Design of Blockchain-Based Lightweight V2I Handover Authentication Protocol for VANET

Seunghwan Son, Joonyoung Lee, Yohan Park, Youngho Park, *Member, IEEE*, and Ashok Kumar Das, *Senior Member, IEEE*

***Abstract*—Connected vehicle means providing different services, such as advanced driver-assistance systems (ADAS) from vehicles connected to the network. Vehicular ad-hoc networks (VANETs) can support vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications to realize connected vehicle. In VANETs, secure communication must be ensured, as otherwise it can lead to traffic accidents and human injuries. Recently, many studies on V2I authentication have been conducted to guarantee the security of V2I communications. However, recent V2I authentication protocols do not consider the handover situation, and it causes unnecessary computations. As vehicles have limited computing resources, unnecessary computation can lead to overload to the vehicles. In recent years, blockchain-based VANET is an active field of research because it can provide decentralization, data integrity and transparency. Using the strength of the blockchain technology, we design a blockchain-based handover authentication protocol for VANETs. In the proposed protocol, vehicles only perform lightweight computations in handover situations for efficiency of the network. We also conduct the formal analysis such as Burrows–Abadi–Needham (BAN) logic, Real-Or-Random (ROR) oracle model, and Automated Validation of Internet Security Protocols and Applications (AVISPA) simulation to the proposed protocol. We simulate the proposed protocol using network simulator 3 (NS-3) to verify that the proposed protocol is practical. Finally, we compare the computational cost and security features of the proposed protocol with existing protocols to show that the proposed protocol is more secure and efficient.**

***Index Terms*—VANET, blockchain, handover, mutual authentication and key agreement, ROR model, NS-3, BAN logic, security.**

I. Introduction

As the necessity of an intelligent transportation system (ITS) is on the rise, vehicular ad-hoc networks (VANETs) are considered as a suitable solution to realize ITS [1], [2]. VANETs are suggested by applying mobile ad-hoc network (MANET) to the vehicular network. In general, VANETs consist of a trusted authority (TA), road side units (RSUs), and vehicles. TA deploys RSUs, registers vehicles, and manages a revocation list of illegitimate vehicles. RSUs are infrastructures that collect raw traffic information from vehicles. After collecting the information, RSUs analyze it and transmit traffic information to vehicles. Vehicles can communicate with nearby vehicles and a RSU through equipped on-board units (OBUs). However, communications on VANETs are performed on wireless channels, which can be exposed to various threats of attackers such as intercepting, eavesdropping, deleting, and modifying messages [3], [4]. In VANETs, attackers may forge messages transmitted from RSUs to vehicles or vice versa, and it can cause serious problems such as traffic accidents and human injury. Therefore, secure V2I authentication protocol is necessary.

Furthermore, vehicles continuously migrate and authenticate with other RSUs in VANETs. If handover authentication is not considered, the authentication process must be conducted from the first once again when an authenticated vehicle migrates to the coverage of other RSUs. These repetitive authentication processes raise unnecessary computation and reduce the efficiency of the network. However, there are not enough researches considering handover in V2I authentication protocols, and existing handover authentication protocols require a high amount of computational loads to vehicles. As vehicles have limited computing power [5], it can overload vehicles and cannot assure real-time communication. Additionally, it should be considered to share the information required for handover securely. If the handover information that is transmitted from one RSU to another RSU is deleted or forged, it may cause problems in the security of the network. Therefore, a lightweight and secure handover authentication protocol is necessary to increase the network efficiency and security.

A. Motivation

In recent years, a lot of researches have been conducted on applying blockchain technology in VANETs [6]–[9]. Their schemes utilized blockchain technology for various purpose such as vehicle's identity management [6], trustworthiness [7], key management [8], and batch verification [9]. These researches applied a consortium blockchain composed of RSUs. We are

Manuscript received May 18, 2021; revised December 13, 2021; accepted January 9, 2022. Date of publication January 13, 2022; date of current version May 23, 2022. This work was supported in part by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant 2020R1I1A3058605, and in part by the Ministry of Education, Korea through BK21 FOUR Project under Grant 4199990113966. Recommended for acceptance by Prof. Falko Dressler. *(Corresponding authors: Youngho Park; Yohan Park.)*

Seunghwan Son, Joonyoung Lee, and Youngho Park are with the School of Electronic and Electrical Engineering, Kyungpook National University, Daegu 41566, South Korea (e-mail: sonshawn@knu.ac.kr; harry250@knu.ac.kr; parkyh@knu.ac.kr).

Yohan Park is with the School of Computer Engineering, Keimyung University, Daegu 42601, South Korea (e-mail: yhpark@kmu.ac.kr).

Ashok Kumar Das is with the Center for Security, Theory, and Algorithmic Research, International Institute of Information Technology, Hyderabad, Telangana 500032, India (e-mail: iitkgp.akdas@gmail.com).

Digital Object Identifier 10.1109/TNSE.2022.3142287

inspired that blockchain technology could be a solution for designing secure and lightweight V2I handover authentication. Blockchain technology has not only decentralized characteristics, but has also advantages in data sharing, because it can provide data provenance, data transparency, and data integrity. RSUs can act as nodes of consortium blockchain in order to share information for handover authentication. When a RSU authenticates a vehicle in its coverage area, a transaction containing information for handover authentication is uploaded to the blockchain after going through the Algorand consensus algorithm [10], which can work even if some RSUs are faulty. Additionally, transactions on the blockchain cannot be forged, because it includes a signature of RSU, and cannot be modified because of characteristics of the blockchain technology. Therefore, other RSUs can authenticate the vehicles using the information recorded in the blockchain.

B. Research Contributions

The main contributions of this paper are as follows.

- We design V2I initial authentication and V2I handover authentication protocol based on blockchain. After a vehicle finishes initial authentication with a RSU, then the vehicle can authenticate to other RSUs using only hash and XOR operations because the corresponding information is stored in the blockchain.
- We propose a vehicle revocation phase without the help of TA for the blockchain-based VANET model. If a RSU detects the abnormal behavior of a vehicle, it can immediately notify the revocation of the vehicle through the blockchain network.
- We analyze the proposed protocol using informal security analysis and formal analysis such as BAN-logic analysis [11], ROR model [12], and AVISPA simulation [13]. The proposed protocol can resist to various attacks and security features.
- We conduct network simulator 3 (NS-3) simulation [14] to practically demonstrate the proposed protocol. Besides, we compare the proposed scheme with the existing schemes. The comparison results showed that the proposed scheme has better efficiency and security than the existing schemes.

C. Paper Organization

We introduce the preliminaries and related studies in Section II and Section III, respectively. We demonstrate the system model in Section IV. We propose a blockchain-based lightweight V2I authentication protocol in Section V. We analyze the security and performance of the proposed scheme and compare with the existing schemes in Section VI and Section VII. Finally, Section VIII concludes the paper.

II. Preliminary

A. Elliptic Curve Cryptosystem

Elliptic Curve Cryptosystem (ECC) is a type of public key cryptography [26]. Let p, q be two large primes, an elliptic curve $E_p(a,b)$ is defined as $y^2 = x^3 + ax + b$ $(4a^3 + 27b^2 \neq 0)$ over the finite field $\mathbb{F}_p$, and let $\mathbb{G}$ be a subgroup of the additive group of points of $E_p(a,b)$ with order q. For an integer $a \in \mathbb{Z}_{\mathbb{q}}$ and a point $P \in \mathbb{G}$, the point multiplication aP over $E_p(a,b)$ is defined as $\overbrace{P + P + P + \cdots + P}^{a \text{ times}} = aP$. The mathematical computational problems of ECC are as follows.

1) *Elliptic curve discrete logarithm (ECDL) problem*: Even if aP $(a \in \mathbb{Z}_q^*)$ is given, it is hard to find a, where $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$.
2) *Elliptic curve computational Diffie-Hellman (ECCDH) problem*: Even if aP and bP $(a, b \in \mathbb{Z}_p^*)$ are given, it is hard to compute abP.
3) *Elliptic curve decisional Diffie-Hellman (ECDDH) problem*: Even if aP, bP and cP $(a, b, c \in \mathbb{Z}_p^*)$ are given, it is hard to determine whether $cP \stackrel{?}{=} abP$.

B. Blockchain

There are three kinds of blockchain: public, private, and consortium blockchain. Public blockchain is represented by bitcoin and Ethereum. In public blockchain, every node keeps the ledgers and participates in consensus, for that reason, it can cause the time delay for generating blocks. Therefore, it is not suitable for VANET environments which real-time communication should be guaranteed. Private blockchain is the opposite of public blockchain. An administrator of the private blockchain conducts the transaction upload, authorizing blockchain nodes, generating blocks, and so on. It can improve the efficiency of the network compared to the public blockchain. However, it can cause the centralized problem because an administrator manages the entire network.

Consortium blockchain consists of authorized nodes to maintain the distributed databases [27]–[30]. Consortium blockchain is partially decentralized and it takes less time for consensus as compared to public blockchains. In this paper, we establish a consortium blockchain consists of RSUs and the TA. As every RSU belongs to the blockchain, the traditional "Practical Byzantine Fault Tolerance (PBFT)" consensus algorithm [31] can delay generating blocks. We apply the Algorand consensus algorithm [10] to the blockchain. The Algorand is based on Proof-of-Stake (PoS) and Byzantine Fault Tolerance (BFT), where randomly selected nodes have voting rights can generate each block. It has low delay to generate blocks and can ensure fault tolerant.

C. Adversary Model

We set Dolev-Yao (DY) model [32] to assume the capabilities of an adversary. The DY model is widely-used in authentication protocols [33]–[37]. An adversary $\mathcal{A}$ has the following assumptions and capabilities.

- $\mathcal{A}$ can be a registered vehicle in the network, and can modify, intercept, eavesdrop, and delete messages on public channels.
- $\mathcal{A}$ can still a smart card of a legitimate vehicle, and can extract the stored values of the card using power

analysis [38]. Besides, it can try to guess the identity and password simultaneously.
- $\mathcal{A}$ can try various attacks including session key disclosure, impersonation, and replay attacks [39], [40].

III. Related Work

This section gives a brief review on existing works that have been done related to authentication and blockchain in VANET domains.

A. Authentication in VANET

We introduce recent mutual authentication and key agreement protocols in VANETs. Lo *et al.* [15] proposed vehicle to RSU and RSU to vehicle authentication schemes for vehicular sensor networks. Lo *et al.* also suggested a batch message verification mechanism using elliptic curve cryptosystem. If a vehicle is revealed as a malicious one during the authentication process, then TA can trace the real identity of the vehicle for revocation.

Liu *et al.* [16] proposed a dual authentication and key agreement protocol for V2V communications. Liu *et al.* provides enhanced security and strong privacy-preserving. However, their scheme generates lots of communication costs and vehicles should carry out high computational operations such as bilinear pairing.

Gao *et al.* [17] proposed an anonymous authentication scheme for VANETs. Their scheme includes pre-handover authentication protocol and handover authentication protocol. However, their scheme used point multiplication operation on a pairing based curve, which generates high computational cost.

Xu *et al.* [18] proposed an anonymous handover authentication protocol for vehicular networks. Their scheme is formally proved using BAN logic and AVISPA simulation tool. However, their scheme used ECC during the handover authentication, it is necessary to design more efficient handover protocol.

Al-Shareeda *et al.* [19] proposed a conditional privacy-preserving mutual authentication scheme in VANET. In their scheme, a vehicle should authenticate to TA, then the vehicle can obtain a pseudo identity pool and the corresponding secret key from RSU. Besides, their scheme does not use the bilinear pairing to reduce the computational cost occuring in the authentication process. However, the existing schemes [15]–[19] does not take into account the handover situation or requires a high amount of computation.

B. Blockchain in VANET

We introduce several researches that applied the blockchain technology to VANETs. Lu *et al.* [20] designed a blockchain-based anonymous reputation system in VANETs. Lu *et al.* applied blockchain to establish a privacy-preserving trust model. Their scheme can prevent distribution of forged messages and public key revocations using blockchain.

Zhang *et al.* [21] utilized a consortium blockchain for the decentralized storage system and secure data sharing. Zhang *et al.* utilized bilinear pairing-based signature to guarantee the reliability and integrity of the transmitting data. Their scheme used data coins to make the vehicles share the date and efficiency of the whole network.

Zheng *et al.* [22] suggested blockchain-based access authentication system. Their scheme used blockchain for secure and decentralized transaction storage and transparency of the vehicles. Their scheme also can guarantee the integrity of traffic events using blockchain.

Feng *et al.* [23] proposed a blockchain-assisted authentication system for VANETs. In their scheme, RSUs and vehicles can verify the transmitted messages without a centralized third party. Their scheme can guarantee the privacy-preserving authentication even if trusted third party is offline. However, the existing researches on VANET applying blockchain technology [20]–[23] do not deal with specific mutual authentication and key agreement protocol, which are essential in wireless communications.

Ma *et al.* [24] utilized distributed storage characteristic of blockchain to reduce the dependency of PKI. They automated the public key revocation and update using the smart contract. However, they do not consider the handover situation.

Wang *et al.* [25] designed a blockchain-assisted trustworthiness computation of vehicles, and proposed V2I authentication scheme considering the handover situation. However, their scheme used bilinear pairing operation and requires high computational cost.

IV. System Model

In this section, we demonstrate a detailed description of the proposed model. The proposed system model consists of four entities: TA, RSU, vehicle, and blockchain. We illustrate the proposed blockchain-based VANET in Fig. 1 and a description of each entity as follows.

- *TA*: TA publishes system public parameters and deploys RSUs. TA also issues a smart card for vehicles in the registration phase. After registering the vehicle, TA stores the pseudo-identity of the vehicle hashed with a shared key between TA and RSUs to the blockchain.
- *RSU*: RSUs authenticate vehicles before communications. Each RSU has enough computing power to authenticate vehicles within its coverage. Also, RSUs keep the ledgers and upload the transactions with their signature as nodes of the blockchain, and randomly selected nodes participate in the consensus process to generate blocks. In handover situations, RSUs can efficiently authenticate vehicles using information stored in the blockchain.
- *Vehicle*: Vehicles are equipped with on-board units (OBUs), which have limited computing capabilities. Vehicles register to TA, and then authenticate with nearby RSU to send or receive real-time traffic information.
- *Blockchain*: Blockchain is a consortium blockchain consists of TA and RSUs. After TA registers a vehicle, TA uploads information about the pseudo-identity of the registered vehicle to the blockchain. Then, a RSU can verify whether the vehicle is registered during the

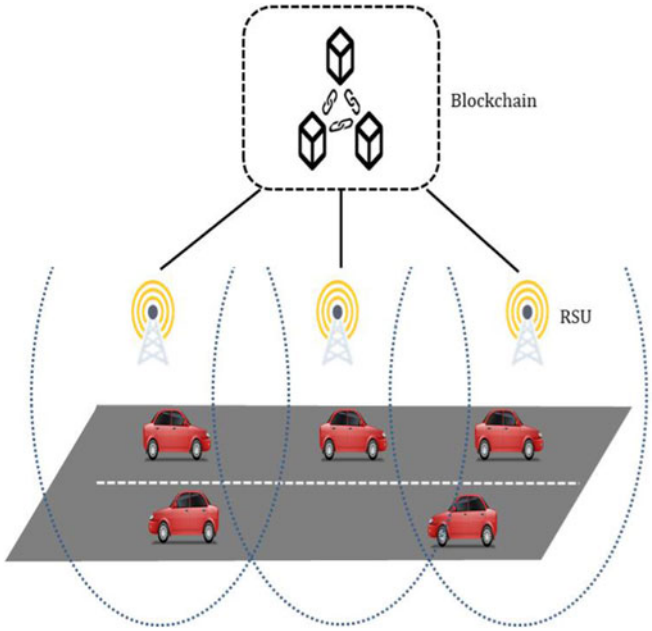

Fig. 1. Blockchain-based VANET model.

authentication process. After the V2I authentication is finished, RSU uploads a transaction which includes the vehicle's temporal identity, a random number, and the RSU's signature to the blockchain. Thus, RSUs can briefly authenticate the vehicle using the information stored in the blockchain. Transactions uploaded to the blockchain can not be forged or modified because the characteristic of the blockchain technology and each transaction include the signature of the RSU.

V. Proposed Scheme

In this section, we propose a blockchain-based V2I authentication protocol. The proposed protocol includes system setup, vehicle registration, initial V2I authentication, blockchain-based V2I handover authentication, and vehicle revocation phases. Before the detailed description of each phase, we briefly explain each phase. First, TA publishes system public parameters for V2I communications and deploys RSUs in the system setup phase. Then, vehicles must carry out the registration process to TA for authenticating and communicating with RSUs. After that, a registered vehicle can conduct initial authentication with a nearby RSU. The initial authentication is performed securely using ECC. After the initial authentication, the authentication information is uploaded to the blockchain. If the authenticated vehicle moves to coverage of another RSU, the vehicle can authenticate with the RSU using only hash and XOR operations. Furthermore, if misbehavior of a vehicle is revealed by a RSU, then the RSU can conduct the vehicle revocation phase without support of TA through the blockchain. Table II presents the notations of the proposed protocol. Furthermore, we assumed that each entity is synchronized with their clocks, which is a general assumption applied in many recent authentication protocols [41]–[43].

A. System Setup

TA generates an elliptic curve $E_p(a,b)$, and P is a generator of $\mathbb{G}$. TA chooses a secret master key s_{TA}, a one-way hash function $h(\cdot)$, and a fuzzy verifier $l : 2^4 \leq l \leq 2^8$. TA deploys secret key and shared key to each RSU in this phase. TA chooses a unique identity ID_j for RSU_j, and then computes $s_j = h(ID_j||s_{TA})$ and $k = h(ID_{TA}||s_{TA})$. TA transmits (ID_j, s_j, k) to RSU_j. After RSU_j receives the message, RSU_j computes a public key $P_j = s_j P$, and stores (k, s_j) securely. These processes are conducted through a secure channel.

B. Vehicle Registration

Before V_i authenticates to a RSU, V_i should be registered to TA. The registration phase is achieved on a secure channel, as shown in Fig. 2. First, V_i chooses unique identity ID_i and password PW_i, and generates a random number x_i. After that, V_i computes $HPW_i = h(ID_i||PW_i), RPW_i = HPW_i \oplus h(x_i)$. V_i sends (ID_i, RPW_i) to TA. Then, TA checks whether ID_i is already registered, and whether RID_i corresponding to ID_i is in the revocation list. If not, TA randomly generates r_i, computes $RID_i = h(ID_i||RPW_i||r_i)$, and stores (ID_i, RPW_i, r_i) in secure memory. TA stores (r_i, l) in SC_i, sends SC_i to V_i, and uploads $h(RID_i||k)$ to the blockchain. If V_i receives SC_i, then V_i computes $RID_i = h(ID_i||RPW_i||r_i)$, $A_i = r_i \oplus HPW_i$, $B_i = x_i \oplus h(r_i)$, and $C_i = h(h(RID_i||x_i)\ mod\ l)$. V_i replaces r_i to (A_i, B_i, C_i) in SC_i.

C. Initial V2I Authentication

After the registration phase, V_i can authenticate to RSU_j. Fig. 3 shows the initial V2I authentication phase. V_i inputs ID_i and PW_i to SC_i, then SC_i computes $HPW_i = h(ID_i||PW_i)$, $r_i = A_i \oplus HPW_i$, $x_i = B_i \oplus h(r_i)$, $RPW_i = HPW_i \oplus h(x_i)$, $RID_i = h(ID_i||RPW_i||r_i)$. Finally, SC_i checks $C_i \stackrel{?}{=} h(h(RID_i||x_i)\ mod\ l)$. If it is equal, V_i generates a random number b_i, and then computes $P_{ij} = (r_i * b_i) * P_j$, $P_i = (r_i * b_i) * P$, $M_1 = RID_i \oplus h(ID_j||P_{ij}||T_1)$, and $M_2 = h(RID_i||P_{ij}||T_1)$. After that, V_i transmits (M_1, M_2, P_i, T_1) to RSU_j. If RSU_j receives the message, then RSU_j checks the timestamp T_1, computes $P_{ij} = P_i * s_j$, $RID_i = M_1 \oplus h(ID_j||P_{ij}||T_1)$, checks whether $h(RID_i||k)$ is in the blockchain, and checks $M_2 \stackrel{?}{=} h(RID_i||P_{ij}||T_1)$. If it is equal, V_i is authenticated. Then, RSU_j generates random numbers b_j, n_j and timestamp T_2, then computes $Q_{ij} = b_j * P_i$, $Q_j = b_j * P$, $TID_i = RID_i \oplus h(n_j||\ ID_j||k)$, $M_3 = TID_i \oplus h(Q_{ij}||RID_i)$, $SK_{ij} = h(Q_{ij}||TID_i||\ RID_i)$, and $M_4 = h(SK_{ij}||T_2)$. After that, RSU_j sends (M_3, M_4, Q_j, T_2) to V_i. After V_i receives the message, V_i computes $Q_{ij} = (r_i * b_i) * Q_j$, $TID_i = M_3 \oplus h(Q_{ij}||RID_i)$, $SK_{ij} = h(Q_{ij}||TID_i||RID_i)$, and checks $M_4 \stackrel{?}{=} h(SK_{ij}||T_2)$. After the authentication process, RSU_j uploads $(TID_i, n_j,\ ID_j, Sig_j(h(TID_i||RID_i||n_j)))$ to the blockchain.

D. Blockchain-Based Handover Authentication

When V_i authenticates with RSU_j migrates to the coverage of RSU_k, then V_i and RSU_k should authenticates each other.

TABLE I
RESEARCH APPLYING BLOCKCHAIN TECHNOLOGY TO VANET

Scheme	Techniques	Main Contributions	Limitations
Lu *et al.* [20]	Lexicographical Merkle tree, Public blockchain	Privacy-preserving authentication, Vehicle Reputation algorithm	Do not support mutual authentication Scalability problem of the public blockchain
Zhang *et al.* [21]	Consortium blockchain, Batch verification	Design of network architecture, Batch verification of vehicles using bilinear pairing	Do not support mutual authentication
Zheng *et al.* [22]	Consortium blockchain, Distributed storage mechanism	Privacy-preserving authentication, Blockchain-based V2I access authentication	Do not support mutual authentication
Feng *et al.* [23]	Consortium blockchain, Attribute-based encryption	Privacy-preserving authentication, Dynamic vehicle revocation	High computational cost of ABE to vehicles Do not support mutual authentication
Ma *et al.* [24]	Bivariate polynomial, Smart contract	Blockchain-based key management, V2I mutual authentication and key agreement	High computational cost to generate blocks, Do not consider handover situation
Wang *et al.* [25]	Consortium blockchain, Bilinear pairing	Vehicle trustworthiness computation, V2I handover authentication	High computational cost to vehicles because of the bilinear pairing operation

TABLE II
NOTATIONS AND THEIR MEANINGS

Notation	Meaning
V_i	i-th vehicle
ID_i, PW_i	Identity and password of V_i
RSU_j, RSU_k	j-th and k-th RSU
ID_j, ID_k	Identity of RSU_j and RSU_k
$E_p(a, b)$	An elliptic curve
SC_i	Smart card of V_i
P	Generator of $\mathbb{G}$
RID_i	Pseudo identity of V_i
TID_i	Temporal identity of V_i
s_{TA}	Master key of TA
k	Shared key of TA and $RSUs$
$Sig_j(\cdot)$	Signature of RSU_j using ECDSA
SK_{ij}	Session key between V_i and RSU_j
SK_{ik}	Session key between V_i and RSU_k
s_j, s_k	Private keys of RSU_j and RSU_k
P_j, P_k	Public keys of RSU_j and RSU_k
n_j, n_k	Random nonces in transactions
T_a	Timestamp ($a = 1, 2, 3, \ldots$)
$h(\cdot)$	One-way Hash function
$\oplus$	Exclusive OR operation
$\|\|$	Concatenation operation
$*$	Ordinary multiplication operation

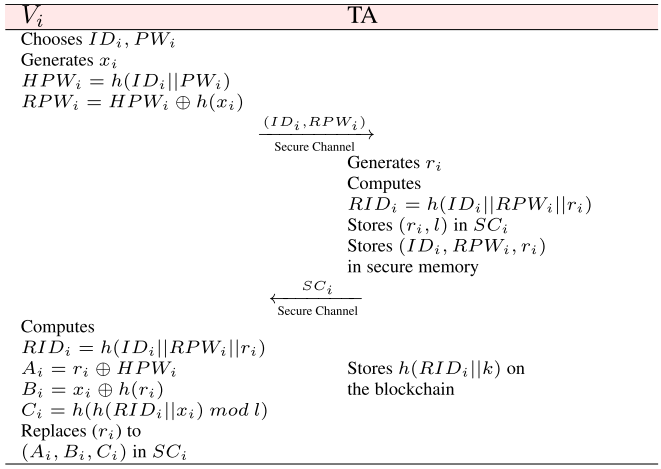

Fig. 2. Vehicle registration phase.

Fig. 4 shows the blockchain-based authentication phase. V_i generates a random number c_i, and then computes $M_5 = h(RID_i||TID_i||ID_k||T_3) \oplus c_i$, $M_6 = h(c_i||RID_i||TID_i)$. After that, V_i sends (TID_i, M_5, M_6, T_3) to RSU_k. After the reception of the message, RSU_k retrieves the transaction $(TID_i, n_j, ID_j,\ Sig_j(h(TID_i||RID_i||n_j)))$ from the blockchain. Thereafter, RSU_k verifies the signature, computes $RID_i^* = TID_i \oplus h(n_i||ID_j||k)$, and checks $h(TID_i||RID_i^*||n_j) \stackrel{?}{=} h(TID_i||RID_i||n_j)$. If it is equal, RSU_k computes $c_i = h(RID_i||TID_i||ID_k||T_3) \oplus M_5$ and also checks whether $M_7 \stackrel{?}{=} h(c_i||RID_i||TID_i)$. If it is equal, RSU_k generates random numbers c_k and n_k, computes $TID_{new} = RID_i \oplus h(n_k||ID_k||k)$, $M_7 = TID_{new} \oplus h(c_i||RID_i)$, $M_8 = c_k \oplus h(c_i||TID_{new}||RID_i)$, $SK_{ik} = h(c_k||c_i||TID_{new}||RID_i)$, and $M_9 = h(SK_{ik}||T_4)$. RSU_k sends (M_7, M_8, M_9, T_4) to V_i. After receiving the message, V_i computes $TID_{new} = M_7 \oplus h(c_i||RID_i)$, $c_k = M_8 \oplus h(c_i||TID_{new}||RID_i)$, and $SK_{ik} = h(c_k||c_i||TID_{new}||RID_i)$. Finally, V_i checks $M_9 \stackrel{?}{=} h(SK_{ik}||T_4)$. If these processes are completed, V_i and RSU_k are mutually authenticated and RSU_k uploads $(TID_{new}, n_k, ID_k, Sig_k(h(TID_{new}||RID_i||n_k)))$ to the blockchain.

E. Vehicle Revocation

During the communications, misbehavior of V_i can be revealed by a RSU. Then, the RSU can upload a transaction to revocate $h(RID_i||k)$ from the blockchain. If so, $h(RID_i||k)$ is revocated, and then V_i cannot communicate with other RSUs because the RSUs are sharing the blockchain transactions and can recognize that V_i is illegal. Furthermore, if V_i tries to re-register to TA, V_i should transmit ID_i to TA during the registration phase. However, TA can retrieve RID_i using ID_i and stored values in the secure memory, thus, TA rejects the registration request of V_i.

VI. SECURITY ANALYSIS

We analyze the security of the proposed scheme using informal analysis and formally prove the correctness and security

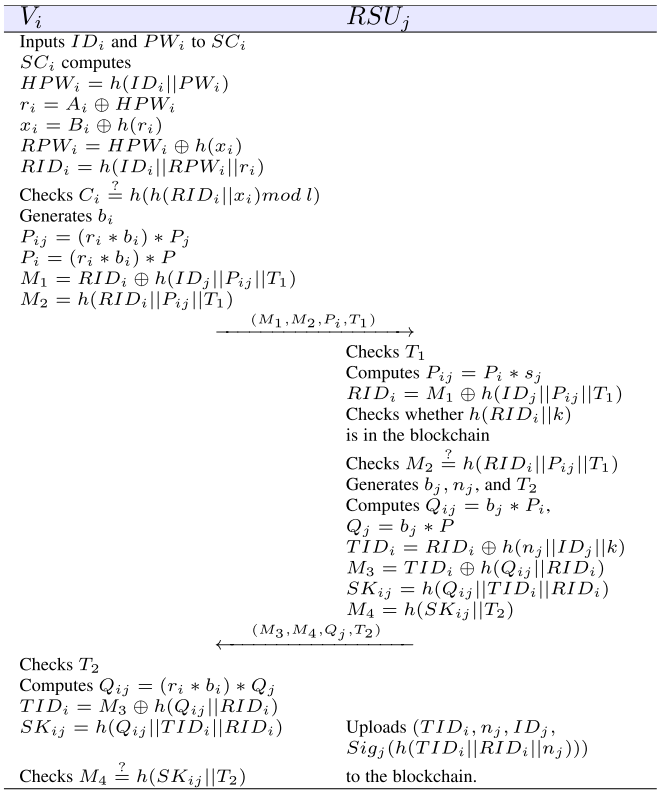

Fig. 3. Initial V2I authentication phase.

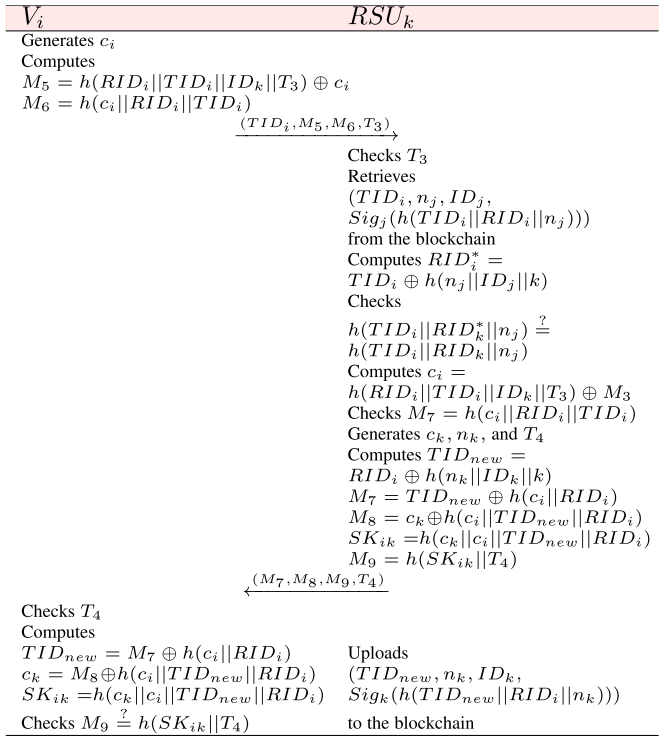

Fig. 4. Blockchain-based handover authentication phase.

utilizing BAN-logic analysis, ROR model, and "Automated Validation of Internet Security Protocols and Applications (AVISPA) software validation simulation tool".

A. *Informal Analysis*

We informally demonstrate that the proposed protocol has resistance to various attacks including replay, guessing, and impersonation attacks and can guarantee a variety of security features such as perfect forward secrecy and anonymity.

1) Replay and MITM Attack: If an adversary obtains messages sent on a public channel, the adversary cannot forge or modify the messages because each message includes the timestamp T_a $(a = 1, 2, 3, 4)$ and the message hashes (M_2, M_4, M_6, M_9), respectively. The adversary cannot obtain the real values hashed in (M_2, M_4, M_6, M_9). Thus, the proposed protocol defends replay and MITM attacks.

2) Smart Card Stolen Attack: By the adversary model, we assumed that an adversary can obtain or steal SC_i and extract the stored value (A_i, B_i, C_i). However, all values stored in SC_i are masked or hashed with ID_i and PW_i. Thus, the adversary cannot obtain any information about V_i, and the proposed protocol has resistance against smart card stolen attack.

3) Offline Guessing Attack: An adversary that obtains SC_i can attempt offline guessing attack using a dictionary containing 10^6 identities and passwords each. Even if the adversary achieves logging in to SC_i with ID_i^A and PW_i^A, the adversary still cannot know whether (ID_i^A, PW_i^A) are legal because D_i is masked with fuzzy verifier l. The probability of whether the guessed (ID_i^A, PW_i^A) are correct is $\frac{l}{10^{12}} \cong \frac{1}{2^{32}}$, which is negligible.

4) Impersonation Attack: A malicious vehicle V_A can impersonate to a legal V_i. In the initial authentication phase, V_A cannot obtain RID_i of V_i. Therefore, V_A cannot impersonate to V_i. Besides, V_A cannot obtain RID_i, thus, V_A cannot generate a legal authentication request message of blockchain-based authentication phase. Thus, the proposed protocol can defend against impersonation attacks.

5) Session Key Disclosure: An adversary can try calculating the session key SK_{ij} or SK_{ik} directly. The adversary must be able to attain Q_{ij} to calculate SK_{ij}. However, the adversary cannot compute Q_{ij} without solving ECDL problem, which is the mathematical problem of ECC. Also, the adversary cannot obtain SK_{ik} without RID_i. However, RID_i is hashed with ID_i and PW_i, which are veiled to the adversary. Therefore, the adversary cannot calculate the session keys.

6) Privileged-Insider Attack: An adversary can attain (ID_i, RPW_i) during vehicle registration phase. However, the adversary cannot compute SK_{ij} because the adversary cannot get Q_{ij} because of ECDL problem, and also cannot obtain RID_i, which is hashed with secret credentials. Also, the adversary cannot calculate SK_{ik} without random numbers c_k and c_i. Accordingly, the proposed protocol has resistance to privileged-insider attack.

7) Stolen Verifier Attack: An adversary can steal the verification table which stored in RSUs. Then, the adversary can attain information stored on the blockchain. Nevertheless, the adversary cannot obtain Q_{ij} because of ECDH problem. Accordingly, the adversary cannot calculate SK_{ij}. Also, the

TABLE III
NOTATIONS OF BAN-LOGIC

Notation	Description
η_1, η_2	Two principals
κ_1, κ_2	Two statements
SK	The session key
$\eta_1 \mid \equiv \kappa_1$	η_1 **believes** κ_1
$\eta_1 \mid \sim \kappa_1$	η_1 once **said** κ_1
$\eta_1 \Rightarrow \kappa_1$	η_1 **controls** κ_1
$\eta_1 \lhd \kappa_1$	η_1 **receives** κ_1
$\#\kappa_1$	κ_1 is **fresh**
$\{\kappa_1\}_K$	κ_1 is **encrypted** with K
$\eta_1 \overset{K}{\longleftrightarrow} \eta_2$	η_1 and η_2 have **shared** key K

adversary cannot calculate SK_{ik} without the secret key k and the pseudo-identity RID_i. Thus, the proposed protocol has resistance to stolen verifier attack.

8) Perfect Forward Secrecy: Even if the secret keys s_j and k are exposed to an adversary, the adversary still cannot calculate the session key of the initial authentication phase SK_{ij} because of Q_{ij}, which cannot be obtained without knowing random numbers b_j, r_i, and b_i. Furthermore, the adversary cannot compute SK_{ik} without knowing RID_i, which is veiled with random numbers c_i and c_k. Therefore, the proposed protocol can guarantee perfect forward secrecy.

9) Ephemeral Key Leakage Attack: If the random numbers (b_i, b_j, n_j) of the initial V2I authentication phase are leaked to an adversary, the adversary cannot reveal RID_i, and cannot calculate SK_{ij}. Also, if random numbers (c_i, ck) of blockchain-based V2I authentication phase are leaked, the adversary cannot calculate SK_{ik} without obtaining RID_i. Therefore, the proposed protocol has resistance to ephemeral key leakage attack.

10) Mutual Authentication: RSU_j and RSU_k can obtain RID_i during authentication phase from a message of V_i, and can retrieve $h(RID_i||k)$ from the blockchain. RID_i is hashed by ID_i, RPW_i, and r_i, which are unknown to any other vehicles except V_i. Therefore, RSUs can authenticate V_i. Furthermore, V_i receives M_4 from initial authentication phase, and M_9 from handover authentication phase. Therefore, V_i can check that the messages are respectively from RSU_j and RSU_k, and the proposed protocol can attain mutual authentication.

11) Anonymity and Untraceability: The authentication phases are conducted using the pseudo identity RID_i, and therefore, the real identity ID_i is not unveiled during the authentication phases. Furthermore, an adversary cannot obtain RID_i of V_i, for that reason, the proposed protocol can guarantee the vehicle anonymity. Also, TID_i is updated in the handover authentications, and the adversary cannot trace V_i using TID_i. Therefore, the proposed protocol can guarantee the untraceability.

B. Formal Proof Using BAN-Logic Analysis

BAN-logic analysis [11] is a verification tool that proves the correctness of the authentication protocol. We demonstrate that proposed handover authentication protocol provides mutual authentication using the BAN-logic analysis. Table III presents the notations of the BAN-logic.

1. Message meaning rule (MMR) :

$$\frac{\eta_1 \mid \equiv \eta_1 \overset{K}{\leftrightarrow} \eta_2, \quad \eta_1 \lhd \{\kappa_1\}_K}{\eta_1 \mid \equiv \eta_2 \mid \sim \kappa_1}$$

2. Nonce verification rule (NVR) :

$$\frac{\eta_1 \mid \equiv \#(\kappa_1), \quad \eta_1 \mid \equiv \eta_2 \mid \sim \kappa_1}{\eta_1 \mid \equiv \eta_2 \mid \equiv \kappa_1}$$

3. Jurisdiction rule (JR) :

$$\frac{\eta_1 \mid \equiv \eta_2 \mid \Longrightarrow \kappa_1, \quad \eta_1 \mid \equiv \eta_2 \mid \equiv \kappa_1}{\eta_1 \mid \equiv \kappa_1}$$

4. Belief rule (BR) :

$$\frac{\eta_1 \mid \equiv (\kappa_1, \kappa_2)}{\eta_1 \mid \equiv \kappa_1}$$

5. Freshness rule (FR) :

$$\frac{\eta_1 \mid \equiv \#(\kappa_1)}{\eta_1 \mid \equiv \#(\kappa_1, \kappa_2)}$$

1) Goals: The goals of BAN-logic to verify the correctness of the proposed scheme are as follows.

Goal 1: $V_i \mid \equiv V_i \overset{SK}{\longleftrightarrow} RSU_k$
Goal 2: $V_i \mid \equiv RSU_k \mid \equiv V_i \overset{SK}{\longleftrightarrow} RSU_k$
Goal 3: $RSU_k \mid \equiv V_i \overset{SK}{\longleftrightarrow} RSU_k$
Goal 4: $RSU_k \mid \equiv V_i \mid \equiv V_i \overset{SK}{\longleftrightarrow} RSU_k$

2) Idealized Forms: The idealized forms of the messages transmitted in the proposed protocol are as follows.

Msg_1: $V_i \rightarrow RSU_k : \{TID_i, c_i, T_3\}_{RID_i}$
Msg_2: $RSU_k \rightarrow V_i : \{TID_{new}, c_k, T_4\}_{RID_i}$

3) Assumptions: The basic assumptions to conduct the BAN logic are as follows.

A_1: $RSU_k \mid \equiv \#(T_3)$
A_2: $V_i \mid \equiv \#(T_4)$
A_3: $RSU_k \mid \equiv V_i \Rightarrow (V_i \overset{SK}{\longleftrightarrow} RSU_k)$
A_4: $V_i \mid \equiv RSU_k \Rightarrow (V_i \overset{SK}{\longleftrightarrow} RSU_k)$
A_5: $RSU_k \mid \equiv V_i \overset{RID_i}{\longleftrightarrow} RSU_k$
A_6: $V_i \mid \equiv V_i \overset{RID_i}{\longleftrightarrow} RSU_k$

4) BAN Logic Implementation: The implementation of the BAN logic to the proposed protocol is as follows.

Step 1: RSU_k receives Msg_1.
$S_1 : RSU_k \lhd \{TID_i, c_i, T_3\}_{RID_i}$
Step 2: The MMR can be applied using S_1 and A_5. Then, RSU_k believes that Msg_1 is from V_i.
$S_2 : RSU_k \mid \equiv V_i \mid \sim (TID_i, c_i, T_3)$
Step 3: The FR can be applied using A_1 and Msg_1. Then RSU_k believes that Msg_1 is fresh.
$S_3 : RSU_k \mid \equiv \#(TID_i, c_i, T_3)$

TABLE IV
QUERIES PERFORMED IN ROR MODEL

Query	Description
$Execute(\rho_{V_i}^{t_1}, \rho_{RSU_j}^{t_2}, \rho_{RSU_k}^{t_3})$	This query represents eavesdropping attack performed by A. A can obtain the messages between honest participants which is transmitted via open channels.
$CorruptSC(\rho_{V_i}^{t_1})$	This query denotes smart card stored in V_i is stolen by A. A can obtain stored values in the smart card.
$Send(\rho^t, M)$	Using this query, A sends message M to participant ρ^t. Also, A can receive the response to sent messages.
$Reveal(\rho^t)$	This query reveals the current session key between ρ^t and its partner A.
$Test(\rho^t)$	The semantic security of the session key can be verified using this query. There is a unbiased coin c, which of the heads represents 1 and the tails represents 0. If A performs $Test$ query, c is flipped, and ρ^t returns the session key when $c = 1$ and a random number when $c = 0$. Otherwise, ρ^t returns $NULL$.

Step 4: The NVR can be applied using S_2 and S_3. Then, RSU_k believes that V_i also believes Msg_1.
$S_4 : RSU_k| \equiv V_i| \equiv (TID_i, c_i, T_3)$
Step 5: The BR can be applied using S_4. Then, RSU_k believes c_i, which is included in Msg_1.
$S_5 : RSU_k| \equiv V_i| \equiv (c_i)$
Step 6: V_i receives Msg_2.
$S_6 : V_i \lhd \{TID_{new}, c_k, T_4\}_{RID_i}$
Step 7: The MMR can be applied using S_6 and A_6. Then, V_i believes that Msg_2 is from RSU_k.
$S_7 : V_i| \equiv RSU_k| \sim (TID_{new}, c_k, T_4)$
Step 8: The FR can be applied using A_2. Then V_i believes that Msg_2 is fresh.
$S_8 : V_i| \equiv \#(TID_{new}, c_k, T_4)$
Step 9: The NVR can be applied using S_7 and S_8. Then, V_i believes that RSU_k also believes Msg_2.
$S_9 : V_i| \equiv RSU_k| \equiv (TID_{new}, c_k, T_4)$
Step 10: The BR can be applied using S_9. Then, V_i believes c_k, which is included in Msg_2.
$S_{10} : V_i| \equiv RSU_k| \equiv (TID_{new}, c_k)$
Step 11: RSU_k and V_i believe that the other party can compute the session key because $SK = h(c_k||c_i||TID_{new}||RID_i)$ can be calculated using the shared values.
$S_{11} : RSU_K| \equiv V_i| \equiv (V_i \overset{SK}{\leftrightarrow} RSU_k)$ **(Goal 4)**
and,
$S_{12} : V_i| \equiv RSU_k| \equiv (V_i \overset{SK}{\leftrightarrow} RSU_k)$ **(Goal 2)**
Step 12: The JR can be applied to S_{11} and S_{12} using A_3 and A_4, respectively. Then, the BAN logic proof is completed.
$S_{13} : RSU_k| \equiv (V_i \overset{SK}{\leftrightarrow} RSU_k)$ **(Goal 3)**
and,
$S_{14} : V_i| \equiv (V_i \overset{SK}{\leftrightarrow} RSU_k)$ **(Goal 1)**

C. ROR Model

In this section, we prove the session key of the proposed protocol is secure under the "Real-Or-Random (ROR) model" [12]. The ROR model is widely-used [44]–[46] to prove that the session key is secure from an adversary A who tries passive and active attacks represented by queries. We denote ρ^t as the t^{th} instance of an executing participant. For instance, let $\rho_{V_i}^{t_1}$, $\rho_{RSU_j}^{t_2}$, and $\rho_{RSU_k}^{t_3}$ be t_1^{th}, t_2^{th}, and t_3^{th} instances of three participants V_i, RSU_j, and RSU_k, respectively. Then, we describe the queries (i.e. attacks) of the ROR model. A can perform the queries described in the Table IV.

Also, $Hash$ query means one-way hash function. We prove the following theorem to prove the session key security of the proposed protocol.

Theorem 1: We denote Adv_A is the advantage of A to distinguish the session key and a random number. Then,

$$Adv_A \leq \frac{q_H^2}{|Hash|} + \frac{2q_{send}}{|D_1||D_2|}, \tag{1}$$

where q_H and q_{send} means the number of $Hash$ and $Send$ queries performed by A, and $|Hash|$ is the range space of the $Hash$. D_1 and D_2 are the uniformly distributed identity and password dictionaries, and $|D_1|$ and $|D_2|$ are range space of each dictionary.

Proof: A can perform four games G_i $(i = 1, 2, 3, 4)$. After end of each game, if A can distinguish the session key and a random number accurately, A wins the game. We denotes $Suc_{G_i}^A$ is an event that A wins game $G_{i]}$, and the advantage of A to win game G_i is defined as $Adv_A^{G_i} = Pr[Suc_{G_i}^A]$, where $Pr[E]$ is an probability of an event E.

G_0 : In this game, A attempts "actual attack" to the proposed protocol. A directly guess the bit c. Since A guess the bit c randomly at the beginning of the game, the equation (2) can be induced by a definition of semantic security.

$$Advan_A = |2Pr[Suc_{G_0}^A] - 1| \tag{2}$$

G_1: A can attempt eavesdropping attack using $Execute$ query in this game. A can obtain all the transmitted messages in the authentication phases such as $(M_1, M_2.P_i, T_1)$, (M_3, M_4, Q_j, T_2), (TID_i, M_5, M_6, T_3), and (M_7, M_8, M_9, T_4). After obtaining the messages, A can executes $Reveal$ and $Test$ queries to verify that the output is the session key or a random number. The session keys $SK_{ij} = h(Q_{ij}||TID_i||RID_i)$ and $SK_{ik} = h(c_k||c_i||TID_{new}||RID_i)$ are protected using the hash function. Therefore, the advantage of A is equal to G_1. It follows that

$$Adv_A^{G_1} = Adv_A^{G_0} \tag{3}$$

G_2: In this game, A performs $Hash$ queries to distinguish the session key and a random number. A can $Hash$ query using the obtatined values using eavesdropping attack. However, A cannot obtain meaningful messages to calculate the session keys using eavesdropping attack. Therefore, A has to find the hash collision in the polynomial time to win this game. The advantage of A can be estimated using birthday paradox [47].

```
role veh(V,RSUJ,RSUK,TA : agent, SKrsujta, SKrsukta, SKvta : symmetric_key, H:
hash_func, SND, RCV : channel(dy))

played_by V
def=
local State: nat,
   MUL, ADD : hash_func,
   P, IDj, Sj, K, Pj, IDk, Sk, Pk, Sta, IDta  : text,
   IDi, PWi, Xi, HPWi, RPWi, Ri, RIDi, L, Ai, Bi, Ci : text,
   Bii, Pij, Pi, M1, M2, T1, Bj, Nj, T2, Qij, Qj, TIDi, M3, SKij, M4 :text,
   Cii, T3, M5, M6, Ck, Nk, T4, M7, M8, M9, SKik, TIDnew: text
const secp1, secp2, secp3, secp4,secp5,secp6, rsuv_bj, vrsuj_bii, rsukv_ck,
vrsuk_nj: protocol_id
init State := 2
transition

1. State = 2 /\ RCV(start) =|>
State' := 3 /\ Xi' := new() /\ HPWi' := H(IDi.PWi)
      /\ RPWi' := xor(HPWi,H(Xi'))
      /\ SND({IDi.RPWi'}_SKvta)
         /\ secret({IDi},secp4,{TA,V})
      /\ secret({PWi,Xi'},secp5,{V})

2. State = 1 /\ RCV({Ri'.L.Xi'}_SKvta) =|>
State' := 2 /\ RIDi' := H(IDi.xor(H(IDi.PWi),H(Xi')).Ri')
      /\ Ai' := xor(Ri',H(IDi.PWi))
      /\ Bi' := xor(Xi',H(Ri'))
      /\ Ci' := H(H(RIDi'.Xi'))
%%%%%%%%%%%%%Login & Authentication phase
      /\ Bii' := new() /\ Pij' := MUL(MUL(Ri'.Bii').MUL(H(IDj.Sta).P))
      /\ Pi' := MUL(MUL(Ri'.Bii').P) /\ T1' := new()
      /\ M1' := xor(RIDi',H(IDj.Pij'.T1'))
      /\ M2' := H(RIDi'.Pij'.T1')
      /\ SND(M1'.M2'.Pi'.T1')
      /\ witness(V,RSUJ,vrsuj_bii,Bii')

3. State = 2
/\ RCV(xor(xor(H(IDi.xor(H(IDi.PWi),H(Xi')).Ri'),H(Nj'.IDj.H(IDta.Sta))),H(MUL(
Bj'.MUL(MUL(Ri'.Bii').P)).H(IDi.xor(H(IDi.PWi),H(Xi')).Ri'))).H(H(MUL(Bj'.MUL(
MUL(Ri'.Bii').P)).xor(H(IDi.xor(H(IDi.PWi),H(Xi')).Ri'),H(Nj'.IDj.H(IDta.Sta))).H(I
Di.xor(H(IDi.PWi),H(Xi')).Ri')).T2').MUL(Bj'.P).T2') =|>
State' := 3 /\ Cii' := new() /\ T3' := new()
         /\ M5' :=
xor(H(H(IDi.xor(H(IDi.PWi),H(Xi')).Ri').xor(H(IDi.xor(H(IDi.PWi),H(Xi')).Ri'),H(
Nj'.IDj.H(IDta.Sta))).IDk.T3'),Cii')
      /\ M6' :=
H(Cii'.H(IDi.xor(H(IDi.PWi),H(Xi')).Ri').xor(H(IDi.xor(H(IDi.PWi),H(Xi')).Ri'),H(N
j'.IDj.H(IDta.Sta))))

/\ SND(xor(H(IDi.xor(H(IDi.PWi),H(Xi')).Ri'),H(Nj'.IDj.H(IDta.Sta))).M5'.M6'.T3')
      /\ witness(V,RSUK,vrsuk_nj,Nj')
      /\ request(RSUJ,V,rsuv_bj,Bj')

4. State = 3
/\ RCV(xor(xor(H(IDi.xor(H(IDi.PWi),H(Xi')).Ri'),H(Nk'.IDk.H(IDta.Sta))),H(Cii'.
H(IDi.xor(H(IDi.PWi),H(Xi')).Ri'))).xor(Ck',
H(Cii'.xor(H(IDi.xor(H(IDi.PWi),H(Xi')).Ri'),H(Nk'.IDk.H(IDta.Sta))).H(IDi.xor(H(I
Di.PWi),H(Xi')).Ri'))).H(H(Ck'.Cii'.xor(H(IDi.xor(H(IDi.PWi),H(Xi')).Ri'),H(Nk'.IDk
.H(IDta.Sta))).H(IDi.xor(H(IDi.PWi),H(Xi')).Ri')).T4').T4') =|>
State' := 4 /\ TIDnew' :=
xor(H(IDi.xor(H(IDi.PWi),H(Xi')).Ri'),H(Nk'.IDk.H(IDta.Sta)))
      /\ SKik' := H(Ck'.Cii'.TIDnew'.H(IDi.xor(H(IDi.PWi),H(Xi')).Ri'))
      /\ request(RSUK,V, rsukv_ck, Ck')

end role
```

Fig. 5. *Role* of Vehicle.

$$|Adv_A^{G_2} - Adv_A^{G_1}| \leq \frac{q_H^2}{2|Hash|} \tag{4}$$

G_3: A can simulate $Send$ and $CorruptSC$ queries in this game. A can obtain the stored value in the smart card (A_i, B_i, C_i). However, A cannot derive the session key using these values, because all the values obtained from the smart card are masked with ID_i, PW_i, which are secret values. To win this game, A has to guess the identity and password pair simultaneously in polynomial time. Let D_1 be a password dictionary and D_2 be a identity dictionary. Then, we get

$$|Adv_A^{G_3} - Adv_A^{G_2}| \leq \frac{q_{send}}{|D_1||D_2|} \tag{5}$$

It only remains to guess c correctly for A to win the game. Finally, we can get the following equation:

$$Adv_A^{G_3} = \frac{1}{2} \tag{6}$$

Using equations (2),(3), and (6), we can get the following equation:

$$\begin{aligned} \frac{1}{2} Adv_A &= \left| Adv_A^{G_0} - \frac{1}{2} \right| \\ &= \left| Adv_A^{G_1} - Adv_A^{G_3} \right| \end{aligned} \tag{7}$$

Applying the triangular inequality to the equation (7), then

$$\begin{aligned} Adv_A &= 2|Adv_A^{G_1} - Adv_A^{G_3}| \\ &\leq 2|Adv_A^{G_1} - Adv_A^{G_2}| + 2|Adv_A^{G_2} - Adv_A^{G_3}| \\ &\leq \frac{q_H^2}{|Hash|} + \frac{2q_{send}}{|D_1||D_2|} \end{aligned} \tag{8}$$

After all the queries are performed, the advantage of A is negligibly small, and therefore, the session key of the proposed protocol is secure under ROR model. ■

D. Formal Security Verification: AVISPA Simulation

In this section, we prove the security of the proposed protocol using "Automated Validation of Internet Security Protocols and Applications (AVISPA)" [13], [48], which is a widely-accepted simulation tool to confirm that an authentication protocol can defend against MITM and replay attacks. In AVISPA, High-Level Protocol Specification Language (HLPSL) [49] is utilized to implement a protocol, and there are four back-ends models: a) "On-the-Fly Model Checker (OFMC)" [50], "Constraint Logic-based Attack Searcher (CL-AtSe)" [51], "Tree Automata based on Automatic Approximations for Analysis of Security Protocol (TA4SP)," and "SAT-based Model Checker (SATMC)". The HLPSL inputs one of the four models. Then, the input is converted to "Intermediate Format (IF)," and generates the output "Output Format (OF)". Generally, an authentication protocol can be said to have has resistance to replay and MITM attacks if OF is safe under CL-AtSe and OFMC models.

Fig. 5 represents the role of V_i based on HLPSL. In the first state, V_i sends (ID_i, HPW_i) to TA in the registration phase. After V_i receives SC_i, V_i authenticates with RSU_i. Next, V_i authenticates with RSU_k. The role of RSU_j, RSU_k, and TA are also implemented similarly to V_i using HLPSL. The HLPSL code demonstrated in Fig. 6 shows that each session, variables and functions used in the environment, and checking the secrecy and authentication for each session. The simulation result is summarized in Fig. 7. It takes 1.16 seconds for translation time in CL-AtSe model, and it takes 156.86 seconds for visiting 4880 nodes with 12 piles depth under OFMC Model. The summaries showed that the proposed protocol is

```
role session(V, RSUJ, RSUK, TA : agent, SKrsujta, SKrsukta, SKvta : symmetric_key,
H: hash_func)

def=
local SEN1, SEN2, SEN3, SEN4, REV1, REV2, REV3, REV4: channel(dy)
composition
roadunitj(RSUJ, RSUK, V, TA, SKrsujta, SKrsukta, SKvta, H, SEN1, REV1)
/\ roadunitk(RSUJ, RSUK, V, TA, SKrsujta, SKrsukta, SKvta, H, SEN2, REV2)
/\ veh(RSUJ, RSUK, V, TA, SKrsujta, SKrsukta, SKvta, H, SEN3, REV3)
/\ authority(RSUJ, RSUK, V, TA, SKrsujta, SKrsukta, SKvta, H, SEN4, REV4)
end role

role environment()
def=
const rsuj, rsuk, v, ta : agent,
skrsujta, skrsukta, skvta: symmetric_key,
h,mul,add: hash_func,
idi,idj, idk, pj, pk, p: text,
rsuv_bj, vrsuj_bii, rsukv_ck, vrsuk_nj: protocol_id,
secp1, secp2, secp3, secp4,secp5,secp6 :protocol_id

intruder_knowledge = {rsuj, rsuk, v, ta, idi, idj, idk, pj, pk, p, h, mul}
composition
session(rsuj, rsuk, v, ta, skrsujta, skrsukta, skvta, h)
/\session(i, rsuk, v, ta, skrsujta, skrsukta, skvta, h)
/\session(rsuj, i, v, ta, skrsujta, skrsukta, skvta, h)
/\session(rsuj, rsuk, i, ta, skrsujta, skrsukta, skvta, h)
/\session(rsuj, rsuk, v, i, skrsujta, skrsukta, skvta, h)

end role

goal
secrecy_of secp1, secp2, secp3, secp4, secp5, secp6
authentication_on rsuv_bj, vrsuj_bii, rsukv_ck, vrsuk_nj
end goal

environment()
```

Fig. 6. *Role* of session, environment, and goal.

safe, and therefore, we can say that the proposed protocol has resistance to replay and MITM attacks.

VII. Performance Analysis

We compare the computational costs occurred during the handover authentication of the proposed protocol with the existing protocols [17], [18], [25]. Besides, we compare the security features with the existing protocols to show that the proposed protocol is more secure.

A. Computational Cost

We simulate the computational cost of each operation using the MIRACL library [52] and pairing-based cryptography (PBC) library [53]. Considering the different computing power of RSU and the vehicle, we conducted experiments in desktop environment and Raspberry PI environment respectively. The specification of the desktop is quad-core i7-4790 CPU, 16 GB RAM, and the operating system is Linux Ubuntu 20.04-desktop-amd64, and Raspberry PI 3B is quad-core ARM Cortex-A53, 1 GB RAM. The operations we execute are as follows:

- T_{bp}: Bilinear pairing operation
- T_{bp}^{mul}: Scalar multiplication operation on a pairing-based group
- T_{ecc}^{mul}: Scalar multiplication on a elliptic curve-based group
- T_{ecc}^{add}: Addition on a elliptic curve-based group

```
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL
PROTOCOL
 /home/span/span/testsuite/results/handover.if
GOAL
 As Specified
BACKEND
 CL-AtSe
STATISTICS
 Analysed  : 4 states
 Reachable  : 0 states
 Translation: 1.16 seconds
 Computation: 0.01 seconds
```

```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/handover.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 156.86s
 visitedNodes: 4880 nodes
 depth: 12 plies
```

Fig. 7. Simulation results using CL-AtSe and OFMC backends of AVISPA.

TABLE V
Simulation Results in Each Environment

Operation	Computational cost	
	Desktop	Raspberry PI 3B
T_{mul}^{ecc}	1.489 ms	2.579 ms
T_{add}^{ecc}	0.008 ms	0.019 ms
T_{mul}^{bp}	2.521 ms	5.611 ms
T_{add}^{bp}	0.018 ms	0.043 ms
T_{bp}	13.440 ms	46.130 ms
T_{hash}	0.003 ms	0.021 ms
$T_{mod-exp}$	1.864 ms	5.119 ms
$T_{aes-enc}$	0.002 ms	0.013 ms
$T_{aes-dec}$	0.001 ms	0.012 ms

- $T_{mod-exp}$: Modular exponentiation
- $T_{aes-enc}$: AES-256 encryption
- $T_{aes-dec}$: AES-256 decryption
- T_h: SHA-256 Hash function

The computational costs of operations for each environment are as summarized in Table V. We do not consider the execution time of XOR operation, which is negligible. Table VI summarizes total computational cost of the proposed protocol and existing protocols occurred in handover situations. V_i is a vehicle, RSU_j and RSU_k are RSUs that authenticate with V_i during initial authentication phase and handover authentication phase, respectively. The computational loads to RSU_k of the proposed protocol is slightly higher than the scheme in [18]. However, the scheme in [18] does not provide specific handover authentication protocol, and requires much more computation cost than our protocol. In the proposed protocol, vehicle only executes hash operations, and therefore, the proposed protocol has considerably lightweight computational cost in the vehicle side.

B. Practical Perspective: NS-3 Simulation

We conduct a simulation study on the proposed protocol using NS-3 simulator to measure the impact of the proposed protocol on network parameters such as throughput and end-to-end delay. We considered three scenarios based on the number of vehicles. For each scenario, the number of vehicles is 10, 20, 30, 40, and 50. The mobility is $20m$ per second for all scenarios. The simulation parameters are summarized in Table VII.

We simulated each scheme using NS-3 to compare the end-to-end delay and throughput. The proposed scheme and the scheme in [17] are two-party authentication, and the schemes of [18] and [25] are three-party authentication. To compare [18] and [25]

TABLE VI
COMPUTATIONAL COST COMPARISON

Scheme	V_i	RSU	
		RSU_j	RSU_k
Gao *et al.* [17]	$T_{mtp}+T_{mul}^{bp}+T_{aes-enc}+T_{aes-dec} \approx$ 21.168 ms	–	$2T_{bp}+T_{mul}^{bp}+T_{aes-enc}+T_{aes-dec} \approx$ 31.925 ms
Xu *et al.* [18]	$3T_{mul}^{ecc}+2T_h \approx$ 7.779 ms	$T_{hash} \approx$ 0.003 ms	$2T_{mul}^{ecc}+2T_h \approx$ 2.984 ms
Wang *et al.* [25]	$T_{bp}+T_{mod-exp}+T_{mul}^{bp} \approx$ 56.86 ms	$2T_{mod-exp} \approx$ 3.728 ms	$T_{bp}+T_{mod-exp}+T_{mul}^{bp} \approx$ 17.825 ms
Proposed	$6T_h \approx$ 0.126 ms	–	$4T_{ecc}^{mul}+T_{ecc}^{add}+12T_h \approx$ 6.024 ms

[0]– : No computation cost.

TABLE VII
SIMULATION PARAMETERS

Parameters	Values
Operating systems	Ubuntu 16.04 LTS
Simulator	NS 3.29
Simulation area	1000 * 1000 m^2
Range of RSUs	250 m
Number of vehicles	10, 20, 30, 40, and 50
Number of RSUs	25
Mobility	20mps for all scenarios
Transmission range	300 m
Routing protocol	Ad Hoc On-Demand Distance Vector (AODV)
Wireless channel bandwidth	6 Mbps
Simulation time	30 minutes

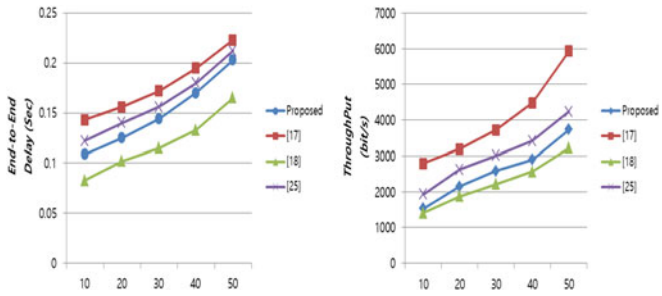

Fig. 8. Simulation results.

with the proposed scheme in the same simulation environment, we conducted the simulation integrating two RSUs used in the scheme of [18] and [25], respectively. Then, we measured end-to-end delay and throughput of the proposed scheme and the other schemes. For the simulation, we assume the hash output and a random nonce are 32 bytes, the BLS signature is 128 bytes, a point on a pairing-based curve is 128 bytes, a point on a elliptic curve is 32 bytes, a token is 32 bytes, a certificate is 256 bytes, a handover request/response is 32 bytes, an identity is 10 bytes, and a timestamp is 4 bytes, In the proposed handover phase, V_i sends 100 bytes length message, and receives 100 bytes length message from RSU_k. In [17], a vehicle sends 548 bytes length message, receives 216 bytes length message from a RSU, and sends 32 bytes length message to the RSU. In [18], V_i send 32 bytes length message to RSU_j, RSU_j sends 32 bytes length message to RSU_k. We integrated it as V_i transmits 64 bytes length message to RSU_k. Then, RSU_j sends 32 bytes length message to V_i. After that, V_i transmits 32 bytes length message to RSU_k and RSU_k sends 64 bytes length message to V_i. In [25], RSU_j transmits 128 bytes length message to RSU_k, and RSU_k sends 32 bytes length message to V_i. We integrated it as RSU_k transmits 160 bytes length message to V_i. After that, RSU_k transmits 128 bytes length message to V_i.

TABLE VIII
SECURITY FEATURES COMPARISON

Security features	[17]	[18]	[25]	Proposed
A1	O	O	O	O
A2	O	O	O	O
A3	O	O	O	O
A4	–	–	–	O
A5	–	–	–	O
A6	–	–	–	O
A7	X	X	X	O
A8	X	X	X	O
A9	O	X	–	O
A10	O	O	O	O
A11	O	O	O	O
A12	X	X	O	O

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

We obtain the end-to-end delay and throughput of each scheme. Fig. 8 shows the simulation results of the proposed scheme and [17], [18], and [25]. The end-to-end delay can be formulated as $\Sigma_{i=1}^{n_p}(T_r - T_s)/n_p$. i, T_r, T_s, and n_p represent a data packet, time for receiving and sending messages, and total number of packets, respectively. The end-to-end delay of the proposed scheme is slightly higher compared to [18]. However, the proposed scheme has lower delay compared to [17] and [25], and more secure than [25]. The throughput can be formulated as $r_p * |p|/T_s$. r_p is the number of received packets, $|p|$ is its size, and T_s is a total time in second. If the total throughput is high, it can cause more load as the number of vehicles increase. Similar to the results of end-to-end delay, the total throughput of the proposed scheme is slightly higher compared to [18], because the total size of the messages in [18] is smaller than the total size of the messages in the proposed scheme. However, the proposed scheme has more security features than [18] as shown in Table VIII and has lower throughput compared to [17] and [25].

C. Security Features

Table VIII presents the security features of the proposed protocol and the existing protocols. We consider security and functional features such as A1: "resistance to replay attack," A2: "resistance to impersonation attack," A3: "resistance to session key disclosure attack," A4: "resistance to privileged-insider attack," A5: "preservation of perfect forward secrecy," A6: "resistance to ephemeral key leakage attack," A7: "support of RSU fault tolerance," A8: "support of handover integrity," A9: "support of mutual authentication," A10: "preservation of anonymity," A11: "preservation of untraceability," and A12: "support of decentralization". As

analyzed in Section VI-A, the proposed protocol can ensure the security features. However, the existing schemes [17], [18], [25] do not consider or cannot ensure the security features. Table VIII demonstrates that the proposed protocol can provide superior security compared to the existing protocols.

The proposed protocol considers more attacks that can occur in wireless channels, and provide better security compared with the existing protocols.

VIII. Conclusion

We designed a V2I handover authentication using blockchain to reduce the unnecessary computations incurred during the re-authentications and a vehicle revocation without help of TA for blockchain-based VANET model. We informally analyzed that the proposed protocol can defend against various attacks and can provide many security features. Also, we proved the correctness and semantic security of the proposed protocol using BAN logic and ROR model, respectively. We used AVISPA simulation tool to verify that the proposed protocol is secure against replay and MITM attacks. Furthermore, compared to the existing protocols, the proposed protocol significantly reduced computational cost on the vehicle and can provide more security features. Finally, we utilized NS-3 to demonstrate that the proposed protocol is practical. In future work, we will implement the proposed scheme and design an improved scheme considering the overhead in the RSU caused during the block consensus.

Acknowledgment

The authors would like to thank the reviewers and the Associate Editor for their valuable suggestions that helped in improving the quality, readability and presentation of the paper.

References

[1] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Netw.*, vol. 61, pp. 33–50, Jun. 2017.

[2] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, "AKM-IoV: Authenticated key management protocol in fog computing-based Internet of Vehicles deployment," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8804–8817, Oct. 2019.

[3] K. Park *et al.*, "LAKS-NVT: Provably secure and lightweight authentication and key agreement scheme without verification table in medical Internet of Things," *IEEE Access*, vol. 8, pp. 119387–119404, 2020.

[4] J. Lee, S. Yu, M. Kim, Y. Park, and A. K. Das, "On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks," *IEEE Access*, vol. 8, pp. 107046–107062, 2020.

[5] H. Zhong, L. Pan, Q. Zhang, and J. Cui, "A new message authentication scheme for multiple devices in intelligent connected vehicles based on edge computing," *IEEE Access*, vol. 7, pp. 108211–108222, 2019.

[6] A. Lei *et al.*, "A blockchain based certificate revocation scheme for vehicular communication systems," *Future Gener. Comput. Syst.*, vol. 110, pp. 892–903, Sep. 2020.

[7] X. Liu, H. Huang, F. Xiao, and Z. Ma, "A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4101–4112, May 2020.

[8] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.

[9] P. Bagga, A. K. Das, A. K. Sutrala, and P. Vijayakumar, "Blockchain-based batch authentication protocol for Internet of Vehicles," *J. Syst. Architecture*, vol. 113, 2021, Art. no. 101877.

[10] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling Byzantine agreements for cryptocurrencies," in *Proc. 26th Symp. Operating Syst. Princ.*, Shanghai, China, 2017, pp. 51–68.

[11] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.

[12] M. Abdalla, P. A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," *Proc. 8th Int. Workshop Theory Pract. Public Key Cryptogr.*, Les Diablerets, Switzerland, vol. 3386, pp. 65–84, 2005.

[13] AVISPA, "Automated validation of internet security protocols and applications," 2020. Accessed: Dec. 2021. [Online]. Available: http://www.avispa-project.org/

[14] "NS-3.28," 2018. Accessed: Dec. 2021. [Online]. Available: http://www.nsnam.org/ns-3-28/

[15] N. Lo and J. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 5, pp. 1319–1328, May 2016.

[16] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2740–2749, Oct. 2017.

[17] T. Gao, X. Deng, N. Guo, and X. Wang, "An anonymous authentication scheme based on PMIPv6 for VANETs," *IEEE Access*, vol. 6, pp. 14686–14698, Feb. 2018.

[18] C. Xu, X. Huang, M. Ma, and H. Bao, "An anonymous handover authentication scheme based on LTE-A for vehicular networks," *Wireless Commun. Mobile Comput.*, vol. 2018. pp. 1–15, Jul. 2018.

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

[20] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.

[21] X. Zhang and X. Chen, "Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 58241–58254, 2019.

[22] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, 2019.

[23] Q. Feng, D. He, S. Zeadally, and K. Liang, "BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks," *IEEE Trans. Ind. Inform.*, vol. 16, no. 6, pp. 4146–4155, Jun. 2020.

[24] Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu, and W. He, "An efficient decentralized key management mechanism for VANET with blockchain," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5836–5849, Jun. 2020.

[25] C. Wang, J. Shen, J. Lai, and J. Liu, "B-TSCA: Blockchain assisted trustworthiness scalable computation for V2I authentication in VANETs," *IEEE Trans. Emerg. Top. Comput.*, vol. 9, no. 3, pp. 1386–1396, Jul.–Sep. 2021.

[26] N. Koblitz, "Elliptic curves cryptosystems," *Math. Comput.*, vol. 48, pp. 203–209, Sep. 1987.

[27] B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz, and M. Alazab, "Blockchain-envisioned secure data delivery and collection scheme for 5G-based IoT-enabled internet of drones environment," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 9097–9111, Aug. 2020.

[28] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Inform.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.

[29] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-Health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, no. 8, Aug. 2018, Art. no. 140.

[30] S. Son, J. Lee, M. Kim, S. Yu, A. K. Das, and Y. Park, "Design of secure authentication protocol for cloud-assisted telecare medical information system using blockchain," *IEEE Access*, vol. 8, pp. 192177–192191, 2020.

[31] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. 3rd USENIX Symp. Operating Syst. Des. Implementation*, New Orleans, LA, USA, 1999, pp. 173–86.

[32] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[33] A. K. Sutrala, P. Bagga, A. K. Das, N. Kumar, J. J. P. C. Rodrigues, and P. Lorenz, "On the design of conditional privacy preserving batch verification-based authentication scheme for Internet of Vehicles deployment," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5535–5548, May 2020.
[34] A. Dua, N. Kumar, A. K. Das, and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4359–4373, May 2018.
[35] M. Kim, S. Yu, J. Lee, Y. Park, and Y. Park, "Design of secure protocol for cloud-assisted electronic health record system using blockchain," *Sensors*, vol. 20, no. 10, May 2020, Art. no. 2913.
[36] S. Yu, J. Lee, Y. Park, and Y. Park, "A secure and efficient three-factor authentication protocol in global mobility networks," *Sensors*, vol. 10, no. 10, May 2020, Art. no. 3565.
[37] S. Yu, J. Lee, K. Lee, K. Park, and Y. Park, "Secure authentication protocol for wireless sensor networks in vehicular communications," *Sensors*, vol. 18, no. 10, pp. 3191–3213, 2018.
[38] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Annu. Int. Cryptol. Conf.*, 1999, pp. 388–397.
[39] J. Lee, S. Yu, M. Kim, Y. Park, and A. K. Das, "On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks," *IEEE Access*, vol. 8, pp. 107046–107062, 2020.
[40] S. Yu *et al.*, "Privacy-preserving lightweight authentication protocol for demand response management in smart grid environment," *Appl. Sci.*, vol. 10, no. 5, Mar. 2020, Art. no. 1758.
[41] K. Park, Y. Park, Y. Park, and A. K. Das, "2PAKEP: Provably secure and efficient two-party authenticated key exchange protocol for mobile environment," *IEEE Access*, vol. 6, pp. 30225–30241, 2018.
[42] Y. Park and Y. Park, "Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks," *Sensors*, vol. 16, no. 12, Dec. 2016, Art. no. 2123.
[43] K. Park, Y. Park, A. K. Das, S. Yu, J. Lee, and Y. Park, "A dynamic privacy-preserving key management protocol for V2G in social Internet of Things," *IEEE Access*, vol. 7, pp. 76812–76832, 2019.
[44] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, K. -K. R. Choo, and Y. H. Park, "On the design of mutual authentication and key agreement protocol in Internet of Vehicles-enabled intelligent transportation system," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1736–1751, Feb. 2021, doi: 10.1109/TVT.2021.3050614.
[45] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6903–6916, Jul. 2019.
[46] B. Bera, A. K. Das, and A. K. Sutrala, "Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment," *Comput. Commun.*, vol. 166, no. 15, pp. 91–109, 2021.
[47] V. Boyko, P. Mackenzie, and S. Patel, "Provably secure password authenticated key exchange using Diffie-Hellman," in *Proc. Int. Conf. Theory Appl. Cryptol. Tech. Adv. Cryptol.*, Bruges, Belgium, 2000, pp. 156–171.
[48] AVISPA, "SPAN, a security protocol animator for AVISPA," Accessed: Dec. 2021. [Online]. Available: http://www.avispa-project.org/
[49] D. V. Oheimb, "The high-level protocol specification language HLPSL developed in the EU project AVISPA," in *Proc. 3rd APPSEM II Workshop Appl. Semantics*, Frauenchiemsee, Germany, 2005, pp. 1–17.
[50] D. Basin, S. Modersheim, and L. Vigano, "OFMC: A symbolic model checker for security protocols," *Int. J. Inf. Secur.*, vol. 4, no. 3, pp. 181–208, 2005.
[51] M. Turuani, "The CL-Atse protocol analyser," in *Proc. Int. Conf. Rewriting Techn. Appl.*, Seattle, WA, USA, 2006, pp. 227–286.
[52] Miracl library, Accessed: Dec. 2021. [Online]. Available: https://github.com/miracl/MIRACL
[53] Pairing-based cryptography library, Accessed: Dec. 2021. [Online]. Available: http://crypto.stanford.edu/pbc/

Seunghwan Son received the B.S. degree in mathematics in 2019 from Kyungpook National University, Daegu, South Korea, where he is currently working toward the M.S. degree with the School of Electronic and Electrical Engineering. His research interests include authentication, blockchain, cryptography, and information security.

Joonyoung Lee received the B.S. and M.S. degrees in electronics engineering in 2018 and 2020, respectively, from Kyungpook National University, Daegu, South Korea, where he is currently working toward the Ph.D. degree with the School of Electronic and Electrical Engineering. His research interests include authentication, Internet of Things, and information security.

Yohan Park received the B.S., M.S., and Ph.D. degrees in electronic engineering from Kyungpook National University, Daegu, South Korea, in 2006, 2008, and 2013, respectively. He is currently a Professor with the School of Computer Engineering, Keimyung University, Daegu, South Korea. His research interests include computer networks, mobile security, and information security.

Youngho Park (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electronic engineering from Kyungpook National University, Daegu, South Korea, in 1989, 1991, and 1995, respectively. He is currently a Professor with the School of Electronic and Electrical Engineering, Kyungpook National University. From 2003 to 2004, he was a Visiting Scholar with the School of Electrical Engineering and Computer Science, Oregon State University, Corvallis, OR, USA. From 1996 to 2008, he was a Professor with the School of Electronic and Electrical Engineering, Sangju National University, Sangju, South Korea. His research interests include computer networks, multimedia, and information security.

Ashok Kumar Das (Senior Member, IEEE) received the M.Sc. degree in mathematics, the M.Tech. degree in computer science and data processing, and the Ph.D. degree in computer science and engineering from the Indian Institute of Technology(IIT) Kharagpur, Kharagpur, India. He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. He has authored more than 270 papers in international journals and conferences in his research areas, including more than 230 reputed journal papers. His current research interests include cryptography and network security including security in smart grid, Internet of Things, Internet of Drones, Internet of Vehicles, cyber-physical systems, cloud computing, and blockchain and AI/ML security. He is on the editorial board of the IEEE SYSTEMS JOURNAL, *Journal of Network and Computer Applications (Elsevier)*, *Computer Communications (Elsevier)*, *IET Communications*, *KSII Transactions on Internet and Information Systems*, and *International Journal of Internet Technology and Secured Transactions (Inderscience)*. He was a Program Committee Member of many international conferences. He was also one of the Technical Program Committee Chair of the first International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, June 2019, and second International Congress on Blockchain and Applications (BLOCKCHAIN'20), L'Aquila, Italy, October 2020. He was the recipient of the Institute Silver Medal from IIT Kharagpur.