{new})$ $SID_i^{new} = h(RID_i^{new}\|\|s)$ $R_{CS} = T_{r_{CS}}(x)$ $M_{CS} = RID_i^{new} \oplus h(T_{r_{CS}}(R_j)\|\|T_s(P_j))$ $N_{CS} = SID_i \oplus h(T_{r_{CS}}(R_j)\|\|T_s(P_j)\|\|RID_i^{new})$ $O_{CS} = SID_i^{new} \oplus h(SID_i\|\|RID_i^{new})$ $H_{CS} = h(SID_i^{new}\|\|\ RID_i^{new})$
	Check $\|T_3' - T_3\| \leq \triangle T$ Generate T_4, random a_j and AID_i^j expiration time ET_i^j Compute	$\xleftarrow{(R_{CS}, M_{CS}, N_{CS}, O_{CS}, H_{CS}, T_3)}$
	$RID_i^{new} = M_{CS} \oplus h(T_{r_j}(R_{CS})\|\|T_{s_j}(P))$ $SID_i = N_{CS} \oplus h(T_{r_{CS}}(R_j)\|\|T_s(P_j)\|\|RID_i^{new})$ $E_j = T_{a_j}(x)$ $M_{j2} = RID_i^{new} \oplus h(T_{a_j}(D_i)\|\|T_4)$ $BID_i^j = h(AID_i^j\|\|s_j)$ $M_{j3} = (O_{CS}\|\|AID_i^j\|\|BID_i^j) \oplus h(RID_i\|\|RID_i^{new})$ $SK = h(AID_i^j\|\|BID_i^j\|\|SID_i\|\|RID_i^{new}\|\|T_{a_j}(D_i))$ $H_{j2} = h(H_{CS}\|\|\ SK\|\|T_4)$ Store $(AID_i^j, RID_i^{new}, ET_i^j)$ in a secure memory	
	$\xleftarrow{(E_j, M_{j2}, M_{j3}, H_{j2}, T_4)}$	
Check $\|T_4' - T_4\| \leq \triangle T$ Compute $RID_i^{new} = M_{j2} \oplus h(T_{r_i}(E_j)\|\|T_4)$ $(O_{CS}\|\|AID_i^j\|\|BID_i^j) = M_{j3} \oplus h(RID_i\|\|RID_i^{new})$ $SID_i^{new} = O_{CS} \oplus h(SID_i\|\|\ RID_i^{new})$ $H_{CS} = h(SID_i^{new}\|\|RID_i^{new})$ $SK = h(AID_i^j\|\|BID_i^j\|\|SID_i\|\|RID_i^{new}\|\|T_{r_i}(E_j))$ Check $H_{j2} \stackrel{?}{=} h(H_{CS}\|\|SK\|\|T_4)$ Compute $Y_i^{new} = (RID_i^{new}\|\|SID_i^{new}) \oplus h(ID_i\|\|PW_i\|\|a_i)$ $Z_i^j = (AID_i^j\|\|\ BID_i^j) \oplus h(RID_i^{new}\|\|SID_i^{new}\|\|a_i)$ $Auth_i^{new} = h\ (RID_i^{new}\|\|SID_i^{new}\|\|AID_i^j\|\|BID_i^j)$ Update Y_i and $Auth_i$ to Y_i^{new} and $Auth_i^{new}$ add Z_i^j in a memory		

Figure 3. Proposed login and initial authentication phase.

4.4. Re-Authentication

Within the expiration time ET_i^j determined in the initial authentication, V_i can perform fast re-authentication with ES_j. When ID_i and PW_i are input to V_i, V_i computes $a_i = X_i^{new} \oplus h(ID_i||PW_i)$, $(RID_i^{new}||SID_i^{new}) = Y_i^{new} \oplus h(ID_i||PW_i||a_i)$, and $(AID_i^j||BID_i^j) = Z_i^j \oplus h(RID_i^{new}||SID_i^{new}||a_i)$, and checks $Auth_i^{new} \stackrel{?}{=} h(RID_i^{new}\ ||SID_i^{new}||\ AID_i^j||BID_i^j)$. If it is equal, V_i generates a timestamp T_5, computes $N_i = h(RID_i^{new}||BID_i^j||T_5)$, and sends (AID_i^j, N_i, T_5) to ES_j. ES_j checks whether $|T_5' - T_5| \leq \triangle T$, retrieves RID_i^{new} and ET_i^j using AID_i^j, and checks ET_i is valid. After that, ES_j computes $BID_i^j = h(AID_i^j||s_j)$ and checks $N_i \stackrel{?}{=} h(RID_i^{new}||BID_i^j||T_5)$. If it is equal, ES_j generates a timestamp T_6 and a random number b_j, computes $AID_i^{j^{new}} = h(AID_i^j||b_j)$, $BID_i^{j^{new}} = h(AID_i^{j^{new}}||s_j)$, $L_j = (AID_i^{j^{new}}||BID_i^{j^{new}}) \oplus h(AID_i^j||BID_i^j||T_6)$, $SK = h(RID_i^{new}||BID_i^{j^{new}}||T_5||T_6)$, and $N_j = h(SK||T_5||T_6)$. ES_j sends (L_j, N_j, T_6) to V_i and updates AID_i^j and BID_i^j to $AID_i^{j^{new}}$ and $BID_i^{j^{new}}$, respectively. V_i checks whether $|T_6' - T_6| \leq \triangle T$, computes $(AID_i^{j^{new}}||BID_i^{j^{new}}) = L_j \oplus h(AID_i^j||BID_i^j||T_6)$ and $SK = h(RID_i^{new}||BID_i^{j^{new}}||T_5||T_6)$, and checks $N_j \stackrel{?}{=} h(SK||T_5||T_6)$. Then, V_i computes $Z_i^{j^{new}} = (AID_i^{j^{new}}||\ BID_i^{j^{new}}) \oplus h(RID_i^{new}||SID_i^{new}||a_i)$ and $Auth_i^{new'} = h(RID_i^{new}||SID_i^{new}\ ||AID_i^{j^{new}}||BID_i^{j^{new}})$ and up-

dates Z_i^j and $Auth_i^{new}$ to $Z_i^{j^{new}}$ and $Auth_i^{new'}$. Figure 4 presents the proposed re-authentication phase.

V_i	ES_j
Input ID_i and PW_i	
Compute $a_i = X_i^{new} \oplus h(ID_i \| PW_i)$	
$(RID_i^{new} \| SID_i^{new}) = Y_i^{new} \oplus h(ID_i \| PW_i \| a_i)$	
$(AID_i^j \| BID_i^j) = Z_i^j \oplus h(RID_i^{new} \| SID_i^{new} \| a_i)$	
Check $Auth_i^{new} \stackrel{?}{=} h(RID_i^{new} \| SID_i^{new} \| AID_i^j \| BID_i^j)$	
Generate a timestamp T_5	
Compute $N_i = h(RID_i^{new} \| BID_i^j \| T_5)$	
$\xrightarrow{(AID_i^j, N_i, T_5)}$	
	Check $\|T_5' - T_5\| \leq \triangle T$
	Retrieve RID_i^{new} and ET_i^j
	Check whether ET_i is valid
	Compute $BID_i^j = h(AID_i^j \| s_j)$
	Check $N_i \stackrel{?}{=} h(RID_i^{new} \| BID_i^j \| T_5)$
	Generate T_6 and b_j
	Compute $AID_i^{j^{new}} = h(AID_i^j \| b_j)$
	$BID_i^{j^{new}} = h(AID_i^{j^{new}} \| s_j)$
	$L_j = (AID_i^{j^{new}} \| BID_i^{j^{new}}) \oplus h(AID_i^j \| BID_i^j \| T_6)$
	$SK = h(RID_i^{new} \| BID_i^{j^{new}} \| T_5 \| T_6)$
	$N_j = h(SK \| T_5 \| T_6)$
	Update AID_i^j and BID_i^j to $AID_i^{j^{new}}$ and $BID_i^{j^{new}}$
	$\xleftarrow{(L_j, N_j, T_6)}$
Check $\|T_6' - T_6\| \leq \triangle T$	
Compute $(AID_i^{j^{new}} \| BID_i^{j^{new}}) = L_j \oplus h(AID_i^j \| BID_i^j \| T_6)$	
$SK = h(RID_i^{new} \| BID_i^{j^{new}} \| T_5 \| T_6)$	
Check $N_j \stackrel{?}{=} h(SK \| T_5 \| T_6)$	
Compute $Z_i^{j^{new}} = (AID_i^{j^{new}} \| BID_i^{j^{new}}) \oplus h(RID_i^{new} \| SID_i^{new} \| a_i)$	
$Auth_i^{new'} = h(RID_i^{new} \| SID_i^{new} \| AID_i^{j^{new}} \| BID_i^{j^{new}})$	
Update Z_i^j and $Auth_i^{new}$ to $Z_i^{j^{new}}$ and $Auth_i^{new'}$	

Figure 4. Proposed re-authentication phase.

4.5. Handover Authentication

When V_i moves to ES_{j+1} from ES_j, V_i can quickly authenticate to ES_{j+1} through the proposed handover authentication. V_i generates a timestamp T_7, computes $O_i = h(RID_i^{new} \| BID_i^j)$, and sends $(ID_j, AID_i^j, O_i, T_7)$ to ES_{j+1}. Then, ES_{j+1} checks whether $|T_7' - T_7| \leq \triangle T$, generates a random number r_{j+1} and a timestamp T_8, computes $R_{j+1} = T_{r_{j+1}}(x)$, and sends $(ID_{j+1}, R_{j+1}, AID_i^j, O_i, T_8)$ to ES_j. After ES_j checks whether $|T_8' - T_8| \leq \triangle T$ and retrieves RID_i^{new} and ET_i^j using AID_i^j. Then, ES_j computes $BID_i^j = h(RID_i^{new} \| s_j)$ and checks $O_i \stackrel{?}{=} h(RID_i^{new} \| BID_i^j)$. If it is equal, ES_j generates a random number k_j and a timestamp T_9, computes $K_j = T_{k_j}(x)$ and $O_j = (RID_i^{new} \| BID_i^j) \oplus h(T_{s_j}(P_{j+1}) \| T_{k_j}(R_{j+1}))$, and sends (K_j, O_j, T_9) to ES_j. After ES_j checks whether $|T_9' - T_9| \leq \triangle T$, computes $(RID_i^{new} \| BID_i^j) = O_j \oplus h(T_{s_{j+1}}(P_j) \| T_{r_{j+1}}(K_j))$ and checks $O_i \stackrel{?}{=} h(RID_i^{new} \| BID_i^j)$. If it is equal, ES_{j+1} generates a timestamp T_{10}, a random number a_{j+1}, and an expiration time ET_i^{j+1}, computes $AID_i^{j+1} = h(AID_i^j \| a_{j+1})$, $BID_i^{j+1} = h(AID_i^{j+1} \| s_{j+1})$, $L_{j+1} = (AID_i^{j+1} \| BID_i^{j+1}) \oplus h(AID_i^j \| BID_i^j \| T_{10})$, $SK = h(RID_i^{new} \| BID_i^{j+1} \| AID_i^{j+1})$, and $N_{j+1} = h(SK \| T_{10})$, sends $(L_{j+1}, N_{j+1}, T_{10})$ and stores $(AID_i^{j+1}, RID_i^{new}, ET_i^{j+1})$ in secure memory. V_i checks whether $|T_{10}' - T_{10}| \leq \triangle T$, $(AID_i^{j+1} \| BID_i^{j+1}) = L_{j+1} \oplus h(AID_i^j \| BID_i^j \| T_{10})$, and $SK = h(RID_i^{new} \| BID_i^{j+1} \| AID_i^{j+1})$ and checks $N_{j+1} \stackrel{?}{=} h(SK \| T_{10})$. After that, V_i computes $Z_i^{j+1} = (AID_i^{j+1} \| BID_i^{j+1}) \oplus h(RID_i^{new} \| SID_i^{new} \| a_i)$ and updates Z_i^j to Z_i^{j+1}. Figure 5 presents the propose handover authentication phase.

V_i	ES_{j+1}	ES_j
Generate T_7		
Compute $O_i = h(RID_i^{new}\|\|BID_i^j)$		
$\xrightarrow{(ID_j, AID_i^j, O_i, T_7)}$		
	check whether $\|T_7' - T_7\| \leq \triangle T$	
	Generate r_{j+1} and T_8	
	Compute $R_{j+1} = T_{r_{j+1}}(x)$	
	$\xrightarrow{(ID_{j+1}, R_{j+1}, AID_i^j, O_i, T_8)}$	
		Check whether $\|T_8' - T_8\| \leq \triangle T$
		Retrieve RID_i^{new} and ET_i^j
		Compute $BID_i^j = h(RID_i^{new}\|\|s_j)$
		Check $O_i \stackrel{?}{=} h(RID_i^{new}\|\|BID_i^j)$
	Check whether $\|T_9' - T_9\| \leq \triangle T$	Generate k_j and T_9
	Compute $(RID_i^{new}\|\|BID_i^j) =$	Compute $K_j = T_{k_j}(x)$
	$O_j \oplus h(T_{s_{j+1}}(P_j)\|\|T_{r_{j+1}}(K_j))$	$O_j = (RID_i^{new}\|\|BID_i^j) \oplus h(T_{s_j}(P_{j+1})\|\|T_{k_j}(R_{j+1}))$
	Check $O_i \stackrel{?}{=} h(RID_i^{new}\|\|BID_i^j)$	$\xleftarrow{(K_j, O_j, T_9)}$
	Generate T_{10}, a_{j+1}, and ET_i^{j+1}	
	Compute $AID_i^{j+1} = h(AID_i^j\|\|a_{j+1})$	
	$BID_i^{j+1} = h(AID_i^{j+1}\|\|s_{j+1})$	
	$L_{j+1} = (AID_i^{j+1}\|\|BID_i^{j+1}) \oplus h(AID_i^j\|\|BID_i^j\|\|T_{10})$	
Check whether $\|T_{10}' - T_{10}\| \leq \triangle T$	$SK = h(RID_i^{new}\|\|BID_i^{j+1}\|\|AID_i^{j+1})$	
Compute	$N_{j+1} = h(SK\|\|T_{10})$	
$(AID_i^{j+1}\|\|BID_i^{j+1}) = L_{j+1} \oplus h(AID_i^j\|\|BID_i^j\|\|T_{10})$	Store $(AID_i^{j+1}, RID_i^{new}, ET_i^{j+1})$	
$SK = h(RID_i^{new}\|\|BID_i^{j+1}\|\|AID_i^{j+1})$	$\xleftarrow{(L_{j+1}, N_{j+1}, T_{10})}$	
Check $N_{j+1} \stackrel{?}{=} h(SK\|\|T_{10})$		
Compute $Z_i^{j+1} =$		
$(AID_i^{j+1}\|\|BID_i^{j+1}) \oplus h(RID_i^{new}\|\|SID_i^{new}\|\|a_i)$		
Update Z_i^j to Z_i^{j+1}		

Figure 5. Proposed handover authentication phase.

5. Security Analysis

We analyzed the the proposed scheme against different attacks using the informal security analysis and formal security analysis. We denote our proposed scheme as CM-SAS in the analysis sections.

5.1. Informal Analysis

In this section, we demonstrate that our scheme has resistance to various attack scenarios.

5.1.1. Resistance to Replay Attacks

A can intercept messages transmitted in public channels and reuse the message to cause delays or harm the network. In our scheme, every message includes a timestamp and a message hash value such as H_{i1}, H_{j1}, H_{CS}, and H_{j2}. If A transmits the message, the time threshold will be exceeded and the message will not be regarded as valid, and if A arbitrarily modifies the message, the hash value of the message is incorrect and it will be rejected by the other party. Therefore, the proposed protocol can defend against replay attacks.

5.1.2. Resistance to Privileged Insider Attacks

In this attack scenario, we assume that A is a privileged insider of CS, and A tries to log in to other networks using the information of V_i. In our scheme, A can obtain ID_i in the registration phase. However, A cannot know any information about PW_i, which is required to log in to another server using ID_i. Therefore, A cannot access other networks by impersonating V_i, and the proposed scheme is secure against the privileged insider attacks.

5.1.3. Resistance to Impersonation Attacks

A can impersonate V_i or ES_j and try to generate a session key with the other entity. In case of masquerading as V_i, A must be able to generate a legitimate message $(ID_j, D_i, M_{i1}, H_{i1}, T_1)$. ID_j is published and D_i and T_1 can be generated by A. However, A cannot generate M_{i1} and H_{i1} without knowing RID_i and SID_i, which can be obtained with correct ID_i and PW_i. Therefore, A fails to send a message disguised as V_i. On the other hand, A must be able to generate $(E_j, M_{j2}, M_{j3}, H_{j2}, T_4)$ to disguise as ES_j. Similarly, A cannot make a legitimate M_{j2}, M_{j3}, and H_{j2}, and the message generated by A will be rejected by V_i. Therefore, the proposed protocol is secure against impersonation attacks.

5.1.4. Support Perfect Forward Secrecy

In the proposed scheme, long-term keys are s, s_j, and SID_j and the session key $SK = h(AID_i^j||BID_i^j||SID_i\ ||RID_i^{new}||T_{a_j}(D_i))$. Among these values, A can calculate RID_i=$M_j \oplus h(T_s(R_j)||T_2)$ and can calculate $SID_i = h(RID_i||s)$. However, A can obtain no more values because RID_i^{new} cannot be calculated without knowing r_i^{new} or a_j or r_i, which are random numbers generated in each session, and AID_i^j and BID_i^j are masked with RID_i^{new}. Therefore, A cannot know AID_j^j, BID_i^j, RID_i^{new}, and $T_{a_j}(D_i)$. It is also impossible to guess the above values simultaneously, and the proposed protocol can guarantee perfect forward secrecy.

5.1.5. Resistance to Ephemeral Session Random Number Leakage Attacks

The session random numbers include $(r_i, r_j, r_i^{new}\ , r_{CS}, a_j)$. To disclose $SK = h(AID_i^j||BID_i^j\ ||SID_i||RI\ D_i^{new}||T_{a_j}(D_i))$, A can calculate $RID_i = M_j \oplus h(T_{r_j}(P)||T_2)$, $RID_i^{new} = h(RID_i||\ r_i^{new})$, and $T_{a_j}(D_i)$. Then, A can obtain AID_i^j and BID_i^j using RID_i and RID_i^{new}. However, A can still cannot obtain SID_i because it is masked with secret keys s and s_j as well as the random numbers. Therefore, A fails to calculate the session key and the proposed scheme is resistant to ephemeral session random number leakage attacks.

5.1.6. Support Vehicle Anonymity and Untraceability

In the proposed protocol, V_i transmits $(ID_j, D_i, M_{i1}, H_{i1}, T_1)$ and receives $(E_j, M_{j2}, M_{j3}, H_{j2}, T_4)$ from ES_j. The transmitted messages in a public channel do not include the identity of V_i. Furthermore, when re-authentication or handover authentication occurs, V_i sends AID_i^j, yet it is updated in each session. Therefore, vehicle anonymity is guaranteed in the proposed protocol. Instead, A can try to trace V_i using the transmitted messages. Messages sent in public channels must contain repetitive values to succeed in this attack. In our scheme, the pseudo identity of V_i is updated in every session and A cannot figure out the value to track V_i, and therefore, a vehicle is untraceable in the proposed scheme.

5.2. Formal Security Under RoR Model

We formally analyzed the session key security of the proposed scheme using a Real-or-Random (RoR) model [24–26]. We conducted the RoR model-based security analysis of the initial authentication scheme because the re-authentication and handover authentication phases were performed based on the initial authentication. We denote p^V and p^{ES} as network participants representing V_i and ES_j, respectively. Under the RoR model, an adversary A executes queries (i.e., attacks) to obtain the agreed session key between network participants. The notations and their descriptions are summarized in Table 3.

Table 3. Queries and their descriptions.

Query	Description
$Execute(p^V, p^{ES})$	It represents an eavesdropping attack carried out by A. A can obtain the messages between p^V and p^{ES} transmitted through a wireless channel.
$Corrupt(p^V)$	It indicates that A succeeded in corrupting V_i. A can extract stored values in V_i using power analysis attack.
$Send(p, M)$	It represents A sending a message to a network participant and that A can receive the response.
$Hash$	It indicates that A performs a one-way hash operation using the obtained values.
$Test(p)$	It is performed to verify the semantic security of the session key. We assume that there is an unbiased coin c, which of the head represents 1 and the tail represents 0, and the results are veiled from A. When A performs *Test* query, c is flipped, and a random number is given to A if $c = 0$, and the session key is given if $c = 1$. At this time, A must be able to determine whether the value is a session key or a random number.

What we can prove through ROR analysis is that the probability of A successfully distinguishing a session key and a random number when performing a *Test* query is not significantly different from 1/2.

Theorem 1. *Let $Advan(A)$ be an advantage function of A to distinguish a random number and the session key after performing the above queries.*

$$Advan(A) \leq \frac{q_{hash}^2}{|Hash|} + \frac{2q_{send}}{|D_{ID}||D_{PW}|} \tag{4}$$

where q_{hash}, q_{send}, D_{ID}, and D_{PW} represent the number of *Hash* queries performed by A, the number of *Send* queries performed by A, and the range space of uniformly distributed identity and password dictionaries, respectively.

- $Game_0$: In $Game_0$, we assume that A has no information about the session key SK and performs no queries. When $P[S_{G_0}(A)]$ denotes the probability of A succeeding in guessing the correct bit c after $Game_0$ ends, we can induce the following equation by the definition of the semantic security:

$$Advan(A) = |2P[S_{G_0}(A)] - 1| \tag{5}$$

- $Game_1$: A performs *Execute* and *Test* queries in the first game. In our scheme, A cannot obtain any values to calculate SK through a public channel. In the proposed scheme, the session key is calculated by $SK = h(AID_i^j||BID_i^j||SID_i||RID_i^{new}||T_{r_i}(E_j))$. A cannot obtain any of the values to calculate SK through a public channel. Therefore, A has no advantage by executing *Execute* query for guessing SK successfully, and we can induce the following equation at the end of $Game_1$:

$$P[S_{G_0}(A)] = P[S_{G_1}(A)] \tag{6}$$

- $Game_2$: A performs *Send* and *Hash* queries to calculate SK in this game. Each message transmitted through a public channel includes a timestamp and message hash value, and A cannot arbitrarily modify the message. Therefore, A must find a hash collision

to compromise SK of our scheme. Then, the advantage function of A after the end of $Game_2$ can be induced as follows:

$$|P[S_{G_2}(A)] - P[S_{G_1}(A)]| \leq \frac{q_{hash}^2}{2|Hash|} \tag{7}$$

- $Game_3$: A can perform $Corrupt$ query and can obtain the stored values of V_i such as X_i, Y_i, and $Auth_i$. If A succeeds to log in and sends an authentication request a message to ES_j, then A can agree on a session key with ES_j disguising as V_i. However, for this attack to succeed, A must successfully guess the correct ID_i and PW_i, which is mathematically impossible. Assuming that A has D_{ID} and D_{PW}, the probability of successful guessing is

$$|P[S_{G_2}(A)] - P[S_{G_3}(A)]| \leq \frac{q_{send}}{|D_{ID}||D_{PW}|} \tag{8}$$

When all the games are over, A performs the $Test$ query and should guess the correct bit c to win the game. A has no advantages through the above games, and we can obtain $P[S_{G_3}(A)] = \frac{1}{2}$. Then, we can obtain the following equation using the triangle inequality:

$$\begin{aligned} \frac{1}{2}Advan(A) &= |P[S_{G_0}(A)] - \frac{1}{2}| \\ &= |P[S_{G_0}(A)] - P[S_{G_3}(A)]| \\ &\leq |P[S_{G_0}(A)] - P[S_{G_1}(A)]| \\ &\quad + |P[S_{G_1}(A)] - P[S_{G_2}(A)]| \\ &\quad + |P[S_{G_2}(A)] - P[S_{G_3}(A)]| \\ &\leq \frac{q_{hash}^2}{2|Hash|} + \frac{q_{send}}{|D_{ID}||D_{PW}|} \end{aligned} \tag{9}$$

Finally, the proof is completed.

5.3. Scyther Tool

We simulated the CM-SAS using the Scyther tool [27], which is a developed for the automatic verification of security protocols. The Scyther tool verifies security for four statuses: Alive, Weakagree, Niagree, and Nisynch. The Alive status is the most basic level, which means that the communication partner is currently in a connectable state. Weakagree status is for checking whether the communication partner is legitimate. For example, the communication partner can decrypt or sign messages as well as being alive. Niagree is short for non-injective agreement. Niagree status means that the responder apparently previously ran the protocol with the sender, and both agreed on the values of the variables. Finally, Nisynch is short for non-injective synchronization, and it means that all the above conditions are satisfied and all messages are sent in the precise order described in the protocol. If a security protocol cannot satisfy the Nisynch status, it means that the protocol could be vulnerable to replay attacks. When a security protocol satisfies the four statuses, the protocol guarantees mutual authentication and resists replay attacks. The simulation result of the CM-SAS is shown in Figure 6. For all participating entities of the CM-SAS, the four statuses are satisfied, and we can say that the CM-SAS can guarantee mutual authentication and is resistant to replay attacks.

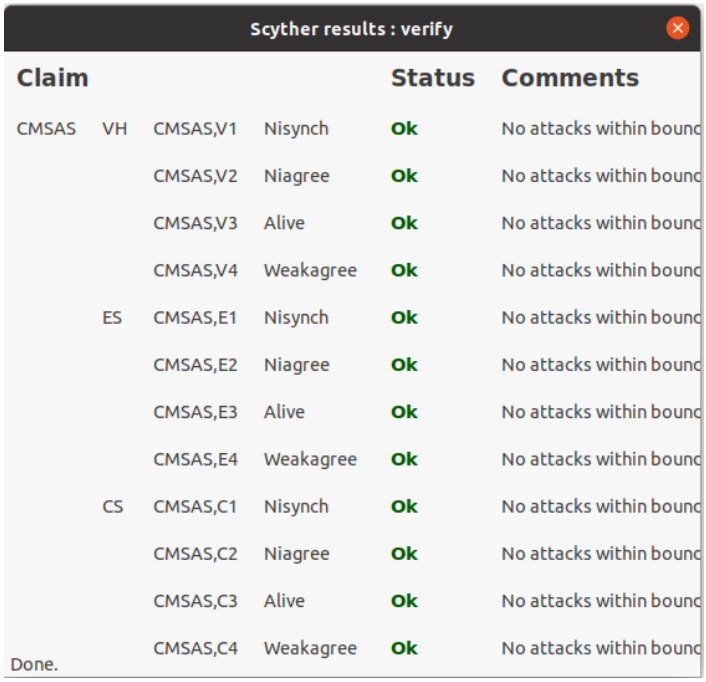


Figure 6. Scyther simulation results.

6. Performance Analysis

We compare the proposed CM-SAS with the existing schemes [11–19] in terms of computational cost, communication cost, and security features.

6.1. Computational Cost

Based on Kilinc and Yanik's report [28], a notation and time cost of each operation is as shown in Table 4. The operations were executed with Ubuntu 12.04.1 LTS 32bit operating system, Intel Pentium Dual CPU E2200 2.20 GHz processor, 2048 MB of RAM. Furthermore, similar to [29], we estimated the time cost of the chaotic map to be one-third of ECC scalar multiplication. We compared the total computational cost in three scenarios: initial authentication, handover authentication, and re-authentication. Some schemes that do not handle handover and re-authentication are considered to repeat the initial authentication in those situations. The computational cost comparison results are summarized in Table 5.

Table 4. Notation and time cost of each operation.

Notation	Meaning	Time Cost
T_{sign}	signature generation	3.85 ms
T_{ver}	signature verification	0.1925 ms
T_{mul}	ECC scalar multiplication	2.226 ms
T_{add}	ECC point addition	0.0288 ms
T_{mod}	modular exponentiation	3.85 ms
T_c	Chebyshev chaotic map	0.742 ms
T_p	bilinear pairing	5.811 ms
T_h	one-way hash	0.0023 ms

In the initial authentication, the CM-SAS has the lowest time cost on the vehicle side compared to the existing schemes, and has the second lowest time cost on the RSU/ES side. Compared to [11,12,14,15], TA/CS participates in the initial authentication and may have additional communication costs, yet it is much more efficient in terms of computational cost. In the handover authentication, the CM-SAS takes an overwhelmingly low computational cost on the vehicle, and on the RSU/ES side, it also takes significantly lower computational

cost. Ref. [15] is the only scheme that considers re-authentication, and the CM-SAS is also much more efficient compared to the scheme of [15]. The computational cost of increasing the number of vehicles and RSU/ESs can be seen in Figure 7. In Figure 7, scenarios 1, 2, and 3 represent the initial, handover, and re-authentication situations, respectively. We assume that the existing schemes that do not design handover or re-authentication should repeat initial authentication in scenarios 2 and 3. Although the computational cost of the CM-SAS is similar to the scheme of [14] in the initial authentication, the CM-SAS is more efficient than other schemes. Furthermore, in the handover and re-authentication, the CM-SAS has a remarkably low computational load compared to any other schemes as the number of authentication increases. Overall, the proposed scheme is the most efficient compared to the existing schemes in terms of computational costs.

Table 5. Computational cost comparison.

	Initial Authentication				**Handover Authentication**				**Re-Authentication**		
	V_i	RSU_j/ES_j	TA/CS	**Total**	V_i	RSU_j/ES_j	RSU_{j+1}/ES_{j+1}	**Total**	V_i	RSU_j/ES_j	**Total**
Wang et al. [11]	$T_p + T_{mul} + 4T_{mod} + T_h \approx$ 23.4393 ms	$T_p + T_{mul} + 6T_{mod} + T_h \approx$ 31.1393 ms	-	54.5786 ms	$T_p + T_{mul} + T_{mod} + T_h \approx$ 11.8893 ms	$2T_{mod} \approx$ 7.7 ms	$T_p + T_{mul} + 3T_{mod} \approx$ 19.587 ms	39.1753 ms	-	-	-
Bojjagani et al. [12]	$2T_{enc} + 2T_{sign} + 2T_{ver} + 2T_h \approx$ 15.7896 ms	$T_{enc} + T_{sign} + T_{ver} + T_h \approx$ 7.8971 ms	-	23.6867 ms	-	-	-	-	-	-	-
Shen et al. [13]	$14T_{mul} + T_h \approx$ 31.1663 ms	$11T_{mul} + 2T_h \approx$ 24.4906 ms	$8T_{mul} + T_h \approx$ 17.8103 ms	73.4672 ms	$5T_{mul} \approx$ 11.13 ms	-	$2T_{mul} \approx$ 4.452 ms	15.582 ms	-	-	-
Wang et al. [14]	$4T_c + T_h \approx$ 2.9703 ms	$4T_c + T_h \approx$ 2.9703 ms	-	5.9406 ms	-	-	-	-	-	-	-
Xi et al. [15]	$3T_{mod} + 2T_{mul} + T_{add} \approx$ 16.0308 ms	$6T_{mod} + 2T_{mul} + T_{add} \approx$ 27.5808 ms	-	43.6116 ms	-	-	-	-	$2T_{mul} + T_{add} \approx$ 4.4808 ms	$2T_{mul} + T_{add} + T_h \approx$ 4.4831 ms	9.9639 ms
Yang et al. [16]	$3T_{mul} + T_{add} + 6T_h \approx$ 6.7207 ms	$7T_{mul} + T_{add} + 4T_h \approx$ 15.6246 ms	-	22.3453 ms	$T_{mul} + 6T_h \approx$ 2.2398 ms	-	$3T_{mul} + 6T_h \approx$ 6.6919 ms	8.9317 ms	-	-	-
Dwivedi et al. [17]	$3T_{mul} + 6T_h \approx$ 6.6918 ms	$3T_{mul} + 6T_h \approx$ 6.6918 ms	-	13.3836 ms	$3T_{mul} + 6T_h \approx$ 6.6918 ms	$6T_{mul} + 10T_h \approx$ 13.379 ms	-	20.0708 ms	-	-	-
Wang et al. [18]	$3T_{mul} + 3T_{add} + 2T_h \approx$ 6.679 ms	$3T_{mul} + 3T_{add} + 2T_h \approx$ 6.679 ms	-	13.538 ms	-	-	-	-	-	-	-
Rani and Tripathi [19]	$2T_{mul} + T_{add} + 8T_h \approx$ 4.4992 ms	$7T_{mul} + 2T_{add} + 7T_h \approx$ 15.6557 ms	$2T_{mul} + T_{add} + 2T_h \approx$ 4.4854 ms	24.6403 ms		-	-	-	-	-	-
CM-SAS	$3T_c + 11T_h \approx$ 2.2513 ms	$9T_c + 10T_h \approx$ 6.6701 ms	$4T_c + 10T_h \approx$ 2.991 ms	11.9433 ms	$5T_h \approx 0.0115$ ms	$3T_c + 6T_h \approx$ 2.2398 ms	$3T_c + 3T_h \approx$ 2.2329 ms	4.4843 ms	$6T_h \approx 0.0138$ ms	$7T_h \approx 0.0161$ ms	0.0299 ms

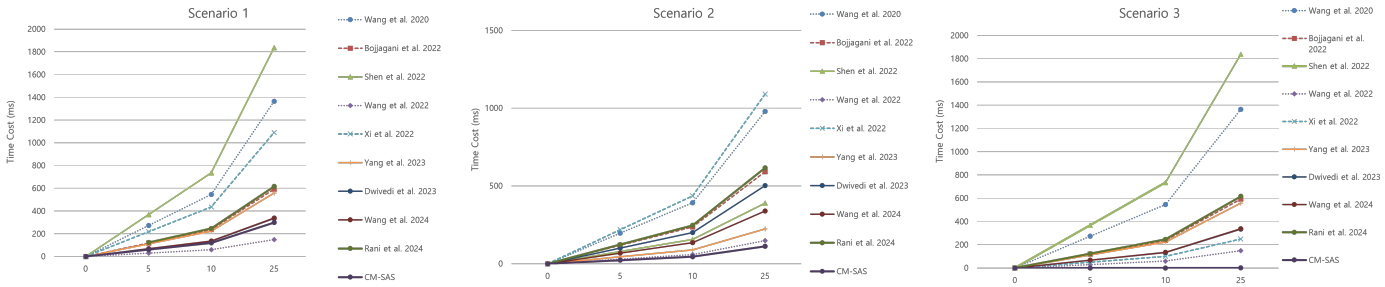


Figure 7. Total computational cost as the number of authentication increases.

6.2. Communication Cost

For a communication cost comparison, we assume that a bit length of an identity, a hash output, a random number, an ECC point, a point of pairing-based group, a request, a timestamp, a token, and a chaotic map are, respectively, 160 bits, 256 bits, 256 bits, 320 bits, 1024 bits, 32 bits, 32 bits, 160 bits, and 256 bits. Furthermore, we assume that the AES-256 algorithm is used for symmetric en/decryption. The comparison results are summarized in Table 6.

In the initial authentication phase, the proposed scheme generates a slightly higher communication cost than other schemes, except the scheme of [13,18]. However, in the handover authentication phase, the proposed scheme has similar communication costs with other schemes that consider handover situations. In the re-authentication phase, the proposed scheme generates much lower communication costs than other schemes, even compared to the scheme of [15], which is the only scheme that considers re-authentication situations. In real IoV environments, handover and re-authentication occur more frequently than the initial authentication, and the proposed scheme has competitive communication cost with existing schemes.

Table 6. Communication cost comparison.

	Initial Authentication				**Handover Authentication**				**Re-Authentication**		
	V_i	RSU_j/ES_j	TA/CS	**Total**	V_i	RSU_j/ES_j	RSU_{j+1}/ES_{j+1}	**Total**	V_i	RSU_j/ES_j	**Total**
Wang et al. [11]	1056 bits	-	-	1056 bits	-	2048 bits	160 bits	2208 bits	-	-	–
Bojjagani et al. [12]	2752 bits	1408 bits	-	4160 bits	-	-	-	-	-	-	-
Shen et al. [13]	1016 bits	3808 bits	960 bits	5784 bits	896 bits	-	1312 bits	2208 bits	-	-	-
Wang et al. [14]	1056 bits	768 bits	-	1824 bits	-	-	-	-	-	-	-
Xi et al. [15]	2240 bits	256 bits	-	2496 bits	-	-	-	-	1728 bits	256 bits	1984 bits
Yang et al. [16]	1696 bits	800 bits	-	2496 bits	1696 bits	800 bits	-	2496 bits	-	-	-
Dwivedi et al. [17]	1376 bits	864 bits	-	2240 bits	1376 bits	864 bits	1472 bits	3712 bits	-	-	-
Wang et al. [18]	3584 bits	3872 bits	128 bits	7584 bits	-	-	-	-	-	-	-
Rani and Tripathi [19]	576 bits	1216 bits	288 bits	2080 bits	-	-	-	-	-	-	-
CM-SAS	960 bits	2016 bits	1312 bits	4288 bits	704 bits	1054 bits	544 bits	2752 bits	544 bits	544 bits	1088 bits

6.3. Security Features

We compare the provided security features of the CM-SAS and existing protocols [11–15]. We consider security and functional features, including A1, "resistance to replay attack"; A2, "resistance to privileged insider attack"; A3, "resistance to impersonation attack"; A4, "preservation of perfect forward secrecy"; A5, "resistance to ephemeral session random number leakage attack"; A6, "preservation of anonymity and untraceability"; A7, "preservation of mutual authentication"; and A8, "considering repeated authentications". Table 7 shows that the CM-SAS can provide more security features than previous schemes.

Table 7. Security feature comparison.

Features	**[11]**	**[12]**	**[13]**	**[14]**	**[15]**	**[16]**	**[17]**	**[18]**	**[19]**	**CM-SAS**
A1	O	O	O	O	O	O	O	O	O	O
A2	–	–	O	O	O	–	–	O	O	O
A3	O	O	O	–	O	O	O	O	O	O
A4	–	–	O	O	–	–	O	–	–	O
A5	–	–	–	O	–	–	O	–	–	O
A6	O	O	O	O	O	O	O	O	O	O
A7	O	O	O	X	O	O	O	O	O	O
A8	O	X	O	X	O	O	O	X	O	O

–: Not considered. X: Insecure. O: Secure.

As shown in Table 7, the CM-SAS can provide more security features than the existing protocols. Furthermore, the proposed scheme has better performance than existing schemes. Therefore, the proposed protocol is more secure and efficient than other schemes.

7. Conclusions

In this paper, we proposed a chaotic map-based seamless authentication scheme (CM-SAS) for IoV environments. In the CM-SAS, an edge server stores a pseudo identity of a vehicle after initial authentication. Then, the edge server can use the stored information to authenticate the vehicle in re-authentication and handover situations. Therefore, the computational costs occurred in redundant authentication are significantly reduced. We have analyzed the CM-SAS using informal methods, the RoR model, and the Scyther tool to

prove that the CM-SAS is resistant to various attacks, guarantees session key security, and provides mutual authentication. We also compared the CM-SAS with cutting-edge schemes, and showed that our scheme has better performance in terms of the computational and communication costs. In the future work, we plan to conduct simulations to apply our plans to a real environment.

Author Contributions: Conceptualization, S.S.; methodology, S.S. and D.K.; software, S.S. and D.K.; validation, D.K. and Y.P.; formal analysis, S.S. and D.K.; writing—original draft preparation, S.S.; writing—review and editing, D.K. and Y.P.; supervision, Y.P.; project administration, Y.P. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (Ministry of Science and ICT) (RS-2024-00450915).

Data Availability Statement: Data are contained within the article.

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

References

1. Ji, B.; Zhang, X.; Mumtaz, S.; Han, C.; Li, C.;Wen, H.; Wang, D. Survey on the internet of vehicles: Network architectures and applications. *IEEE Commun. Stand. Mag.* **2020**, *4*, 34–41. [CrossRef]
2. Contreras-Castillo, J.; Zeadally, S.; Guerrero-Ibañez, J.A. Internet of vehicles: Architecture, protocols, and security. *IEEE Internet Things J.* **2018**, *5*, 3701–3709. [CrossRef]
3. Girdhar, M.; Hong, J.; Moore, J. Cybersecurity of autonomous vehicles: A systematic literature review of adversarial attacks and defense models. *IEEE Open J. Veh. Technol.* **2023**, *4*, 417–437. [CrossRef]
4. Yan, C.; Wang, C.; Shen, J.; Dev, K.; Guizani, M.; Wang, W. Edge-assisted hierarchical batch authentication scheme for VANETs. *IEEE Trans. Veh. Technol.* **2024**, *73*, 1253–1262. [CrossRef]
5. Tian, J.F.; Ni, R. An identity authentication and key agreement protocol for the Internet of Vehicles based on trusted cloud-edge-terminal architecture. *Veh. Commun.* **2024**, *49*, 100825. [CrossRef]
6. Mazhar, S.; Rakib, A.; Pan, L.; Jiang, F.; Anwar, A.; Doss, R.; Bryans, J. State-of-the-art authentication and verification schemes in VANETs: A survey. *Veh. Commun.* **2024**, *49*, 100804. [CrossRef]
7. Rawat, P.; Singh, K.D.; Chaouchi, H.; Bonnin, J.M. Wireless sensor networks: A survey on recent developments and potential synergies. *J. Supercomput.* **2014**, *68*, 1–48. [CrossRef]
8. Manivannan, D.; Moni, S.S.; Zeadally, S. Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs). *Veh. Commun.* **2020**, *25*, 100247. [CrossRef]
9. 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]
10. Zhang, L. Cryptanalysis of the public key encryption based on multiple chaotic systems. *Chaos Solitons Fractals* **2008**, *37*, 669–674. [CrossRef]
11. Wang, C.; Shen, J.; Lai, J.F.; Liu, J. B-TSCA: Blockchain assisted trustworthiness scalable computation for V2I authentication in VANETs. *IEEE Trans. Emerg. Top. Comput.* **2020**, *9*, 1386–1396. [CrossRef]
12. Bojjagani, S.; Reddy, Y.C.A.P.; Anuradha, T.; Rao, P.V.V.; Reddy, B.R.; Khan, M.K. Secure authentication and key management protocol for deployment of Internet of Vehicles (IoV) concerning intelligent transport systems. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 24698–24713. [CrossRef]
13. Shen, M.; Lu, H.; Wang, F.; Liu, H.; Zhu, L. Secure and efficient blockchain-assisted authentication for edge-integrated internet-of-vehicles. *IEEE Trans. Veh. Technol.* **2022**, *71*, 12250–12263. [CrossRef]
14. Wang, W.; Han, Z.; Alazab, M.; Gadekallu, T.R.; Zhou, X.; Su, C. Ultra super fast authentication protocol for electric vehicle charging using extended chaotic maps. *IEEE Trans. Ind. Appl.* **2022**, *58*, 5616–5623. [CrossRef]
15. Xi, N.; Li, W.; Jing, L.; Ma, J. ZAMA: A ZKP-based anonymous mutual authentication scheme for the IoV. *IEEE Internet Things J.* **2022**, *9*, 22903–22913. [CrossRef]
16. 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]
17. Dwivedi, S.K.; Amin, R.; Vollala, S.; Khan, M.K. B-HAS: Blockchain-assisted efficient handover authentication and secure communication protocol in VANETs. *IEEE Trans. Netw. Sci. Eng.* **2023**, *10*, 3491–3504. [CrossRef]
18. 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. [CrossRef]

19. Rani, D.; Sachin, T. BTTAS: Blockchain-based Two-Level Transferable Authentication Scheme for V2I communication in VANET. *Comput. Electr. Eng.* **2024**, *120*, 109767. [CrossRef]
20. Dolev, D.; Yao, A.C.-C. On the security of public key protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 198–207. [CrossRef]
21. Canetti, R.; Krawczyk, H. Analysis of key-exchange protocols and their use for building secure channels. In *International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings of the EUROCRYPT 2001: Advances in Cryptology— EUROCRYPT 2001, Innsbruck, Austria, 6–10 May 2001*; Springer: Berlin/Heidelberg, Germany, 2001; Volume 2045, pp. 453–474.
22. Sutrala, A.K.; Obaidat, M.S.; Saha, S.; Das, A.K.; Alazab, M.; Park, Y. Authenticated key agreement scheme with user anonymity and untraceability for 5G-enabled softwarized industrial cyber-physical systems. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 2316–2330. [CrossRef]
23. Yu, S.; Park, Y. A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions. *IEEE Internet Things J.* **2022**, *9*, 20214–20228. [CrossRef]
24. Abdalla, M.; Fouque, P.A.; Pointcheval, D. Password-based authenticated key exchange in the three-party setting. In *Proceedings of the International Workshop on Public Key Cryptography, Les Diablerets, Switzerland, 23–26 January 2005*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 65–84.
25. Ryu, J.; Son, S.; Lee, J.; Park, Y.; Park, Y. Design of secure mutual authentication scheme for metaverse environments using blockchain. *IEEE Access* **2022**, *10*, 98944–98958. [CrossRef]
26. Prajapat, S.; Gautam, D.; Kumar, P.; Jangirala, S.; Das, A.K.; Park, Y.; Lorenz, P. Secure lattice-based aggregate signature scheme for vehicular Ad Hoc networks. *IEEE Trans. Veh. Technol.* **2024**, *73*, 12370–12384. [CrossRef]
27. Scyther Tool. Available online: https://people.cispa.io/cas.cremers/scyther/ (accessed on 6 December 2024).
28. Kilinc, H.H.; Yanik, T. A survey of SIP authentication and key agreement schemes. *IEEE Commun. Surv. Tutor.* **2013**, *16*, 1005–1023. [CrossRef]
29. Abbasinezhad-Mood, D.; Ostad-Sharif, A.; Mazinani, S.M.; Nikooghadam, M. Provably secure escrow-less Chebyshev chaotic map-based key agreement protocol for vehicle to grid connections with privacy protection. *IEEE Trans. Ind. Inform.* **2020**, *16*, 7287–7294. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.