IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 25 May 2023, accepted 9 June 2023, date of publication 14 June 2023, date of current version 21 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3286016

RESEARCH ARTICLE

Design of Secure and Lightweight Authentication Scheme for UAV-Enabled Intelligent Transportation Systems Using Blockchain and PUF

SEUNGHWAN SON[1], DEOKKYU KWON[1], (Graduate Student Member, IEEE), SANGWOO LEE[2], YONGSUNG JEON[2], ASHOK KUMAR DAS[3], (Senior Member, IEEE), AND YOUNGHO PARK[1], (Member, IEEE)

[1]School of Electronic and Electrical Engineering, Kyungpook National University, Daegu 41566, South Korea
[2]Electronics and Telecommunications Research Institute, Daejeon 34129, South Korea
[3]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India

Corresponding author: Youngho Park (parkyh@knu.ac.kr)

This work was supported by the Institute of Information and Communications Technology Planning and Evaluation (IITP) Grant by the Korean Government through the Ministry of Science and Information and Communication Technology (MSIT) (Study on Wireless Covert Channel Risk Verification) under Grant 2020-0-00913.

ABSTRACT Unmanned-aerial-vehicle (UAV)-enabled intelligent transportation system (ITS) is an advanced technology that can provide various services including autonomous driving, real-time creation of high-definition maps, and car sharing. In particular, a UAV-enabled ITS can be realized through the combination of traditional vehicular ad hoc networks (VANETs) and UAVs that can act as flying roadside units (RSUs) at the outskirts and monitor road conditions from predefined locations to spot car accidents and any law violations. Notably, to realize these services, real-time communication between UAVs and RSUs must be guaranteed. However, UAVs have limited computing powers, and if extensive computation is required during communication, the provision of real-time ITS services may be hindered. Furthermore, UAVs and RSUs communicate via public channels that are prone to various attacks, such as replay, impersonation, trace, and session key disclosure attacks. Thus, in this article, a secure and lightweight authentication scheme is proposed for UAVs and RSUs using the blockchain technology. The proposed scheme is analyzed using informal and formal methods including Burrows–Abadi–Nikoogadam (BAN) logic, automated validation of internet security protocols and applications (AVISPA) simulation tool, and real–or–random (RoR) model, and its performance is compared with that of related schemes. The results reveal that the proposed scheme is more efficient and secure as compared to the other competing schemes.

INDEX TERMS Blockchain, wireless communication, unmanned aerial vehicle, lightweight authentication, physically unclonable function, security.

I. INTRODUCTION

Intelligent transportation system (ITS) [1] is a technology that scientifically automates the operation of the transportation system to improve efficiency and safety. Through ITS, various services such as autonomous driving, real-time creation of high-definition maps, and car sharing can be realized. These services are provided through various interactions such as V2I (Vehicle-to-Infrastructure), V2V (Vehicle-to-Vehicle), and V2P (Vehicle-to-Person), and the ultimate goal is to realize complete full automation driving [3]. So far, conditional automation has been partly implemented, and the realization of high automation and full automation is expected in the near future.

However, there are still some difficulties in realizing a high level of autonomous driving. For the first reason, vehicles

The associate editor coordinating the review of this manuscript and approving it for publication was Jiankang Zhang.

generally have a limited field of view [4], [5], and the raw data available from vehicles have low qualities which are unsuitable for high-level autonomous drivings. For the second reason, Equipping RSU in all suburban and rural areas is expensive and inefficient, ITS services is available to vehicles driving in non-RSU-equipped rural areas. Unmanned aerial vehicles (UAVs)(i.e., drones) can be a solution for these problems [6], [7]. For example, UAVs can be deployed on congested roads with limited vehicle visibility to monitor road conditions. Furthermore, UAVs can be deployed in rural areas and can act as gateways between vehicles and RSUs to provide real-time ITS services. UAV-enabled ITS has a lot of potential and is developed actively.

However, UAVs and RSUs communicate via wireless channels that are prone to replay, man-in-the-middle (MITM), impersonation, node capture, and other attacks [8], [9], [10]. In the events of such attacks, misinformation can be transmitted to the vehicles, resulting in traffic paralysis and car accidents. Thus, to ensure secure communications against such attacks, a mutual authentication protocol between UAVs and RSUs must be designed. However, the characteristics of the environment should be carefully considered when designing a suitable protocol. The primary concerns in this regard can be summarized as follows:

- UAVs are mobile, and these devices frequently authenticate with different RSUs. UAVs have limited computing powers [11], [12]. Hence, if extensive computations are required by UAVs during the authentication phase, the UAVs become overloaded, and providing real-time ITS services may be difficult.
- RSUs use the data stored in their database to authenticate a UAV. However, if the data stored in an RSU are modified without permission [13], [14], an adversary can impersonate a UAV and can attempt to authenticate with the RSU to transmit incorrect traffic information to vehicles driving in the area.
- UAVs generally present security vulnerabilities against physical capture attacks. In this regard, if an adversary hijacks a UAV and performs a side-channel attack, the stored values of the UAV can be acquired. Several previous studies have claimed that although an adversary can authenticate and communicate with other entities using the hijacked UAV, it does not affect the entire network communication [15], [16]. However, the potential threat to the network resulting from compromised UAVs cannot be ignored.

To resolve the above issues, we consider using a physically unclonable function (PUF) [17] and the blockchain [18]. A PUF can generate unique and non-replicable secrets based on device manufacturing variations and is resistant to physical capture attacks. Generally, PUF challenge/response values are stored on a centralized server. It means that there is a risk of database attack, and the stored PUF values can be changed without permission. It can be resolved by storing PUF values on the blockchain. The blockchain is a shared database with immutable characteristics that can help RSUs authenticate UAVs. We propose a lightweight and secure authentication scheme between UAVs and RSUs using these two technologies. The key contributions of this study can be summarized as follows:

- A lightweight and secure authentication protocol is designed using the blockchain and a PUF for UAV-based ITSs. The proposed scheme is deemed resistant to physical capture attacks because the PUF is incorporated in the UAV. Furthermore, the hashed pseudo-identity of the UAV is stored through the blockchain, and RSUs can authenticate the UAV by retrieving the corresponding transaction. The proposed scheme does not require public key computations in UAVs.
- We propose a UAV revocation phase because UAVs are physically susceptible to be captured and damaged. When a UAV is revoked, the UAV is no longer considered valid for RSUs, and it cannot successfully authenticate with the RSUs.
- The security of the proposed scheme is analyzed using informal and formal analyses such as the real-or-random (RoR) model [19], Burrows–Abadi–Nikoogadam (BAN) logic [20], and automated validation of internet security protocols and applications (AVISPA) [21] simulation tool. Further, the computation and communication costs and security features are compared with those of existing schemes, and the obtained results reveal that the proposed scheme is superior to other schemes.

A. PAPER STRUCTURE

In Section II, recent studies that support the background of the current study are discussed. In Section III, the preliminaries used in the proposed scheme are introduced. In Sections IV and V, the proposed model and scheme are described. In Section VI, the analysis of the proposed scheme using formal and informal methods and a comparison of the proposed scheme with existing schemes are presented. Finally, Section VII provides the conclusions.

II. RELATED RESEARCH

The concept of UAV-enabled ITSs have recently emerged. In 2017, Menouar et al. [22] first presented a UAV-enabled ITS for smart cities. The authors considered the construction of an efficient and secure transportation system to be important in smart cities, and they proposed the use of drones in ITSs to provide services more efficiently. They focused on the deployment of drones for realizing an efficient transportation system. After that, researches on UAV deployment and scheduling have been actively researched in UAV-enabled ITS. Zeng et al. [23] proposed a UAV-enabled multicasting system for minimizing connection time and increasing efficiency of utilizing UAVs. Ghazzai et al. [24] proposed a scheduling frame work for UAV-based ITS. They focused on leveraging the UAV fleet efficiently because UAVs have limited battery capacity and should be recharge frequently. Outay et al. [25] presented recent advances and challenges in

TABLE 1. Summary of the related schemes in UAV-enavled ITS environments.

Scheme	Main Contributions	Limitations
Raza *et al.* [26]	designed an UAV-assisted VANET communication architecture, proposed a flexible and cost effective depolyment of UAVs for ITS environments	security issues were not considered, do not support mutual authentication protocol
Gope *et al.* [27]	proposed a privacy-preserving authentication scheme for IoD environments	have a centralization problem because of using a single USP
Zhang *et al.* [28]	proposed an authentication protocol between drones and vehicles, conduct formal security analysis	generate high computational costs because of using ECC cryptosystem
Khan *et al.* [29]	proposed a privacy-preserving authentication scheme for UAV-enabled ITS, conduct formal security analysis	generate high computational costs because of using ECC cryptosystem
Cheng *et al.* [30]	proposed a dynamic membership authentication between UAVs and RSUs	generate high communication and computational costs because TA participates in the authentication phase and using ECC cryptosystem
M. El-Zawawy *et al.* [31]	proposed a drone-assisted V2V communication scheme, conduct formal security analysis	generate high computational costs because of using ECC cryptosystem

applications of UAV in ITS. They discussed countermeasures and their implications for overcoming the challenges associated with the widespread deployment of UAVs in vehicular networks. As the concept of UAV-enabled ITS has been materialized and is about to be realized, researches on secure authentication protocols in UAV-enabled ITS environments have been proposed.

In 2019, Raza et al. [26] proposed a UAV-assisted vehicular ad hoc network (VANET) communication architecture for smart cities. They pointed out that VANETs typically suffer from network scalability, persistent connectivity, and routing overheads. They suggested the use of UAVs to improve the communication in VANETs to provide efficient and timely services. However, they did not present a specific communication protocol necessary for UAV-assisted VANETs.

Gope et al. [27] proposed a privacy-preserving authenticated key agreement scheme for internet-of-drone environments. The authors were chiefly concerned with the privacy issues of UAVs, including the location, identity, and session key. Their scheme used two PUFs during authentication to enhance security and update it in each session. However, in their scheme, a single USP performed authentications for all drones and could suffer from centralization.

Zhang et al. [28] proposed a key agreement protocol between drones and VANETs. They considered that drones could be deployed in rural and mountainous areas to address the communication problems of VANETs. They primarily handled the authentication between drones and vehicles. The authors of [28] proposed a mutual authentication scheme in a UAV-enabled ITS. However, their scheme used a public key cryptosystem such as an elliptic curve cryptosystem (ECC), which incurred high computational costs for drones and could not handle the authentication between a drone and an RSU.

Khan et al. [29] presented a privacy-preserving authentication scheme for a UAV-enabled ITS. They asserted that heterogeneous data sharing between UAVs and VANETs can cause security issues, and they deployed a backbone UAV to resolve these issues. In their scheme, a backbone UAV and a member UAV authenticated each other using an ECC, which, however, incurred a high computational cost.

Cheng et al. [30] proposed a dynamic membership authentication method. However, in their scheme, RSUs and UAVs authenticated each other through a trust authority (TA), and they suffered from a centralization issue. Furthermore, UAVs transmitted authentication request messages to the TA encrypted with a public-key cryptosystem, which is typically unsuitable for resource-limited UAVs.

M. El-Zawawy et al. [31] proposed a drone-assisted V2V communication considering various active attacks, and formally analyze their scheme using BAN logic and AVISPA simulation tool. Their scheme is efficient compared to the previous schemes. However, their scheme suffers from high computational costs because of using ECC cryptosystem.

Based on the above literature review of UAV-enabled ITSs, we noted that only limited studies have been conducted to solve the associated issues, including high computational loads, centralized data storage, risk of database forgery, and drone physical capture attacks. To remedy this, in this paper, a blockchain and PUF-based authentication scheme is proposed for UAV-enabled ITSs.

III. PRELIMINARIES

In this section, several preliminaries of the proposed scheme are introduced, and our justifications for adopting these techniques are described.

A. PHYSICALLY UNCLONABLE FUNCTION (PUF)

The concept underlying the use of a PUF is based on the following: Even if multiple integrated circuits (ICs) undergo the same manufacturing process, the produced ICs may be different owing to manufacturing variabilities [17]. Accordingly, each IC is unique, and one cannot generate two identical PUFs even if the complete design is known. Generally, PUFs can leverage this uniqueness to derive confidential

information. For example, when a user inputs a challenge c into a PUF, it outputs a response r corresponding to c. If different challenges are entered into the PUF, it always yields different responses. However, even when equivalent challenges are entered, the PUF can produce different responses in a noisy environment; thus, PUFs must be used in an ideal or noise-resistant environment. Fortunately, Pandey et al. addressed this issue using SRAM [32]. In this study, the PUF technology was utilized to provide resistance against UAV physical capture attacks. Each UAV transmits PUF values when registering on the network. The UAV can then authenticate with a RSU using the PUF values.

B. ADVERSARY MODEL

Further, the security of the proposed scheme under the Dolev–Yao (DY) [33] and the Canetti–Krawczyk (CK) models [34] was analyzed. Since its introduction in 1983, the DY model has been used extensively to analyze authentication schemes [8], [35], [36]. The basic assumptions of an adversary in the DY model are as follows:

- A has complete control of the messages transmitted via public channels. A can eavesdrop these messages and even modify or delete these messages.
- A can physically select a UAV, following which A can extract the stored values of the UAV using a power analysis attack [37], [38], [39].
- A can attempt various attacks using the values obtained from the previous two assumptions. These include impersonation, MITM, replay, and session key disclosure attacks.

Recently, attack techniques have become increasingly clever and sneaky, thus necessitating improvements in the assumptions of adversaries. Accordingly, the CK model, which has additional capabilities, is proposed based on the DY model.

- A can obtain long-term or short-term keys of the network and attempt to obtain the session key. Here, the long-term keys include the secret keys of entities participating in the network, and the short-term keys include the session random numbers generated during the authentication process [9], [36], [40].

In the informal analysis section, an analysis of the proposed scheme using the two aforementioned adversary models will be presented.

C. BLOCKCHAIN

The blockchain technology was firstly conceptualized to realize decentralized currencies. Particularly, early blockchains such as Bitcoin and Ethereum are completely decentralized, and every node can participate in the consensus. One of the most representative characteristics of the blockchain is its immutability. Based on this, when a transaction is uploaded after consensus, it is virtually impossible to modify the content of this transaction. This can be advantageous for the applications of the blockchain technology to other industries. However, as stated, early blockchains are entirely decentralized, and every node can participate in the consensus, such as PoW or PoS. This inevitably causes delays in the transaction-upload process. To address this issue, the concept of a consortium blockchain, namely a hyperledger, has been proposed [41]. In the consortium blockchain, authorized nodes participate in the consensus process; moreover, the integrity and immutability of the blockchain technology can be exploited, and delays caused during the consensus process can be minimized. In particular, the consortium blockchain can provide advantages in data sharing owing to its data integrity and transparency. In the proposed scheme, the blockchain is adopted to store the information required for authentication, such as PUF challenges/responses and pseudo identities of UAVs.

IV. SYSTEM MODEL

The system model of the proposed scheme is depicted in Fig. 1. The proposed model consists of the following five entities: a TA, RSU, UAV, and vehicle. A detailed description of each model is provided below.

- **Trusted authority**: The TA initializes a network and publishes public parameters. However, all the entities must be registered to the TA for further communications. After the TA registers a UAV, it uploads a transaction containing the hashed value of the pseudo identity information of the UAV to authenticate the UAV on the blockchain.
- **Roadside unit**: The RSU has adequate computing power to manage vehicles within its managing area. The RSU receives traffic information from UAVs and can provide ITS services to vehicles. Furthermore, RSUs are members of the blockchain, and these units are responsible for writing and maintaining ledgers. Typically, RSUs can authenticate UAVs using the information stored on the blockchain. After authentication, the RSU updates the pseudo identity of the UAV and uploads a new transaction regarding the updated identity of the UAV. Subsequently, the blockchain is updated after the practical Byzantine fault tolerance consensus algorithm between the RSUs, and other RSUs can authenticate the UAV through the transaction. RSUs are generally considered trustworthy during communication; however, an adversary can attempt to compromise the database or steal stored data.
- **Unmanned aerial vehicle**: UAVs equipped with PUFs aid the RSUs in providing ITS services to vehicles. Typically, after a UAV registers to a TA, the PUF challenges/responses and the hashed pseudo identity of the UAV are uploaded to the blockchain. As stated, UAVs can be deployed in congested areas or rural areas to monitor traffic conditions and transmit the information to a nearby RSU. Then, the RSU can process the received data and send the processed data to the UAV, and the UAV can provide ITS services to vehicles driving in the surrounding area.

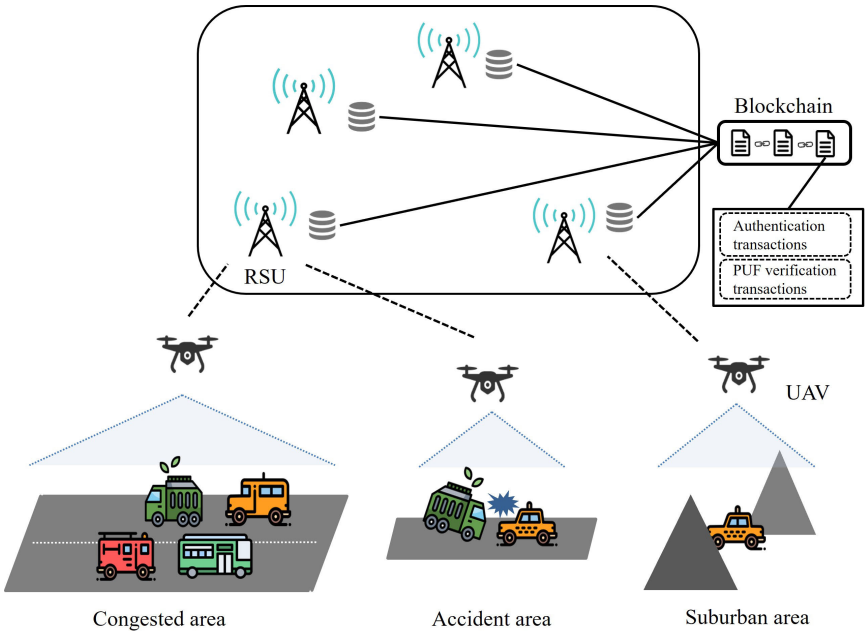

FIGURE 1. Proposed system model.

- **Vehicle**: Vehicles transmit road information to the RSU while driving and receive services for autonomous driving. In rural areas, vehicles can transmit traffic data to a deployed UAV to avail ITS services.

V. PROPOSED SCHEME

The proposed lightweight and secure authentication scheme for UAV-enabled ITSs is demonstrated using a blockchain-based PUF. The proposed scheme includes the initialization, registration, and authentication phases. In the initialization phase, the TA generates and publishes the necessary parameters for the network. In the registration phase, the TA registers the network entities, including RSUs and UAVs, and deploys secret parameters. Furthermore, the TA uploads the PUF challenges/responses and hashes the pseudo-identity of the UAV on the blockchain. During the authentication phase, the RSU authenticates the UAV. Here, the UAV sends an authentication request to the RSU, following which the RSU tests the validity of the message through the transaction uploaded on the blockchain and PUF using a smart contract. If the message is deemed valid, the RSU regards the UAV as valid and generates a session key for further communication. The notations involved in the proposed scheme are listed in Table 1, and a detailed description of each phase is given below.

A. INITIALIZATION

The TA generates an identity ID_{TA} and a secret key of the network s_{TA}, and it sets an elliptic curve E_p with order q and a one-way hash function with a 256 bit output $h(.)$. The TA then selects a generator P of E_p and computes $k = h(ID_{TA}||s_{TA})$, which are then used for the shared key between the RSUs in the network. The TA publishes $(ID_{TA}, E_p, P, h(.))$ and stores (s_{TA}, k).

TABLE 2. Notations and their meanings.

Notation	Description
TA	Trusted authority
UAV_i	i-th UAV
RSU_j	j-th RSU
s_j	Secret key of RSU_j
k	Shared key between TA and RSU
RID_i	Pseudo identity of UAV_i
PID_i	Secret pseudo identity of UAV_i
L_{i1}, L_j, L_{i2}	Message hash value
A_i, A_j, B_i	Masked value required for authentication
$Sig_{s_j}(.)$	Signature generated by s_j
(C_i, R_i)	PUF challenge/response of UAV_i
T_1	Timestamp
ID_i	Identity of UAV_i

B. REGISTRATION

1) RSU REGISTRATION

To register RSU_j, the TA chooses a unique identity ID_j and generates a random number s_j. Then, the TA transmits (ID_j, s_j, k) to RSU_j via a secure channel. Then, RSU_j computes the public key $P_j = s_j.P$ and stores (s_j, k) in a secure database.

2) UAV REGISTRATION

UAV_i generates an identity ID_i and a set of PUF challenges/responses $\{C_i^k, R_i^k\}$ $(k = 1, \ldots, n)$. Subsequently, UAV_i sends $(ID_i, \{C_i^k, R_i^k\})$ to the TA. The TA then tests whether ID_i has already been registered. If not, the TA generates random numbers n_i and r_i and computes $K_i = h(ID_i||s_{TA})$, $RID_i = h(ID_i||r_i)$, and $PID_i = h(RID_i||k)$. Subsequently, the TA uploads $(h(RID_i||PID_i||n_i||h(PID_i))||n_i||Sig_{TA}(h(RID_i||PID_i\ ||n_i)))$ to the blockchain and generates a smart contract containing PUF information related to K_i. The TA transmits (RID_i, n_i, PID_i, K_i) to UAV_i via a secure channel, and UAV_i stores (RID_i, PID_i, n_i, K_i) in memory.

UAV_i		RSU_j
Generates a timestamp T_1 Computes $A_i = K_i \oplus h(PID_i\|\|T_1)$, $L_{i1} = h(ID_j\|\|K_i\|\|n_i\|\|T_1)$		
	$\xrightarrow{\{RID_i, A_i, L_{i1}, T_1\}}$	
		Checks if $\|T_1 - T_1^*\| < \Delta T$? Computes $PID_i = h(RID_i\|\|k)$ Retrieves $h(RID_i\|\|PID_i\|\|n_i\|\|h(PID_i\|\|n_i\|\|$ $Sig_{TA}(h(RID_i\|\|PID_i\|\|n_i))))$ from the blockchain Computes $K_i = A_i \oplus h(PID_i\|\|T_1)$ Checks $L_{i1} \stackrel{?}{=} h(ID_j\|\|K_i\|\|n_i\|\|T_1)$ Retrieves C_i^k using K_i and chooses one Generates r_i^{new}, n_i^{new} and T_2 Computes $RID_i^{new} = h(RID_i\|\|r_i^{new})$, $PID_i^{new} = h(PID_i\|\|k)$, $A_j = RID_i^{new}\|\|PID_i^{new} \oplus h(ID_j\|\|RID_i\|\|$ $PID_i\|\|T_2)$, $B_j = n_i^{new}\|\|C_i \oplus h(T_2\|\|RID_i^{new}\|\|PID_i^{new})$, $L_j = h(RID_i^{new}\|\|PID_i^{new}\|\|C_i\|\|T_2)$
	$\xleftarrow{\{A_j, B_j, L_j, T_2\}}$	
Checks if $\|T_2 - T_2^*\| < \Delta T$? Computes $RID_i^{new}\|\|PID_i^{new}$ $= A_j \oplus h(ID_j\|\|RID_i\|\|PID_i\|\|T_2)$, $n_i\|\|C_i = B_j \oplus h(T_2\|\|RID_i^{new}\|\|PID_i^{new})$, Checks $L_j \stackrel{?}{=} h(RID_i^{new}\|\|PID_i^{new}\|\|C_i\|\|T_2)$ Updates (RID_i, n_i, PID_i) to $(RID_i^{new}, n_i^{new}, PID_i^{new})$ Generates a timestamp T_3 and R_i using C_i Computes $B_i = R_i \oplus h(PID_i\|\|PID_i^{new}\|\|n_i\|\|n_i^{new}\|\|T_2)$, $L_{i2} = h(C_i\|\|R_i\|\|T_3)$, $SK_{ij} = h(R_i\|\|PID_i\|\|PID_i^{new}\|\|n_i\|\|n_i^{new}\|\|T_3)$		
	$\xrightarrow{\{B_i, L_{i2}, T_3\}}$	
		Checks if $\|T_3 - T_3^*\| < \Delta T$? Computes $R_i = B_i \oplus h(PID_i\|\|PID_i^{new}\|\|n_i\|\|n_i^{new}\|\|T_2)$ Checks $L_{i2} \stackrel{?}{=} h(C_i\|\|R_i\|\|T_3)$ Checks validity of $h(R_i)$ from C_i $SK_{ij} = h(R_i\|\|PID_i\|\|PID_i^{new}\|\|n_i\|\|n_i^{new}\|\|T_3)$ Deletes R_i Uploads $h(RID_i^{new}\|\|PID_i^{new}\|\|n_i^{new}\|\|h(PID_i^{new}\|\|$ $n_i^{new}\|\|Sig_{s_j}(h(RID_i^{new}\|\|PID_i^{new}\|\|n_i^{new}))))$ to the blockchain

FIGURE 2. Proposed authentication phase between UAV_i and RSU_j.

C. AUTHENTICATION

Notably, when UAV_i is deployed in a specific area, it should first authenticate with a nearby RSU_j. Here, UAV_i generates timestamp T_1 and computes $A_i = K_i \oplus h(PID_i||T_1)$ and $L_{i1} = h(ID_j||K_i||n_i||T_1)$, and RSU_j verifies the validity of T_1, computes $PID_i = h(RID_i||k)$, and retrieves $(h(RID_i||PID_i||n_i||h(PID_i))||n_i||Sig_{TA}(h(RID_i||PID_i||n_i)))$ from the blockchain. Subsequently, RSU_j computes $K_i = A_i \oplus h(PID_i||T_1)$ and checks $L_{i1} \stackrel{?}{=} h(ID_j||K_i||n_i||T_1)$. Then, RSU_j retrieves the smart contract using K_i, selects C_i, and generates r_i^{new}, n_i^{new}, and T_2. Next, RSU_j computes $RID_i^{new} = h(RID_i||r_i^{new})$, $PID_i^{new} = h(RID_i^{new}||k)$, $A_j = (RID_i^{new}||PID_i^{new}) \oplus h(ID_j||RID_i||PID_i||T_2)$, $B_j = (n_i^{new}||C_i) \oplus h(T_2||RID_i^{new}||PID_i^{new})$, and $L_j = h(RID_i^{new}||PID_i^{new}||C_i||n_i^{new}||T_2)$. RSU_j transmits (A_j, B_j, L_j, T_2) to UAV_i via a public channel. UAV_i receives the message and computes $(RID_i^{new}||PID_i^{new}) = A_j \oplus h(ID_j||RID_i||PID_i||T_2)$, $(n_i^{new}||C_i) = B_j \oplus h(T_2||RID_i^{new}||PID_i^{new})$, and $L_j' = h(RID_i^{new}||PID_i^{new}||C_i||n_i^{new}||T_2)$. Subsequently, UAV_i checks whether $L_j' \stackrel{?}{=} L_j$, and if it is equal, UAV_i updates (RID_i, n_i, PID_i) to $(RID_i^{new}, n_i^{new}, PID_i^{new})$ in memory. UAV_i generates a timestamp T_3 and a PUF response R_i from C_i, and it computes $B_i = R_i \oplus h(PID_i||PID_i^{new}||n_i||n_i^{new}||T_2)$, $SK_{ij} = h(R_i||PID_i||PID_i^{new}||n_i||n_i^{new}||T_3)$, and $L_{i2} = h(C_i||SK_{ij}||T_3)$. Following this, UAV_i sends (B_i, L_{i2}, T_3) to RSU_j. After receiving the message, RSU_j tests the validity of T_3, computes $R_i = B_i \oplus h(PID_i||PID_i^{new}||n_i||n_i^{new}||T_2)$, and checks the validity of C_i and R_i using the smart contract

uploaded on the blockchain. The verification algorithm for the PUF values is presented in Algorithm 1. If it is valid, RSU_j computes $SK_{ij} = h(R_i||PID_i||PID_i^{new}||n_i||n_i^{new}||T_3)$ and checks whether $L_{i2} \stackrel{?}{=} h(C_i||SK_{ij}||T_3)$. Subsequently, RSU_j successfully authenticates UAV_i. RSU_j deletes R_i and uploads $(h(RID_i^{new}||PID_i^{new}||n_i^{new}||h(PID_i^{new}))||n_i^{new}||Sig_{TA}(h(RID_i^{new}||PID_i^{new}||n_i^{new})))$ to the blockchain. Fig. 2 presents the proposed authentication phase.

D. UAV REVOCATION

If a UAV is identified to behave maliciously, it cannot communicate with other entities in the network. When such misbehavior of UAV_i is detected, RSU_j uploads a transaction to revoke $h(PID_i)$ and render the smart contract on K_i invalid. Subsequently, other RSUs consider the pseudo-identity of the UAV_i to be invalid, and UAV_i cannot authenticate with the RSUs in the network.

VI. SECURITY ANALYSIS

The proposed scheme was further analyzed by using both informal and formal methods. In particular, the proposed scheme was demonstrated to be secure against various attacks based on an informal analysis, and the correctness of the scheme was verified using the "Burrows–Abadi–Needham logic (also known as the BAN logic)" analysis [20].

A. INFORMAL ANALYSIS

The proposed protocol was demonstrated to be secure against a variety of attacks.

1) REPLAY AND MITM ATTACKS

Based on the assumptions described in Section III-C, an attacker A acquires messages transmitted through a public channel. Following this, A can use the messages to attempt replay and MITM attacks. However, each message contains a timestamp T_1, T_2, and T_3, and the network entities test the validity of the timestamp when they receive a message. Therefore, the proposed scheme is resistant to replays and MITM attacks.

2) UAV PHYSICAL CAPTURE AND IMPERSONATION ATTACKS

When A physically selects UAV_i, it can extract the stored values (PID_i, RID_i, n_i, K_i) of UAV_i using a power analysis attack. Following this, A can transmit an authentication request message to RSU_j and receive a response message containing the PUF challenge C_i. However, A cannot generate a corresponding response R_i because the PUF is resistant to power analysis attacks. Therefore, the proposed scheme is secure against UAV physical capture and impersonation attacks.

3) SESSION KEY DISCLOSURE ATTACK

A can determine the session key using the messages transmitted through a public channel and the obtained values. Because the hash function is collision resistant, A must guess PID_i, PID_i^{new}, n_i, n_i^{new}, and R_i to determine SK_{ij}. Here, the bits of each value are 256, and the total number of bits is 1024. However, correctly guessing 1024 bits is probabilistically impossible. Therefore, the proposed scheme is resistant to session-key disclosure attacks.

Algorithm 1 PUF Response Verification

Input: (K_i, C_i, R_i')
Output: True or false;

```
Compute h(R_i') using R_i'
Retrieve R_i using C_i
if there is not C_i in memory then
    return False;
else
    if h(R_i') ?= h(R_i) then
        return True;
    end if
end if
```

4) DISTRIBUTED DENIAL-OF-SERVICE (DDoS) ATTACK

A can generate numerous authentication request messages and transmit them to RSU_j to paralyze a network. However, RID_i is updated in each session, and A cannot determine RID_i^{new} before UAV_i generates a new authentication-request message. Furthermore, even if A obtains RID_i^{new}, A cannot acquire PID_i^{new}, and generating a message hash value L_{i1} is impossible. Therefore, the message generated by A must be rejected, and the proposed scheme is resistant to DDoS attacks.

5) PERFECT FORWARD SECRECY

The long-term keys of the proposed scheme may constitute s_{TA}, s_j, k, and the transactions and smart contracts uploaded to the blockchain. However, A cannot determine SK_{ij} solely using the long-term keys without R_i. R_i should be obtained using a PUF device equipped with UAV_i because RSU_j deletes R_i in each session. Therefore, the proposed scheme guarantees perfect forward secrecy.

6) KNOWN SESSION-SPECIFIC TEMPORARY INFORMATION (KSSTI) ATTACK

If A obtains the random numbers including n_i and r_i generated during a session, A can determine $RID_i^{new} = h(RID_i||r_i^{new})$. However, A cannot calculate any other values, such as PID_i and R_i, that are necessary to obtain SK_{ij}. Consequently, the proposed scheme is secure against KSSTI attacks.

7) ANONYMITY AND UNTRACEABILITY

UAV_i authenticates RSU_j using pseudo identity RID_i. Therefore, the anonymity of UAV_i is guaranteed. Furthermore, RID_i is changed in each session. Thus, A cannot determine the relevance of the messages sent by the same UAV_i from different sessions, and A cannot trace UAV_i using messages received

TABLE 3. BAN logic notations.

Notation	Description
p_1, p_2	Two principals
s_1, s_2	Two statements
SK	The session key
$p_1 \mid \equiv s_1$	p_1 believes s_1
$p_1 \mid \sim s_1$	p_1 once said s_1
$p_1 \Rightarrow s_1$	p_1 controls s_1
$p_1 \lhd s_1$	p_1 receives s_1
$\#s_1$	s_1 is fresh
$\{s_1\}_K$	s_1 is encrypted with K
$p_1 \overset{K}{\longleftrightarrow} p_2$	p_1 and p_2 have shared key K

from a public channel. Therefore, the proposed scheme provides anonymity and untraceabiity.

8) STOLEN VERIFIER ATTACK

A can block the verification table of the proposed scheme and attempt various attacks, such as impersonation and session key disclosure attacks. However, in the authentication phase, A cannot be disguised as UAV_i because A cannot generate a legitimate PUF response R_i. Furthermore, A cannot impersonate RSU_j without knowing k and s_j. Similarly, A cannot obtain SK_{ij}; therefore, the proposed scheme is secure against a stolen verifier attack.

9) DECENTRALIZATION

Even if a database of RSU_j is compromised and part of the stored data is modified or deleted, it can be easily restored because the proposed scheme adopts the blockchain technology. Therefore, it can be asserted that the proposed model can provide decentralized storage and is more secure than the traditional centralized storage models.

B. BAN LOGIC ANALYSIS

In this section, the BAN logic of the proposed protocol is described. In particular, the BAN logic is a formal analysis method that can be used to verify the correctness of an authentication protocol. Table 3 lists the relevant notations and their corresponding meanings, and given below are the basic rules used for the BAN logic analysis.

1. Message meaning rule (MMR):

$$\frac{p_1 \mid \equiv p_1 \overset{K}{\leftrightarrow} p_2, \quad p_1 \lhd (s_1)_K}{p_1 \mid \equiv p_2 \mid \sim s_1}$$

2. Nonce verification rule (NVR):

$$\frac{p_1 \mid \equiv \#(s_1), \quad p_1 \mid \equiv p_2 \mid \sim s_1}{p_1 \mid \equiv p_2 \mid \equiv s_1}$$

3. Jurisdiction rule (JR):

$$\frac{p_1 \mid \equiv p_2 \mid \Longrightarrow s_1, \quad p_1 \mid \equiv p_2 \mid \equiv s_1}{p_1 \mid \equiv s_1}$$

4. Belief rule (BR):

$$\frac{p_1 \mid \equiv (s_1, s_2)}{p_1 \mid \equiv s_1}$$

5. Freshness rule (FR):

$$\frac{p_1 \mid \equiv \#(s_1)}{p_1 \mid \equiv \#(s_1, s_2)}$$

1) GOALS

The objectives for proving the correctness of the proposed protocol are defined as follows:

Goal 1: $UAV_i \mid \equiv UAV_i \overset{SK}{\longleftrightarrow} RSU_j$

Goal 2: $UAV_i \mid \equiv RSU_j \mid \equiv UAV_i \overset{SK}{\longleftrightarrow} RSU_j$

Goal 3: $RSU_j \mid \equiv UAV_i \overset{SK}{\longleftrightarrow} RSU_j$

Goal 4: $RSU_j \mid \equiv UAV_i \mid \equiv UAV_i \overset{SK}{\longleftrightarrow} RSU_j$

2) ASSUMPTIONS

The BAN logic assumptions of the proposed protocol are as follows.

A_1: $UAV_i \mid \equiv \#(T_2)$

A_2: $RSU_j \mid \equiv \#(T_1, T_3)$

A_3: $UAV_i \mid \equiv RSU_j \Rightarrow (UAV_i \overset{SK}{\longleftrightarrow} RSU_j)$

A_4: $RSU_j \mid \equiv UAV_i \Rightarrow (UAV_i \overset{SK}{\longleftrightarrow} RSU_j)$

A_5: $UAV_i \mid \equiv UAV_i \overset{(PID_i)}{\longleftrightarrow} RSU_j$

A_6: $RSU_j \mid \equiv UAV_i \overset{(PID_i)}{\longleftrightarrow} RSU_j$

3) IDEALIZATIONS

The messages transmitted during the proposed authentication phase and the idealized form of each message are as follows:

- Message 1: UAV_i sends $\{ID_j, RID_i, A_i, L_{i1}, T_1\}$ to RSU_j, and the idealized form of the message is
  Msg_1: $UAV_i \rightarrow RSU_j : \{n_i, T_1\}_{PID_i}$
- Message 2: RSU_j sends $\{A_j, B_j, L_j, T_2\}$ to UAV_i, and the idealized form of the message is

Msg_2 :
$RSU_j \rightarrow UAV_i : \{PID_i^{new}, n_i^{new}, C_i, T_2\}_{PID_i}$

- Message 3: UAV_i sends $\{B_i, L_{i2}, T_3\}$to RSU_j, and the idealized form of the message is

Msg_3 : $UAV_i \rightarrow RSU_j : \{R_i, T_3\}_{PID_i}$

4) BAN LOGIC ANALYSIS

Based on the assumptions and idealized forms, a BAN logic analysis is performed as follows:

Step 1: RSU_j receives Msg_1.
S_1: $RSU_j \lhd \{n_i, T_1\}_{PID_i}$

Step 2: S_2 can be derived by applying A_6 to the MMR.
S_2: $RSU_j \mid \equiv UAV_i \mid \sim \{n_i, T_1\}$

Step 3: S_3 can be derived by applying A_2 to the FR.
S_3: $RSU_j \mid \equiv \#\{n_i, T_1\}$

Step 4: S_4 can be derived by applying S_2 and S_3 to the NVR.

S_4: $RSU_j| \equiv UAV_i| \equiv (n_i, T_1)$

Step 5: S_5 can be derived by applying S_4 to the BR.
S_5: $RSU_j| \equiv UAV_i| \equiv (n_i)$

Step 6: UAV_i receives Msg_2.
S_6: $UAV_i \lhd \{PID_i^{new}, n_i^{new}, C_i, T_2\}_{PID_i}$

Step 7: S_7 can be derived by applying S_6 to the MMR.
S_7: $UAV_i| \equiv RSU_j| \sim \{PID_i^{new}, n_i^{new}, C_i, T_2\}$

Step 8: S_8 can be derived by applying S_7 to the FR.
S_8: $UAV_i| \equiv \#\{PID_i^{new}, n_i^{new}, C_i, T_2\}$

Step 9: S_9 can be derived by applying S_7 and S_8 to the NVR.
S_9: $UAV_i| \equiv RSU_j| \equiv \{PID_i^{new}, n_i^{new}, C_i, T_2\}$

Step 10: S_{10} can be derived by applying BR using S_{11}.
S_{10} : $UAV_i| \equiv RSU_j| \equiv \{PID_i^{new}, n_i^{new}, C_i\}$

Step 11: UAV_i can believe that RSU_j and can obtain the session key $SK = h(R_i||PID_i||PID_i^{new}||n_i||n_i^{new}||T_3)$ as UAV_i sends R_i and T_3 to RSU_j.
S_{11} : $UAV_i| \equiv RSU_i| \equiv (UAV_i \overset{SK}{\longleftrightarrow} RSU_j)$**(Goal 2)**

Step 12: S_{12} can be derived by applying S_{11} to the JR.
S_{12} : $UAV_i| \equiv (UAV_i \overset{SK}{\longleftrightarrow} RSU_j)$ **(Goal 1)**

Step 13: RSU_j receives Msg_3. As in Steps 1-5, S_{13} can be derived.
S_{13} : $RSU_j| \equiv UAV_i| \equiv (R_i, T_3)$

Step 14: RSU_j can believe that UAV_i obtains the session key $SK = h(R_i||PID_i||PID_i^{new}||n_i||n_i^{new}||T_3)$.
S_{14} : $RSU_j| \equiv UAV_i| \equiv (UAV_i \overset{SK}{\longleftrightarrow} RSU_j)$**(Goal 4)**

Step 15: S_{15} can be derived by applying S_{14} to the JR.
S_{15} : $RSU_j| \equiv (UAV_i \overset{SK}{\longleftrightarrow} RSU_j)$ **(Goal 3)**

C. REAL-OR-RANDOM (RoR) MODEL

The RoR model [19] is a formal analysis method adopted to prove the session-key security of an authentication protocol. In this process, even if A performs various queries (i.e., attacks), the probability of obtaining a session key is less than ϵ. Table 4 lists the queries executed in the RoR model.

Theorem 1: Let q_H denote the number of *Hash* queries performed by A, $|Hash|$ denote the range space of the hash function, and Adv_A denote the probability of A distinguishing the session key and a random number. Based on the foregoing, the following inequality holds:

$$Adv_A \leq \frac{q_H^2}{|Hash|} + \frac{q_s}{|PUF|}. \tag{1}$$

Proof: If Adv_A is sufficiently large, it implies that A can distinguish between the session key and a random number to some extent. We presented that Adv_A is negligible by proving the validity of Equation (1). We assumed that A can conduct four games, G_i $(i = 1, 2, 3, 4)$, and in each game, A executes queries, and at the end of each game, A executes the *Test* query. Following this, $Adv_A^{G_i}$ for the game is determined.

G_1 : First, $Adv_A^{G_1}$ is defined when A has no information regarding the session key and does not execute any query.

TABLE 4. Queries performed in the ROR model.

Query	Description
$Execute$	It represents an eavesdropping attack performed by A. A can obtain the messages transmitted between honest participants via open channels.
$Hash$	It represents that A can use the hash function employed in the system.
$Corrupt$	It indicates that secure values stored in UAV_i are extracted by A using a power analysis attack.
$Send$	It implies that A sends a message to a participant in the network. Further, A can receive responses to the sent messages. For example, if A can generate a legitimate authentication request message for UAV_i, A can receive a response from RSU_j based on the message.
$Test$	It is used to verify the semantic security of a session key. Let us consider an unbiased coin c, for which the head represents one, and the tail represents 0. When A performs a $Test$ query, c is flipped, and it returns the session key when $c = 1$ and a random number when $c = 0$. Otherwise, c returns $NULL$. At this moment, A must guess whether the return value is the session key, without knowing the outcome of the coin toss.

This can be related to the definition of semantic security.

$$Adv_A = |2Adv_A^{G_1} - 1|, \tag{2}$$

G_2 : A can execute the *Execute* query during this attack. A can obtain messages including $(RID_i, A_i, L_{i1}, T_1)$, (A_j, B_j, C_j, T_2), and (B_i, L_{i2}, T_3) transmitted via a public channel. The session key is determined by $SK_{ij} = h(PID_i||PID_i^{new}||n_i||n_i^{new}||T_3)$, which is masked by a hash function; therefore, A has no advantage over G_1.

$$Adv_A^{G_1} = Adv_A^{G_2} \tag{3}$$

G_3 : A can attempt a *Hash* query to obtain the session key. However, A cannot access any information regarding the session key using the messages obtained from G_2. Therefore, Adv_{G_3} is equivalent to finding a collision in the hash function, which can be estimated using the birthday paradox [42].

$$|Adv_A^{G_3} - Adv_A^{G_2}| \leq \frac{q_H^2}{|Hash|}. \tag{4}$$

G_4 : In this game, A can perform *Send* and *Corrupt* queries to correctly guess the session key. Subsequently, A can extract the values stored in UAV_i. Then, A can obtain PID_i, PID_i^{new}, n_i, and n_i^{new}. However, A must determine R_i to obtain the session key. Here, A must guess R_i and receive a message from RSU_j. Let q_s be the number of *Send* queries executed by A, and let $|PUF|$ be the size of the PUF response value. The advantage function can then be derived as follows:

$$|Adv_A^{G_4} - Adv_A^{G_3}| \leq \frac{q_s}{|PUF|}. \tag{5}$$

After all the games are performed, A must correctly guess c.

$$Adv_A^{G_4} = \frac{1}{2} \tag{6}$$

```
role uav(UAV,TA,RSU:agent,SKuta,SKrta,SKur: symmetric_key, H,PUF,MUL: hash_func,
SND,RCV:channel(dy))
played_by UAV
def=
local State: nat,
T1,T2,T3,IDi,IDj,RIDi,PIDi,RIDin,PIDin,Pj,SK,PNi,Nin,Ki,Ri,Rin,Rii,Ci,K,Sj,Sta,Li,Lii,Lj:text,
Ai,Aj,Bj,Bi:text
const reg1,reg2,reg3,reg4,auth1,auth2,auth3,auth4,auth5,auth6:protocol_id
init State:=0
transition

1. State=0 /\ RCV(start)=|>
State':=2/\SND({IDi.Ci.Rii}_SKuta)
/\secret(Rii,reg3,UAV)
2. State=2/\ RCV({H(IDi.Ri').H(H(IDi.Ri').K).H(IDi.Sta).Nij}_SKuta)=|>
State':=4/\secret({H(IDi.Ri').H(H(IDi.Ri').K).H(IDi.Sta).Nij},reg4,{TA,UAV})

3. State=5/\RCV(start)=|>
State':=7/\T1':=new()
/\Ai':=xor(H(IDi.Sta),H(H(H(IDi.Ri).K).T1'))
/\Li':=H(IDj.H(IDi.Sta).Ni.T1')
/\SND(RIDi.Ai'.Li'.T1')
/\witness(UAV,RSU,auth1,K)

4. State=7/\RCV(xor(H(H(IDi.Ri').Rin').H(H(H(IDi.Ri').Rin').K),H(IDj.H(IDi.Ri').H(H(IDi.Ri').K).T2')).
xor(Nin'.Ci',H(T2'.H(H(IDi.Ri').Rin').H(H(H(IDi.Ri').Rin').K))).H(H(H(IDi.Ri').Rin').H(H(H(IDi.Ri').Rin').K
).Ci'.T2))=|>
State':=9/\Rii':=PUF(Ci)
/\T3':=new()
/\Bi':=xor(Ri',H(H(IDi.Ri').K).H(H(H(IDi.Ri').Rin').K).Ni.Nin'.T2)
/\Lii':=H(Ci.PUF(Ci).T3')
/\SK':=H(Ri'.H(H(IDi.Ri').K).H(H(H(IDi.Ri').Rin').K).Ni.Nin.T3')
/\SND(Bi'.Lii'.T3')
/\request(RSU,UAV,auth2,{Rin',Nin'})
/\witness(UAV,RSU,auth3,{Ri'})
end role
```

FIGURE 3. Role of *UAV*.

The following equation can be derived using Equations (2),(3), and (6):

$$\begin{aligned}\frac{1}{2}Adv_A &= |Adv_A^{G_2} - \frac{1}{2}| \\ &= |Adv_A^{G_4} - Adv_A^{G_2}| \end{aligned} \tag{7}$$

Finally, the following equation can be derived and proven.

$$\begin{aligned} Adv_A &= 2|Adv_A^{G_4} - Adv_A^{G_2}| \\ &\leq 2|Adv_A^{G_4} - Adv_A^{G_3}| + 2|Adv_A^{G_3} - Adv_A^{G_2}| \\ &\leq \frac{q_H^2}{|Hash|} + \frac{q_s}{|PUF|} \end{aligned} \tag{8}$$

As the advantage function of A is negligibly small, the session key of the proposed scheme satisfies semantic security.

D. AVISPA SIMULATION

The proposed scheme was simulated using AVISPA, which is widely accepted as a tool to verify the security of an authentication protocol [21]. In the AVISPA tool, an authentication protocol is implemented using a high-level protocol specification language (HLPSL) [43], and the results can be derived based on the following four models: ''on-the-fly model checker (OFMC) [44],'' ''tree automata based on automatic approximations for analysis of security protocols,C'' ''constraint logic-based attack searcher(CL-AtSe) [45],'' and ''SAT-based model checker (SATMC).'' Generally, the OFMC and CL-AtSe are used for simulations because these two models support exclusive OR operations. If the simulation result is ''SAFE,C'' we can state that the protocol is secure against replay attacks and MITM attacks. Fig. 3 shows the role of *UAV*. The code includes

```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/itsuav.if

GOAL
 As Specified

BACKEND
 CL-AtSe

STATISTICS
 Analysed  : 3 states
 Reachable  : 0 states
 Translation: 0.10 seconds
 Computation: 0.00 seconds
```

```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS

PROTOCOL
 /home/span/span/testsuite/results/itsuav.if

GOAL
 as_specified

BACKEND
 OFMC

COMMENTS

STATISTICS
 parseTime: 0.00s
 searchTime: 0.50s
 visitedNodes: 51 nodes
 depth: 6 plies
```

FIGURE 4. Simulation results.

communication messages sent and received by *UAV* during the UAV registration and authentication process. The simulation results are depicted in Fig. 4, and the proposed protocol is deemed safe. Therefore, it can be concluded that the proposed protocol is resistant against replay and MITM attacks.

VII. PERFORMANCE ANALYSIS

The proposed scheme was compared with existing schemes [27], [29], [30] in terms of the computational cost, communication cost, and security features to demonstrate the improved efficiency and security of the proposed scheme. The other related papers do not address authentication between an UAV and a RSU.

A. COMPUTATIONAL COSTS ANALYSIS

For this analysis, the time required for each operation was recorded using the MIRACL library [46]. Different computing powers of the UAVs and RSUs were considered and experimented with in separate environments. First, an experiment was performed on a desktop with an i7-4790 intel CPU and 16 GB RAM and a Linux Ubuntu 20.04-desktop-amd64 operating system to reflect the high computing power of the RSUs. In addition, the same experiment was performed on a Raspberry PI 3B with ARM Cortex-A53 and 1 GB RAM to reflect the low computing power of UAVs. The executed operations and results are summarized in Table 5. The PUF response generated by a fuzzy extractor was set for noise resilience, and the time cost was assumed to be the same as that for the ECC scalar multiplication operation.

Based on the results summarized in Table 5, the total computational cost of each scheme was recorded. In the scheme proposed by Gope et al. [27], the UAV conducted four fuzzy extractor operations and four hash operations, whereas the RSU conducted three hash operations. In the scheme proposed by Khan et al. [29], the UAV performed four ECC point multiplications, two ECC additions, and four hash operations, whereas the RSU conducted four ECC point multiplications, one ECC point addition, and four hash operations. In the

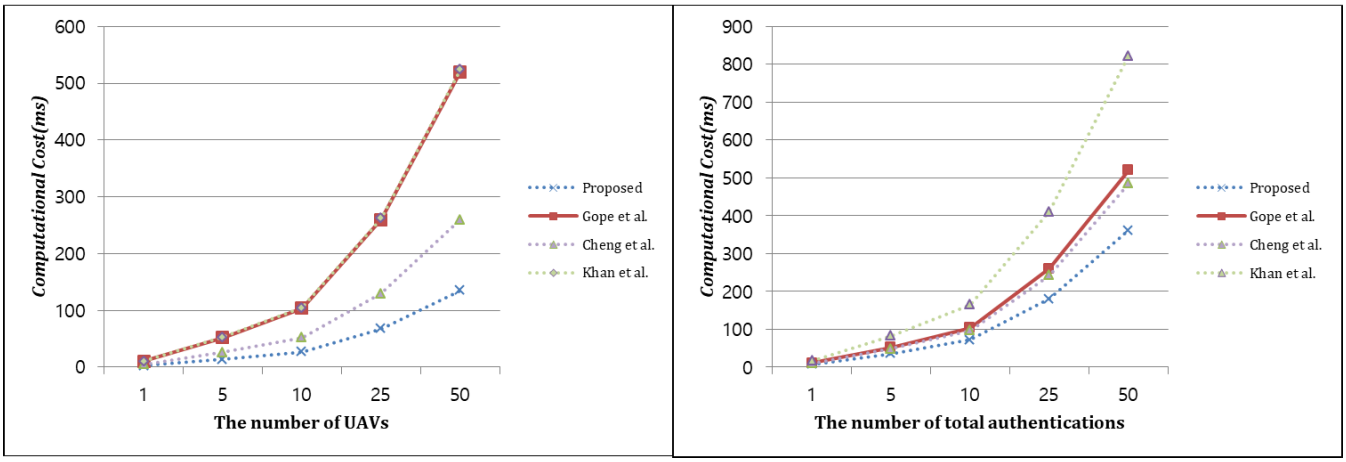

FIGURE 5. Computational cost with an increase in the number of UAVs and authentications.

TABLE 5. Time consumption for each operation.

Scheme	Total execution time	Desktop	Raspberry PI
T_{mul}	ECC scalar multiplication	1.489 ms	2.579 ms
T_{add}	ECC point addition	0.008 ms	0.019 ms
T_h	One-way hash	0.003 ms	0.021 ms
T_f	Fuzzy extractor	1.489 ms	2.579 ms

TABLE 6. Computational cost comparison.

Scheme	UAV	RSU
Gope *et al.* [27]	10.4 ms	0.012 ms
Khan *et al.* [29]	10.476 ms	5.976 ms
Cheng *et al.* [30]	5.198 ms	4.495 ms
Proposed	2.705 ms	4.516 ms

scheme proposed by Cheng et al. [30], the UAV performed two ECC multiplications, one ECC addition, and one hash operation, whereas the RSU conducted four ECC multiplications, two ECC additions, and four hash operations. In the proposed scheme, the UAV performed one fuzzy extractor operation and six hash operations, and the RSU conducted four ECC multiplications, two ECC additions, and 11 hash operations. Table 6 summarizes the total computational cost for each scheme.

As can be inferred, the proposed scheme incurs a higher computational cost than the scheme proposed by [27] on the RSU side owing to signature generation and verification for uploading transactions on the blockchain. However, the proposed scheme incurs a much lower computational cost than existing schemes on the UAV side. Fig. 5 illustrates the total computational cost with an increase in the number of UAVs and authentications. As indicated in Fig. 5, the proposed scheme is more efficient compared to the other schemes. Notably, in actual environments, the differences in computing power between RSUs and UAVs may be larger than those between a desktop and Raspberry PI; consequently, the results could be much improved. Comprehensively, it can be stated that the proposed scheme has better efficiency in terms of the computational cost compared to existing schemes.

B. COMMUNICATION COSTS ANALYSIS

Further, the communication costs incurred during the authentication phase were also compared. For this, we assumed that the ECC point, hash output, fuzzy challenge/response, identity, random nonce, and timestamp were 320, 256, 256, 128, 256, and 32 bits, respectively. In the scheme proposed in [27], the UAV sends (PID_u^i, N_u, ID_{mec}) to the USP, receives $(PID^*, N_s, C_i, Res_{Serv})$, and transmits $(R_{i+1}^{x*}, R_{i+1}^{y*}, Res_{Uav}, EL)$ to the USP. These messages contain five hash outputs, one PUF challenge, two PUF responses, two random numbers, and one identity, with a total cost of 2678 bits. In the scheme detailed in [29], the UAV transmits $(t_{muav}, r_{muav}, ID_{muav}, C_{muav}, H)$ to the RSU, which then sends $(t_{rsu}, r_{rsu}, ID_{rsu}, C_{rsu}, H')$ to the UAV. Each message has 1256 bits as it includes a timestamp, random nonce, identity, ECC point, and hash output. In the scheme detailed in [30], the UAV sends $(ID_U, ID_T, M_{UT}, AM_{UT})$ and receives $(ID_T, ID_U, V_U, S_{TU}, T_U)$. The first message includes three identities, three hash outputs, and a timestamp with a total cost of 1184 bits. The second message includes two identities: a random nonce, hash output, and timestamp, and the total cost is 800 bits. In the proposed scheme, the first message is $(RID_i, A_i, L_{i1}, T_1)$, and it includes three hash outputs and a timestamp, and the total cost is 800 bits. The second message is A_j, B_j, C_i, T_2, and it includes three hash outputs, a random nonce, PUF challenge, and timestamp, and the total cost is 1312 bits. The last message is B_i, L_{i2}, T_3, which includes two hash outputs and a timestamp, and the total cost is 544 bits. Table 7 summarizes the total communication cost of each scheme.

Although the proposed scheme incurs a higher communication cost compared to the other schemes, it incurs a much lower communication cost on the UAV side. Furthermore, the proposed protocol provides superior security compared to the other schemes, as indicated in Table 8.

TABLE 7. Communication cost comparison.

Scheme	Total communication cost
Gope *et al.* [27]	2678 bits
Khan *et al.* [29]	2512 bits
Cheng *et al.* [30]	1984 bits
Proposed	2656 bits

TABLE 8. Comparison of security features.

Security features	[27]	[29]	[30]	Proposed
Replay and MITM attacks	O	O	O	O
Session key disclosure attack	O	O	O	O
UAV physical capture attack	O	X	X	O
DDoS attack	O	O	O	O
Perfect forward secrecy	O	–	O	O
KSSTI attack	O	–	–	O
Anonymity and untraceability	O	X	X	O
Stolen verifier attack	X	O	O	O
Decentralized storage	X	X	X	O

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

C. SECURITY FEATURES ANALYSIS

Further, the security features of the proposed method were compared with those of the related protocols [27], [29], [30]. The following attacks were considered: a) ''resistance to replay and MITM attacks,'' b) ''resistance to a session key disclosure attack,'' c) ''resistance to an impersonation attack,'' d) ''resistance to a UAV physical capture attack,'' e) ''resistance to a DDoS attack,'' f) ''preservation of perfect forward secrecy,'' g) ''resistance to a KSSTI attack,'' h) ''preservation of anonymity and untraceability,'' i) ''resistance to a stolen verifier attack'', and j) ''support decentralization.'' The comparison results are summarized in Table 8. It is evident that the proposed scheme demonstrates superior security compared to the other related schemes in similar environments [27], [29], [30].

VIII. CONCLUSION AND FUTURE WORK

A secure and lightweight authentication scheme for UAV-enabled ITSs is proposed using the blockchain and a PUF. In the proposed scheme, the hash pseudo-identity and PUF challenge/response of the UAV are uploaded to the blockchain after registration, and an RSU can authenticate a drone by retrieving the blockchain. Furthermore, after authentication, the RSU updates the pseudo identity of the UAV and uploads a new transaction to the blockchain. Subsequently, other RSUs can recursively authenticate the UAV. The proposed scheme has resistance to various attacks such as trace and ephemeral key-leakage attacks, and provide perfect forward secrecy and decentralization. Further, the proposed scheme is formally analyzed using the BAN logic to prove the correctness of the scheme, AVISPA simulation tool to demonstrate that the proposed scheme has resistance to replay and MITM attacks, and RoR model to prove the session key security of the scheme. Finally, the performance of the proposed scheme is compared with that of related schemes in terms of the computational cost, communication cost, and security features. The results reveal that the proposed scheme demonstrates superior performance compared to the related schemes. In future studies, we aim to design a scheme by considering the computational efficiency of RSUs as well as UAVs.

REFERENCES

[1] G. Dimitrakopoulos and P. Demestichas, ''Intelligent transportation systems,'' *IEEE Veh. Technol. Mag.*, vol. 5, no. 1, pp. 77–84, Mar. 2010.

[2] Y. Yang and R. Bagrodia, ''Evaluation of VANET-based advanced intelligent transportation systems,'' in *Proc. 6th ACM Int. Workshop Veh. Internetworking*, Sep. 2009, pp. 3–12.

[3] P. Szikora and N. Madarász, ''Self-driving cars—The human side,'' in *Proc. IEEE 14th Int. Sci. Conf. Informat.*, Nov. 2017, pp. 383–387.

[4] S. Wang, A. Huang, and T. Zhang, ''Performance evaluation of IEEE 802.15.4 for V2V communication in VANET,'' in *Proc. Int. Conf. Comput. Inf. Sci.*, Jun. 2013, pp. 1603–1606.

[5] A. Ghazy and T. Ozkul, ''Design and simulation of an artificially intelligent VANET for solving traffic congestion,'' in *Proc. 6th Int. Symp. Mechatronics Appl.*, Mar. 2009, pp. 1–6.

[6] H. Sedjelmaci, M. A. Messous, S. M. Senouci, and I. H. Brahmi, ''Toward a lightweight and efficient UAV-aided VANET,'' *Trans. Emerg. Telecommun. Technol.*, vol. 30, no. 8, Aug. 2019, Art. no. e3520.

[7] S. Jobaer, Y. Zhang, M. A. I. Hussain, and F. Ahmed, ''UAV-assisted hybrid scheme for urban road safety based on VANETs,'' *Electronics*, vol. 9, no. 9, p. 1499, Sep. 2020.

[8] J. Ryu, J. Oh, D. Kwon, S. Son, J. Lee, Y. Park, and Y. Park, ''Secure ECC-based three-factor mutual authentication protocol for telecare medical information system,'' *IEEE Access*, vol. 10, pp. 11511–11526, 2022.

[9] M. Wazid, A. K. Das, K. R. Choo, and Y. Park, ''SCS-WoT: Secure communication scheme for Web of Things deployment,'' *IEEE Internet Things J.*, vol. 9, no. 13, pp. 10411–10423, Jul. 2022.

[10] Y. Cho, J. Oh, D. Kwon, S. Son, S. Yu, Y. Park, and Y. Park, ''A secure three-factor authentication protocol for E-governance system based on multiserver environments,'' *IEEE Access*, vol. 10, pp. 74351–74365, 2022.

[11] Z. Liu, C. Zhan, Y. Cui, C. Wu, and H. Hu, ''Robust edge computing in UAV systems via scalable computing and cooperative computing,'' *IEEE Wireless Commun.*, vol. 28, no. 5, pp. 36–42, Oct. 2021.

[12] L. Gupta, R. Jain, and G. Vaszkun, ''Survey of important issues in UAV communication networks,'' *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1123–1152, 2nd Quart., 2016.

[13] Y. Hao, Y. Cheng, and K. Ren, ''Distributed key management with protection against RSU compromise in group signature based VANETs,'' in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2008, pp. 1–5.

[14] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, ''Blockchain-based decentralized trust management in vehicular networks,'' *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

[15] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, ''Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of Drones deployment,'' *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3572–3584, Apr. 2019.

[16] 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.

[17] C. Herder, M. Yu, F. Koushanfar, and S. Devadas, ''Physical unclonable functions and applications: A tutorial,'' *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[18] S. Nakamoto. (2008). *Bitcoin: A Peer-To-Peer Electronic Cash System*. Accessed: Nov. 2022. [Online]. Available: http://bitcoin.org/bitcoin.pdf

[19] M. Abdalla, P. A. Fouque, and D. Pointcheval, ''Password-based authenticated key exchange in the three-party setting,'' in *Proc. 8th Int. Workshop Theory Pract. Public Key Cryptography (PKC)* (Lecture Notes in Computer Science), Les Diablerets, Switzerland, vol. 3386, 2005, pp. 65–84.

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

[21] L. Viganò, ''Automated security protocol analysis with the AVISPA tool,'' *Electron. Notes Theor. Comput. Sci.*, vol. 155, pp. 61–86, May 2006.

[22] H. Menouar, I. Guvenc, K. Akkaya, A. S. Uluagac, A. Kadri, and A. Tuncer, ''UAV-enabled intelligent transportation systems for the smart city: Applications and challenges,'' *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 22–28, Mar. 2017.

[23] Y. Zeng, X. Xu, and R. Zhang, "Trajectory design for completion time minimization in UAV-enabled multicasting," *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2233–2246, Apr. 2018.
[24] H. Ghazzai, H. Menouar, A. Kadri, and Y. Massoud, "Future UAV-based ITS: A comprehensive scheduling framework," *IEEE Access*, vol. 7, pp. 75678–75695, 2019.
[25] F. Outay, H. A. Mengash, and M. Adnan, "Applications of unmanned aerial vehicle (UAV) in road safety, traffic and highway infrastructure management: Recent advances and challenges," *Transp. Res. A, Policy Pract.*, vol. 141, pp. 116–129, Nov. 2020.
[26] A. Raza, S. H. R. Bukhari, F. Aadil, and Z. Iqbal, "An UAV-assisted VANET architecture for intelligent transportation system in smart cities," *Int. J. Distrib. Sensor Netw.*, vol. 17, no. 7, p. 15501477211031750, 2021.
[27] P. Gope and B. Sikdar, "An efficient privacy-preserving authenticated key agreement scheme for edge-assisted Internet of Drones," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13621–13630, Nov. 2020.
[28] J. Zhang, J. Cui, H. Zhong, I. Bolodurina, and L. Liu, "Intelligent drone-assisted anonymous authentication and key agreement for 5G/B5G vehicular ad-hoc networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 4, pp. 2982–2994, Oct. 2021.
[29] M. A. Khan, I. Ullah, A. Alkhalifah, S. U. Rehman, J. A. Shah, M. I. Uddin, M. H. Alsharif, and F. Algarni, "A provable and privacy-preserving authentication scheme for UAV-enabled intelligent transportation systems," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3416–3425, May 2022.
[30] Y. Cheng, S. Xu, M. Zang, and W. Kong, "LPPA: A lightweight privacy-preserving authentication scheme for the Internet of Drones," in *Proc. IEEE 21st Int. Conf. Commun. Technol. (ICCT)*, Oct. 2021, pp. 656–661.
[31] M. A. El-Zawawy, A. Brighente, and M. Conti, "Authenticating drone-assisted Internet of vehicles using elliptic curve cryptography and blockchain," *IEEE Trans. Netw. Service Manage.*, early access, Oct. 28, 2022, doi: 10.1109/TNSM.2022.3217320.
[32] S. Pandey, S. Deyati, A. Singh, and A. Chatterjee, "Noise-resilient SRAM physically unclonable function design for security," in *Proc. IEEE 25th Asian Test Symp. (ATS)*, Hiroshima, Japan, Nov. 2016, pp. 55–60.
[33] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.
[34] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Proc. Int. Conf. Theory Appl. Cryptogr. Techn.*, 2001, pp. 453–474.
[35] A. K. Das, B. Bera, M. Wazid, S. S. Jamal, and Y. Park, "On the security of a secure and lightweight authentication scheme for next generation IoT infrastructure," *IEEE Access*, vol. 9, pp. 71856–71867, 2021.
[36] S. Son, Y. Park, and Y. Park, "A secure, lightweight, and anonymous user authentication protocol for IoT environments," *Sustainability*, vol. 13, no. 16, p. 9241, Aug. 2021.
[37] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Annu. Int. Cryptol. Conf.*, 1999, pp. 388–397.
[38] S. Son, J. Lee, Y. Park, Y. Park, and A. K. Das, "Design of blockchain-based lightweight V2I handover authentication protocol for VANET," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, pp. 1346–1358, May 2022.
[39] D. Kwon, S. Son, Y. Park, H. Kim, Y. Park, S. Lee, and Y. Jeon, "Design of secure handover authentication scheme for urban air mobility environments," *IEEE Access*, vol. 10, pp. 42529–42541, 2022.
[40] S. Yu and Y. Park, "A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions," *IEEE Internet Things J.*, vol. 9, no. 20, pp. 20214–20228, Oct. 2022.
[41] E. Androulaki et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Pro. 13th EuroSys Conf.*, Apr. 2018, pp. 1–15.
[42] V. Boyko, P. Mackenzie, and S. Patel, "Provably secure password authenticated key exchange using Diffie–Hellman," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 1807. Bruges, Belgium: Springer, 2000, pp. 156–171.
[43] D. Von Oheimb, "The high-level protocol specification language HLPSL developed in the EU project AVISPA," in *Proc. 3rd APPSEM II Workshop Appl. Semantics (APPSEM)*, Tallinn, Estonia, 2005, pp. 1–17.
[44] D. Basin, S. Mödersheim, and L. Viganò, "OFMC: A symbolic model checker for security protocols," *Int. J. Inf. Secur.*, vol. 4, no. 3, pp. 181–208, Jun. 2005.
[45] M. Turuani, "The CL-atse protocol analyser," in *Proc. Int. Conf. Rewriting Techn. Appl.*, 2006, pp. 277–286.
[46] *Miracl Library*. Accessed: May 2023. [Online]. Available: https://github.com/miracl/MIRACL

SEUNGHWAN SON received the B.S. and M.S. degrees in mathematics from the School of Electronic and Electrical Engineering, Kyungpook National University, Daegu, South Korea, in 2019 and 2021, respectively, where he is currently pursuing the Ph.D. degree. His research interests include authentication, blockchain, cryptography, and information security.

DEOKKYU KWON (Graduate Student Member, IEEE) received the B.S. degree in electronics engineering and the M.S. degree in electronics and electrical engineering from Kyungpook National University, Daegu, South Korea, in 2020 and 2022, respectively, where he is currently pursuing the Ph.D. degree with the School of Electronic and Electrical Engineering. His research interests include the Internet of Drones, wireless sensor networks, mutual authentication, and information security.

SANGWOO LEE received the B.S., M.S., and Ph.D. degrees in electronics from Kyungpook National University, Daegu, Republic of Korea, in 1999, 2001, and 2009, respectively. Since 2001, he has been a Principal Engineering Staff with the Electronics and Telecommunications Research Institute (ETRI), Daejeon, South Korea. He was a Visiting Research Fellow with the WMG, University of Warwick, U.K., from 2016 to 2017. He is currently a Rapporteur of Q13, security aspects on ITS in ITU-T SG17. His research interests include information security based on cryptography, hardware architectures for cryptographic algorithms, and ITS security. He is also the Editor of X.1371, X.1372, X.1374, and X.1375 for ITS security.

YONGSUNG JEON received the B.S., M.S., and Ph.D. degrees in electronics engineering from Kyungpook National University, in 1986, 1990, and 2010, respectively. He was with the Agency for Defense and Development (ADD), Daejeon, South Korea, from 1992 to 1999. He has been with the Electronics and Telecommunications Research Institute (ETRI), Daejeon, since 1999, where he is currently a Principal Research Engineer. His research interests include wireless covert channel, information security, and cryptography.

ASHOK KUMAR DAS (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering, the M.Tech. degree in computer science and data processing, and the M.Sc. degree in mathematics from IIT Kharagpur, India. He was a Visiting Faculty with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA, USA. He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. His Google Scholar H-index is 70 and i10-index is 202 with over 13,900 citations. His current research interests include cryptography, system and network security, including security in smart grids, the Internet of Things (IoT), the Internet of Drones (IoD), the Internet of Vehicles (IoV), cyberphysical systems (CPS), cloud computing, blockchain, and AI/ML security. He has authored over 320 papers in international journals and conferences in the above areas, including over 275 reputed journal articles. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He also served as one of the technical program committee chairs for the first International Congress on Blockchain and Applications (BLOCKCHAIN 2019), Avila, Spain, in June 2019, the International Conference on Applied Soft Computing and Communication Networks (ACN 2020), Chennai, India, in October 2020, and the second International Congress on Blockchain and Applications (BLOCKCHAIN 2020), L'Aquila, Italy, in October 2020. He was/is on the editorial board of IEEE SYSTEMS JOURNAL, *Journal of Network and Computer Applications* (Elsevier), *Computer Communications* (Elsevier), *Journal of Cloud Computing* (Springer), *Cyber Security and Applications* (Elsevier), *IET Communications*, *KSII Transactions on Internet and Information Systems*, and *International Journal of Internet Technology and Secured Transactions* (Inderscience).

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. From 1996 to 2008, he was a Professor with the School of Electronic and Electrical Engineering, Sangju National University, South Korea. From 2003 to 2004, he was a Visiting Scholar with the School of Electrical Engineering and Computer Science, Oregon State University, USA. He is currently a Professor with the School of Electronic and Electrical Engineering, Kyungpook National University. His research interests include computer networks, multimedia, and information security.