IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 13, 2020, accepted September 3, 2020, date of publication September 8, 2020, date of current version September 24, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3022778

IoV-SMAP: Secure and Efficient Message Authentication Protocol for IoV in Smart City Environment

SUNGJIN YU[1], JOONYOUNG LEE[1], KISUNG PARK[2], ASHOK KUMAR DAS[3], (Senior Member, IEEE), AND YOUNGHO PARK[1], (Member, IEEE)

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

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

This work was supported by the National Research Foundation of Korea (NRF) funded by the Ministry of Education through the Basic Science Research Program under Grant 2020R1I1A3058605.

ABSTRACT With the emergence of the concept of smart city and the increasing demands for a range of vehicles, Internet of Vehicles (IoV) has achieved a lot of attention by providing multiple benefits, including vehicle emergence, accidents, levels of pollution, and traffic congestion. Moreover, IoV provides various services by combining vehicular ad-hoc networks (VANET) with the Internet of Things (IoT) in smart cities. However, the communication among vehicles is susceptible to various security threats because the sensitive message is transmitted via a insecure channel in the IoV-based smart city environment. Thus, a secure message authentication protocol is indispensable to ensure various services for IoV in a smart city environment. In 2020, a secure message authentication protocol for IoV communication in smart cities has been proposed. However, we discover that the analyzed scheme suffers from various potential attacks such as impersonation, secret key disclosure, and off-line guessing attacks, and also does not ensure authentication. To solve the security threats of the analyzed scheme, we design a secure and efficient message authentication protocol for IoV in a smart city environment, called IoV-SMAP. The proposed IoV-SMAP can resist security drawbacks and provide user anonymity, and mutual authentication. We demonstrate the security of IoV-SMAP by performing informal and formal analyses such as the Real-or-Random (ROR) model, and Automated Validation of Internet Security Protocols and Application (AVISPA) simulations. In addition, we compare the performance of IoV-SMAP with related existing competing authentication schemes. We demonstrate that IoV-SMAP provides better security along with efficiency than related competing schemes and is suitable for the IoV-based smart city environment.

INDEX TERMS Message authentication, IoV, smart city, ROR model, AVISPA simulation.

I. INTRODUCTION

A report on global road safety by the "World Health Organization (WHO)" in 2019 [1], shows that traffic accidents are approximately 1.25 million each year and it is the eighth leading cause of death for citizens of all ages. If certain precautions are not taken to address these problems, traffic accidents will become the fifth leading cause of death by 2030 [2]. In this regard, systematic methods for improving road safety and preventing vehicular accidents have been studied in the scientific communities for many years.

With the advances in "Vehicular Ad-Hoc Networks (VANET)", "Internet of Things (IoT)", and road infrastructure have made the realization of smart cities possible in the future [3]–[7]. The smart cities emerged as "a strategy to alleviate the challenges of rapid and continuous urbanization which at the same time provide a better quality of life for citizens" [8]. However, the significant issues in smart cities are the challenge to gather/deliver data to the deployed hundreds of thousands of actuators and sensors integrated into smart objects (e.g. vehicles, buildings, infrastructures, and so on). Internet of Vehicles (IoV) combined with VANET and IoT is considered a promising solution to resolve this problem. IoV

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

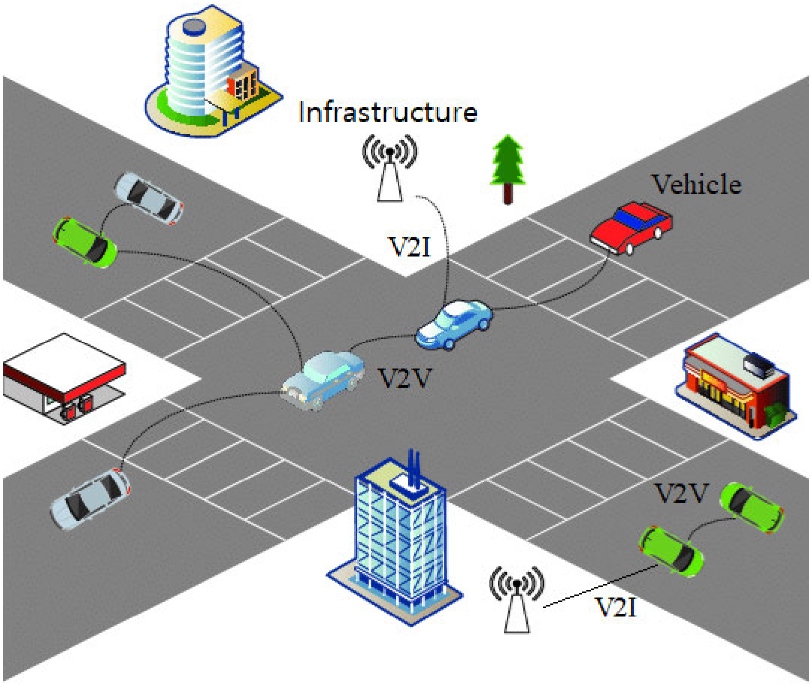


FIGURE 1. System model for IoV in smart city environment.

has been rapidly evolving in the past few years due to useful features, including congestion avoidance, low operational costs, and road safety assurance features [9]. IoV refers to communication models that communicate between vehicles and other objects by utilizing "Vehicle-to-Vehicle (V2V)" and "Vehicle-to-Infrastructure (V2I)" interactions [10]. IoV is a significant part of the industrial field and enables data sharing, interaction, control, management, and gathering of big data on roads, vehicles, buildings, infrastructure, and surroundings. IoV is composed of vehicles and infrastructure as shown in Figure 1. The vehicles collect or sense traffic information about the speed, location, and transmit it to infrastructures or other vehicles. In addition, the infrastructure provides useful services and other traffic information to passengers and drivers. However, despite several advantages that IoV offers, there are some challenges and difficulties to be solved. In VANET-based IoV communication, it may cause serious privacy problems because sensitive messages are transmitted via an insecure channel. If sensitive data of the legitimate driver is exposed, a malicious attacker can cause a vehicular accident by reporting the wrong traffic information such as slippery road, and ground slippage to the vehicle. In addition, the increasing demands for applications and services in existing vehicular networks, another significant concern is lightweight property. Due to the dynamic nature of the vehicles, the OBU should perform data computation in real-time without delay. Therefore, a secure and efficient message authentication protocol for IoV in a smart city environment is essential to resolve these problems.

A "secure and efficient message authentication protocol" should satisfy the following security requirements:

- Anonymity and untraceability: The designed protocol for IoV must be secure so that "a malicious adversary cannot reveal and trace the real identity of the legitimate drivers".
- Authentication: The designed protocol for IoV must mutually authenticate between entities and successfully obtain a significant message.
- Confidentiality: The messages exchanged among the participants need to be safely sent utilizing a secret data so that only authorized participating entities can validate the message.
- Resistance against well-known attacks: The designed protocol for IoV needs to be against various potential attacks, such as "impersonation", "man-in-the-middle (MiTM)", and "off-line guessing" attacks and so on.
- Resistance against smart card theft attack: An attacker can extract the stored secret information in the lost smart card. The knowledge of extracted information should not be sufficient for an attacker to fetch sensitive credentials in order to impersonate an authorized driver or object.
- Resistance against off-line password guessing attack: The designed protocol for IoV needs to resist the guessing of a driver's real password in the case when an adversary has the exchanged messages or the extracted smart card credentials.
- Resistance against privileged insider attack: A "privileged insider attack" should be prevented when an insider of the trusted authority having privileges can access the secret information as well as misuse the credentials.

In 2020, Vasudev *et al.* [11] designed a secure message authentication protocol for IoV communication in smart cities. Vasudev *et al.* claimed that their scheme is able to prevent potential attacks and ensure secure authentication, and anonymity. However, we discover that their scheme suffers from many drawbacks such as impersonation, secret key disclosure, MiTM attacks, and also does not provide mutual authentication. Therefore, we propose a secure and efficient message authentication protocol for IoV in smart city environment to resolve these observed security problems.

A. THREAT MODEL

We present the attack assumptions comprising the well-known "Dolev-Yao (DY) threat model" [12] to examine the security of the proposed scheme (IoV-SMAP). The capabilities of a malicious adversary are as follows. Referring to the DY model [12], an adversary is able to eavesdrop, modify, replay, inject, or delete the transmitted messages via a public channel. An adversary is able to steal the legal driver's smart card and extract the secret credentials stored in memory by performing the power analysis attacks [13]–[15]. After getting the secret data of the smart card, an adversary may attempt potential attacks including "offline password guessing", "forward secrecy", and "impersonation attacks", and so on [16], [17].

In addition, we apply the current *de facto* "Canetti and Krawczyk (CK)-adversary threat model" [18], which is more powerful than the DY threat model. Under the CK-adversary can compromised the session states, secret keys and also session keys through a session-hijacking attack apart from all the capabilities of the adversary under the DY threat model. Thus, the session key generation between two entities must be dependant of both the "short-term (temporal) secrets" and "long-term (permanent) secrets".

B. MOTIVATION

As depicted in Section II, most of the related schemes fail to ensure the required security functionalities such as "masquerade attack", "off-line password guessing attack", "MiTM attack", "session key exposure attack", "replay attack", "mutual authentication", and "anonymity", which are considered to be major requirements in the IoV environment. In addition, most of the existing schemes are unsuitable for IoV environments as it utilizes bilinear pairing, signature, and encryption which consume high computation cost. These facts motivated us to come up with secure message authentication and key agreement scheme design which can provide security features and resolve security drawbacks and threats that exist in related authentication schemes in the IoV environment.

C. RESEARCH CONTRIBUTIONS

The main contributions of our proposed IoV-SMAP can be summarized as follows.

- We analyze that Vasudev *et al.*'s scheme suffers from security flaws such as impersonation, secret key disclosure, MiTM attacks. We also discover that their scheme is unable to provide secure authentication.
- We propose a secure and efficient message authentication protocol. The proposed IoV-SMAP resolves the security drawbacks of the Vasudev *et al.*'s scheme. Thus, IoV-SMAP not only satisfies various security properties but also prevents potential attacks.
- We perform the formal (mathematical) security analysis by using the "Real-or-Random (ROR) model" [19] to prove "session key security" of IoV-SMAP.
- We perform the simulation analysis utilizing "Automated Validation of Internet Security Protocols and Application (AVISPA) [20], [21]" to prove that IoV-SMAP prevents against MiTM and replay attacks, which is formal security verification simulation tool.
- We provide the comparative performance study of IoV-SMAP with the existing competing schemes in terms of "computational time", "communication cost", and "storage overhead" through the performance evaluation. According to the "security and performance analysis", we present that IoV-SMAP ensures better security along with more "security and functionality features", and ensures efficient performances as compared with existing schemes.

D. PAPER ORGANIZATION

The outline of our paper is summarized as follows. The discussion of the related work on authentication schemes related to the IoV applications is given in Section II. Section III proves the security drawbacks of Vasudev *et al.*'s scheme and Section IV proposes a secure message authentication protocol for IoV in smart city environment (IoV-SMAP) to solve the security problems of the existing schemes. Section V proves the security of IoV-SMAP by performing formal and informal security analysis. In Section VI, we perform simulation of the proposed IoV-SMAP for formal security verification. Section VII presents the results of the performance evaluation of the IoV-SMAP compared with those of the existing competing authentication schemes. At the end, the paper is concluded in Section VIII.

II. RELATED WORK

In the last few decades, many authentication and key agreement schemes [22], [23], [25] have been presented for IoV in smart city environments to provide user privacy and useful services. Li *et al.* [24] presented "an authentication framework with privacy-preservation and non-repudiation" for VANET. However, Dua *et al.* [25] pointed out that Li *et al.*'s scheme [24] is unable to prevent session key disclosure attacks and is unable to provide user anonymity. Wang *et al.* [26] presented a privacy-preserving two-factor based authentication scheme for VANET. Amin *et al.* [27] proved that Wang *et al.*'s scheme [26] is unable to resist off-line password guessing, impersonation, and smart card stolen attacks and cannot ensure user anonymity. Liu *et al.* [28] proposed "a secure and efficient privacy-preserving authentication and key agreement scheme" utilizing bilinear pairing, signature, and encryption for V2V communication in the IoV environment. However, their scheme [28] is not suitable for IoV environment in terms of computation cost and execution time due to high-cost operations. In addition, these schemes [24]–[28] are inefficient and inapplicable for actual vehicular communication in smart city environment because they utilize public-key cryptosystems (PKC) that require high computation, communication, and storage overheads.

In recent years, many lightweight researches [29]–[31] have been designed on IoV combined with VANET and IoT to solve these problems. Ying and Nayak [29] proposed a secure and lightweight authentication scheme for IoV. However, Chen *et al.* [30] analyzed that Ying *et al.*'s scheme [29] suffers from many drawbacks such as location spoofing, replay, and off-line identity guessing attacks and also consumed considerable time for authentication. Thus, Chen and Xiang [30] presented a secure authentication scheme for IoVs to resolve the security drawbacks of Ying *et al.*'s scheme [29]. However, Chen *et al.*'s scheme [30] has the disadvantage of high total storage costs because it stores large amounts of data in memory. Kaiwartya *et al.* [31] presented a five-layer architecture for IoVs with coordination, perception, artificial intelligence (AI), and application as layers. These layers provide communications for IoVs, including V2V, V2I, V2R, V2P and V2S. However, Kaiwartya *et al.* [31] does not deal with a security protocol for registration and authentication in IoV environments. Vasudev *et al.* [11] presented a secure and efficient message authentication protocols for IoV communication such as V2V, V2S, V2R, V2I, and V2P to address problems of Kaiwartya *et al.*'s [31]. Vasudev *et al.* [11] claimed that their scheme is able to resist various security threats. However, we demonstrate that Vasudev *et al.*'s scheme [11] does not resist potential attacks such as secret key exposure, impersonation, and MiTM attacks, and also does not provide mutual authentication. Thus, we design a secure and efficient message authentication protocol for IoV in smart city environment to resolve security threats of the existing schemes.

III. CRYPTANALYSIS OF VASUDEV *et al.*'s SCHEME

In 2020, Vasudev *et al.*'s scheme [11] claimed that their protocol is able to resist various security threats. However, we demonstrate that Vasudev *et al.*'s scheme is unable to resists various security threats such as secret key disclosure, MiTM, and impersonation attacks and also does not ensure authentication. We analyze V2V and V2I processes in Vasudev *et al.*'s scheme [11]. Vasudev *et al.*'s scheme is comprised of three processes: setup, registration, and authentication. The symbols used in our paper are summarized in Table 1.

TABLE 1. Notations.

Symbol	itemize
V_i	Vehicle
VS	Vehicle server
IS	Infrastructure
ID_{V_i}	V_i's identity
PW_{V_i}	V_i's password
SK	Session key
R_i, B_i	Random nonce of V_i and IS
K_{VS}	Master key of VS
T_1, T_2	Current timestamps
ΔT	Maximum transmission delay
$h(\cdot)$	Hash function
$\oplus$	XOR operation
$\|\|$	Concatenation operation

A. IMPERSONATION ATTACK

A malicious adversary (MA) may attempt to masquerade legal drivers through stolen smart card. Referring to Section I-A, we assume that MA is able to extract the secret data stored in the smart card. In addition, MA is able to eavesdrop, modify, replay, inject, or delete the transmitted messages via a public channel. Thus, MA can perform the impersonation as shown in the following detailed steps.

1) V2V SCENARIO

Step 1: MA first intercepts the transmitted messages via a public channel and extracts the secret data $\{Z_a, U_a, W_a\}$ stored in smart card. Then, MA computes $K_{VS} = Z_a \oplus h(U_a||W_a), p_a = A_a \oplus h(K_{VS}||T_1)$, and $M_{reqst} = B_a \oplus p_a \oplus K_{VS}$. After that, the MA selects a new random nonce p_{MA} and calculates $A_{MA} = h(K_{VS}||T_1) \oplus p_{MA}$ and $B_{MA} = M_{reqst} \oplus p_{MA} \oplus K_{VS}$, where T_1 is the current timestamp. Then, MA sends $\{A_{MA}, B_{MA}, T_1\}$ to the V_E.

Step 2: After reception of messages, the V_E checks the timestamp T_1. If it is valid, the V_E inputs ID_{E_i}, PW_{E_i}, and z_{v_e}. Then, the V_E computes $U^*_{v_e} = h(ID_{E_i}||z_{v_e})$ and $W^*_{v_e} = h(PW_{E_i}||z_{v_e})$ and checks $U^*_{v_e} \overset{?}{=} U_{v_e}$ and $W^*_{v_e} \overset{?}{=} W_{v_e}$. If it is equal, V_E generates a timestamp T_2 and calculates $K_{VS} = Z_{v_e} \oplus h(U_{v_e}||W_{v_e})$, $p_{MA} = A_{MA} \oplus h(K_{VS}||T_1)$, $M_{reqst} = B_{MA} \oplus p_{MA} \oplus K_{VS}$, $C_{MA} = h(p_{MA}||\Delta T_1||K_{VS})$, and $D_{MA} = C_{MA} \oplus K_{VS} \oplus p_{MA}$. Finally, the V_E encrypts the $EM_{rply} = Enc_{C_{MA}}(M_{rply})$ and sends $\{EM_{rply}, D_{MA}, T_2\}$ to the MA.

Step 3: After reception of messages, the MA computes $C^*_{MA} = h(p_{MA}||\Delta T_1||K_{VS})$ and $C_{MA} = D_{MA} \oplus K_{VS} \oplus p_{MA}$ and checks $C^*_{MA} \overset{?}{=} C_{MA}$. Finally, the MA decrypts $M_{rply} = Dec_{C_{MA}}(EM_{rply})$.

2) V2I SCENARIO

Step 1: According to the Section I-A, the MA obtains the secret credentials through public channel and smart card. MA calculates $K_{VS} = Z_a \oplus h(U_a||W_a)$, $t_a = \beta_a \oplus K_{VS} \oplus T_{10}$, $X_a = h(t_a||K_{VS}||T_{10})$, and $Y_a = M_{rqst} \oplus t_a \oplus K_{VS}$. Then, the MA selects a new random nonce t_{MA} and computes $B_{MA} = t_{MA} \oplus K_{VS} \oplus T_{10}$, $X_{MA} = h(t_{MA}||K_{VS}||T_{10})$, and

$Y_{MA} = M_{rqst} \oplus t_{MA} \oplus K_{VS}$. After that, the MA sends $\{B_{MA}, X_{MA}, Y_{MA}, T_{10}\}$ to the IS.

Step 2: After reception of messages, the IS calculates $K_{VS} = Q_i \oplus h(ID_{IS_i}||x_i)$, $t_{MA} = \beta \oplus T_{10} \oplus K_{VS}$ and $X_i = h(t_{MA}||K_{VS}||T_{10})$ and checks $X_i^* \overset{?}{=} X_i$. If it is correct, the IS generates a T_{11} and computes $M_{rqst} = Y_i \oplus t_{MA} \oplus K_{VS}$, $A_{MA} = h(t_{MA}||\Delta T_{10}||K_{VS}||X_{MA})$, $U_{MA} = A_{MA} \oplus K_{VS} \oplus X_{MA} \oplus t_{MA}$. Finally, the IS encrypts $EM_{rpy} = Enc_{A_{MA}}(M_{rpy})$ and sends $\{EM_{rpy}, U_{MA}, T_{11}\}$ to the MA.

Step 3: After reception of messages, the MA calculates $A_{MA}^* = U_{MA} \oplus K_{VS} \oplus X_{MA} \oplus t_{MA}$ and decrypts $M_{rpy} = DEC_{A_{MA}}(EM_{rpy})$.

As a result, Vasudev *et al.*'s scheme is fragile to the impersonation attack because the MA is able to masquerade as a legitimate driver successfully.

B. SECRET KEY DISCLOSURE ATTACK

According to Section III-A1 and III-A2, we prove that MA is able to masquerade legal driver V_i and obtain the vehicle server's secret key K_{VS} and symmetric key $\{C_e, A_e\}$ between each entity as follows. Referring to Section I-A, the MA is able to extract secret credentials $\{Z_a, U_a, W_a\}$ stored in smart card. Then, MA can calculate vehicle server's secret key $K_{VS} = Z_a \oplus h(U_a||W_a)$, and random nonce $p_a = A_a \oplus h(K_{VS}||T_1)$. Consequently, the MA is able to perform the secret key disclosure attack by calculating $C_e = D_e \oplus K_{VS} \oplus p_a$ and disguise as legitimate drivers.

C. MAN-IN-THE-MIDDLE ATTACK

The MA attempts to trick two entities in IoV communication, which means that MA is able to masquerade a legitimate driver. However, referring to Section III-A1 and III-A2, the MA is able to masquerade the legal driver and generate the symmetric key $\{C_e, A_e\}$, and the vehicle server's master key K_{VS}. Consequently, Vasudev *et al.*'s scheme is not secure against MiTM attack.

D. AUTHENTICATION

Vasudev *et al.* claimed that their scheme ensures secure message authentication between each entity. However, referring to Section III-A1 and III-A2, a MA is able to obtain the VS's secret key K_{VS} and symmetric key between each entity. Then, the MA can generate authentication request messages $\{B_a, I_a, G_a, Y_a, R_a\}$ and response messages $\{EM_{rply}, EM_{rp}, EM_{rep}, EM_{rpy}, EM_{reply}\}$, and achieve message authentication with other entities successfully. Consequently, Vasudev *et al.*'s scheme does not ensure secure message authentication.

IV. THE PROPOSED SCHEME

This section presents a secure message authentication protocol for IoV communication to solve the security threats of the existing scheme. IoV-SMAP is composed of three processes: a) initialization, b) registration, and c) authentication.

A. INITIALIZATION PROCESS

The vehicle server (VS) registers all IoV objects in the communication system. The VS selects a random nonce RN_{vs} and calculates a secret key $K_{VS} = h(ID_{vs}||RN_{vs})$. The VS stores a pre-computed master key K_{VS} in the secure database. The VS also selects a "collision-resistant one-way hash function $h(\cdot)$" (for example, Secure Hash Algorithm (SHA-256) [32]).

B. REGISTRATION PROCESS

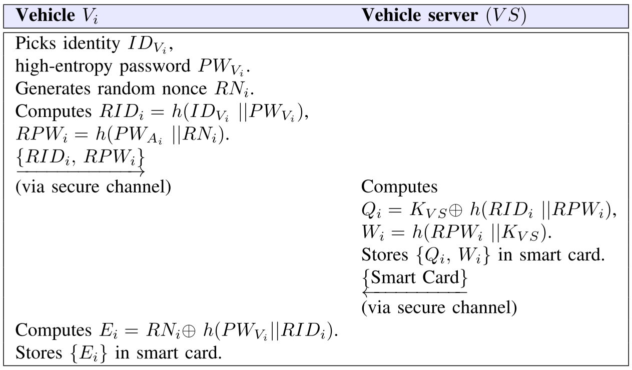
The registration process includes both V2V and V2I registration, which are explained in the following subsections.

1) V2V REGISTRATION PROCESS

If a vehicle V_i wants to access the traffic information with other IoV objects in the system, the V_i must register within the VS using the following steps:

- **Step 1:** V_i selects its identity ID_{V_i} and a high-entropy password PW_{V_i}, and then generates a random nonce RN_i. After that, V_i calculates $RID_i = h(ID_{V_i}\ ||PW_{V_i})$ and $RPW_i = h(PW_{A_i}\ ||RN_i)$, and sends the registration information $\{RID_i,\ RPW_i\}$ to the VS via a secure channel.
- **Step 2:** Upon reception of the information from V_i, the VS computes $Q_i = K_{VS} \oplus h(RID_i\ ||RPW_i)$ and $W_i = h(RPW_i\ ||K_{VS})$. Finally, the VS stores $\{RN_{vs}\}$ in secure database. In addition, VS stores $\{Q_i,\ W_i\}$ in the smart card and sends smart card to the V_i.
- **Step 3:** After reception of smart card, the V_i computes $E_i = RN_i \oplus h(PW_{V_i}||RID_i)$ and stores $\{E_i\}$ in smart card.

The V2V registration process is summarized in Figure 2.



Vehicle V_i	**Vehicle server** (VS)
Picks identity ID_{V_i}, high-entropy password PW_{V_i}. Generates random nonce RN_i. Computes $RID_i = h(ID_{V_i}\ ||PW_{V_i})$, $RPW_i = h(PW_{A_i}\ ||RN_i)$. $\xrightarrow{\{RID_i,\ RPW_i\}}$ (via secure channel)	
	Computes $Q_i = K_{VS} \oplus h(RID_i\ ||RPW_i)$, $W_i = h(RPW_i\ ||K_{VS})$. Stores $\{Q_i,\ W_i\}$ in smart card. $\xleftarrow{\{\text{Smart Card}\}}$ (via secure channel)
Computes $E_i = RN_i \oplus h(PW_{V_i}||RID_i)$. Stores $\{E_i\}$ in smart card.	

FIGURE 2. V2V registration process of IoV-SMAP.

2) V2I REGISTRATION PROCESS

If the infrastructure (IS) wants to exchange traffic information with the IoV objects in the system, the IS must register within the VS with the following steps:

- **Step 1:** The IS selects the identity ID_{IS} and sends it to the VS via a secure channel.

- **Step 2:** Upon reception of the information, the VS generates a random nonce N_{VS} and calculates $C_i = h(ID_{IS} ||N_{VS}) \oplus K_{VS}$. Finally, the VS sends $\{C_i, N_{VS}\}$ to the IS via a secure channel.
- **Step 3:** After reception of the message, the IS stores $\{C_i, N_{VS}\}$ in the secure database.

The V2I registration process is also summarized in Figure 3.

Infrastructure (IS)	Vehicle server (VS)
Picks identity ID_{IS}.	
$\xrightarrow{\{ID_{IS}\}}$	
(via secure channel)	
	Generates random nonce N_{VS}.
	Computes
	$C_i = h(ID_{IS} \|\|N_{VS}) \oplus K_{VS}$.
	$\xleftarrow{\{C_i,\ N_{VS}\}}$
	(via secure channel)
Stores $\{C_i,\ N_{VS}\}$ in secure database.	

FIGURE 3. **V2I registration process of IoV-SMAP.**

C. V2V AUTHENTICATION PROCESS

If a vehicle V_A wants to access traffic information with the other IoV objects in the system, the V_A performs the following process as shown in Figure 4.

Vehicle (V_A)	**Vehicle** (V_E)
Inputs ID_{A_i} and PW_{A_i}	
Computes	
$RID_i = h(ID_{A_i}\|\|PW_{A_i})$	
$RN_i = E_i \oplus h(PW_{A_i}\|\|RID_i)$	
$RPW_i = h(PW_{A_i}\|\|RN_i)$	
$K_{VS} = Q_i \oplus h(RID_i\|\|RPW_i)$	
$W_i = h(RPW_i\|\|K_{VS})$	
Checks $W_i^* \overset{?}{=} W_i$	
Generates a random nonce R_1	
and timestamp T_1	
Computes	Checks $\|T_1^* - T_1\| \leq \Delta T$
$M_1 = R_1 \oplus h(K_{VS}\|\|T_1)$	Inputs ID_{E_i} and PW_{E_i}
$M_2 = M_{request1} \oplus h(R_1\|\|K_{VS})$	Computes
$M_{AE} = h(M_{request1}\|\|R_1\|\|K_{VS}\|\|T_1)$	$RN_e = E_e \oplus h(ID_{E_i}\|\|PW_{E_i})$
	$RID_e = h(ID_{E_i}\|\|RN_e)$
$\xrightarrow{Msg_{V2V1} = \{M_1, M_2, M_{AE}, T_1\}}$	$RPW_e = h(PW_{E_i}\|\|RN_e)$
(via public channel)	$K_{VS} = Q_e \oplus h(RID_e\|\|RPW_e)$
	$W_e = h(RPW_e\|\|K_{VS})$
	Checks $W_e^* \overset{?}{=} W_e$
	Computes $R_1 = M_1 \oplus h(K_{VS}\|\|T_1)$
	$M_{request1} = M_2 \oplus h(R_1\|\|K_{VS})$
	$M_{AE}^* = h(M_{request1}\|\|R_1\|\|K_{VS}\|\|T_1)$
	Checks $M_{AE}^* \overset{?}{=} M_{AE}$
	Generates a random nonce R_2
	and timestamp T_2
	$M_3 = (M_{response1}\|\|R_2) \oplus h(K_{VS}\|\|R_1\|\|T_2)$
	$SK = h(R_1\|\|R_2\|\|K_{VS})$
Checks $\|T_2^* - T_2\| \leq \Delta T$	$M_{EA} = h(M_{response1}\|\|SK\|\|T_2)$
$(M_{response1}\|\|R_2) = M_3 \oplus h(K_{VS}\|\|R_1\|\|T_2)$	$\xleftarrow{Msg_{V2V2} = \{M_3, M_{EA}, T_2\}}$
$SK = h(R_1\|\|R_2\|\|K_{VS})$	(via public channel)
$M_{EA} = h(M_{response1}\|\|SK\|\|T_2)$	
Checks $M_{EA}^* \overset{?}{=} M_{EA}$	
Both V_A and V_E store the shared common session key SK	

FIGURE 4. **V2V authentication process of IoV-SMAP.**

- **Step 1:** The V_A inputs its identity ID_{A_i} and password PW_{A_i} and calculates $RID_i = h(ID_{A_i} ||PW_{A_i})$, $RN_i = E_i \oplus h(PW_{A_i} ||RID_i)$, $RPW_i = h(PW_{A_i} ||RN_i)$, $K_{VS} = Q_i \oplus h(RID_i ||RPW_i)$, and $W_i = h(RPW_i ||K_{VS})$, and checks $W_i^* \overset{?}{=} W_i$. If it is equal, the V_A generates a message $M_{resquest1}$, a random nonce R_1 and timestamp T_1. Then, V_A calculates $M_1 = R_1 \oplus h(K_{VS} ||T_1)$, $M_2 = M_{request1} \oplus h(R_1 ||K_{VS})$, and $M_{AE} = h(M_{request1} ||R_1 ||K_{VS} ||T_1)$ and sends the message $Msg_{V2V1} = \{M_1, M_2, M_{AE}, T_1\}$ to the V_E via a public channel.
- **Step 2:** After reception of message Msg_{V2V1}, the V_E checks $|T_1^* - T_1| \leq \Delta T$. If it is correct, the V_E inputs ID_{E_i} and PW_{E_i}, and computes $RN_e = E_e \oplus h(ID_{E_i} ||PW_{E_i})$, $RID_e = h(ID_{E_i} ||RN_e)$, $RPW_e = h(PW_{E_i} ||RN_e)$, $K_{VS} = Q_e \oplus h(RID_e ||RPW_e)$, and $W_e = h(RPW_e ||K_{VS})$, and checks $W_e^* \overset{?}{=} W_e$. If the condition is valid, the V_E computes $R_1 = M_1 \oplus h(K_{VS} ||T_1)$, $M_{request1} = M_2 \oplus h(R_1 ||K_{VS})$, $M_{AE}^* = h(M_{request1} ||R_1 ||K_{VS} ||T_1)$, and checks $M_{AE}^* \overset{?}{=} M_{AE}$. After that, the V_E generates a message $M_{response1}$, a random nonce R_2 and a timestamp T_2. Finally, the V_E computes $M_3 = (M_{response1} ||R_2) \oplus h(K_{VS} ||R_1 ||T_2)$, $SK = h(R_1 ||R_2 ||K_{VS})$, and $M_{EA} = h(M_{response1} ||SK ||T_2)$ and sends the message $Msg_{V2V2} = \{M_3, M_{EA}, T_2\}$ to the V_A via a public channel.
- **Step 3:** After reception of message Msg_{V2V2}, the V_A checks $|T_2^* - T_2| \leq \Delta T$. If the condition is valid, the V_A calculates $(M_{response1} ||R_2) = M_3 \oplus h(K_{VS} ||R_1 ||T_2)$, $SK = h(R_1 ||R_2 ||K_{VS})$, and $M_{EA} = h(M_{response1} ||SK|| T_2)$ and checks $M_{EA}^* \overset{?}{=} M_{EA}$. If it is correct, the V_A and the V_E are mutually authenticated successfully, and share the established session key SK for future secret communications.

D. V2I AUTHENTICATION PROCESS

If a vehicle V_i wants to exchange the traffic information from the IS, the V_i performs the following steps as shown in Figure 5.

Vehicle (V_i)	**Infrastructure** (IS)
Inputs ID_{V_i} and PW_{V_i}	
Computes	
$RID_i = h(ID_{V_i}\|\|PW_{V_i})$	
$RN_i = E_i \oplus h(PW_{V_i}\|\|RID_i)$	
$RPW_i = h(PW_{V_i}\|\|RN_i)$	
$K_{VS} = Q_i \oplus h(RID_i\|\|RPW_i)$	
$W_i = h(RPW_i\|\|K_{VS})$	
Checks $W_i^* \overset{?}{=} W_i$	
Generates a random nonce B_1	
and timestamp T_3	
Computes $V_1 = B_1 \oplus h(T_3\|\|K_{VS})$	
$V_2 = M_{request2} \oplus h(K_{VS}\|\|B_1)$	Checks $\|T_3^* - T_3\| \leq \Delta T$
$V_{VI} = h(B_1\|\|M_{request2}\|\|K_{VS}\|\|T_3)$	Computes $K_{VS} = C_i \oplus h(ID_{IS}\|\|N_{vs})$
$\xrightarrow{Msg_{V2I1} = \{V_1, V_2, V_{VI}, T_3\}}$	$B_1 = V_1 \oplus h(T_3\|\|K_{VS})$
(via public channel)	$M_{request2} = h(K_{VS}\|\|B_1) \oplus V_2$
	$V_{VI} = h(B_1\|\|M_{request2}\|\|K_{VS}\|\|T_3)$
	Checks $V_{VI}^* \overset{?}{=} V_{VI}$
	Generates a random nonce B_2
	and timestamp T_4
	Computes
	$V_3 = h(K_{VS}\|\|B_1\|\|T_4) \oplus (M_{response2}\|\|B_2)$
	$SK = h(B_1\|\|B_2\|\|K_{VS})$
	$V_{IV} = h(K_{VS}\|\|SK\|\|M_{response2}\|\|T_4)$
Checks $\|T_4^* - T_4\| \leq \Delta T$	
$(M_{response2}\|\|B_2) = V_3 \oplus h(K_{VS}\|\|B_1\|\|T_4)$	$\xleftarrow{Msg_{V2I2} = \{V_3, V_{IV}, T_4\}}$
$SK = h(B_1\|\|B_2\|\|T_4)$	(via public channel)
$V_{IV} = h(K_{VS}\|\|SK\|\|M_{response2}\|\|T_4)$	
Checks $V_{IV}^* \overset{?}{=} V_{IV}$	
Both V_i and IS store the shared common session key SK	

FIGURE 5. **V2I authentication process of IoV-SMAP.**

- **Step 1:** The V_i inputs its identity ID_{V_i} and password PW_{V_i}, and computes $RID_i = h(ID_{V_i} \,||PW_{V_i})$, $RN_i = E_i \oplus h(PW_{V_i} \,||RID_i)$, $RPW_i = h(PW_{V_i} \,||RN_i)$, $K_{VS} = Q_i \oplus h(RID_i \,||RPW_i)$, and $W_i = h(RPW_i \,||K_{VS})$ and checks $W_i^* \overset{?}{=} W_i$. If the condition is satisfied, the V_i generates a message $M_{request2}$, a random nonce B_1, and timestamp T_3. After that, the V_i computes $V_1 = B_1 \oplus h(T_3 \,||K_{VS})$, $V_2 = M_{request2} \oplus h(K_{VS} \,||B_1)$ and $V_{VI} = h(B_1 \,||M_{request2} \,||K_{VS} \,||T_3)$ and sends the message $Msg_{V2I1} = \{V_1, V_2, V_{VI}, T_3\}$ to the *IS* over a public channel.
- **Step 2:** Upon reception of the message Msg_{V2I1}, the *IS* checks $|T_3^* - T_3| \leq \Delta T$. If it is valid, the *IS* calculates $K_{VS} = C_i \oplus h(ID_{IS} \,||N_{VS})$, $B_1 = V_1 \oplus h(T_3 \,||K_{VS})$, $M_{request2} = h(K_{VS} \,||B_1) \oplus V_2$, and $V_{VI} = h(B_1 \,||M_{request2} \,||K_{VS} \,||T_3)$ and checks $V_{VI}^* \overset{?}{=} V_{VI}$. If the condition is correct, the *IS* generates a message $M_{response2}$, a random nonce B_2, and a timestamp T_4. Finally, the *IS* computes $V_3 = h(K_{VS} \,||B_1 \,||T_4) \oplus (M_{response2} \,||B_2)$, $SK = h(B_1 \,||B_2 \,||K_{VS})$, and $V_{IV} = h(K_{VS} \,||SK \,||M_{response2} \,||T_4)$ and sends the message $Msg_{V2I2} = \{V_3, V_{IV}, T_4\}$ to the V_i via an open channel.
- **Step 3:** After reception of message Msg_{V2I2}, the V_i checks $|T_4^* - T_4| \leq \Delta T$. If the condition is valid, the V_i computes $(M_{response2} \,||B_2) = V_3 \oplus h(K_{VS} \,||B_1 \,||T_4)$, $SK = h(B_1 \,||B_2 \,||T_4)$ and $V_{IV} = h(K_{VS} \,||SK \,||M_{response2} \,||T_4)$ and checks $V_{IV}^* \overset{?}{=} V_{IV}$. If it is legitimate, the V_i and the *IS* are mutually authenticated successfully, and also share the session key *SK* for their future secret communications.

V. SECURITY ANALYSIS

This section proves the security of IoV-SMAP utilizing informal and formal security analysis including ROR model, which is a well-known security analysis model. We analyze only the V2V process in IoV-SMAP. The other IoV processes are omitted because they are very similar to the V2V process.

A. FORMAL SECURITY ANALYSIS USING ROR MODEL

This section performs the ROR model [19] to demonstrate the session key (SK) security of IoV-SMAP by the passive/active adversary *MA*. This section briefly introduces the ROR model prior to performing SK security proof for the IoV-SMAP. In the IoV-SMAP, there are two participants the vehicle $P_{V_A}^{t_1}$ and the other $P_{V_E}^{t_2}$, where $P_{V_A}^{t_1}$ and $P_{V_E}^{t_2}$ are instances t_1^{th} of V_A and t_2^{th} of V_E, respectively. We define queries such as *Execute*, *Corrupt*, *Send*, *Test*, and *Reveal* for the ROR model to perform formal (mathematical) analysis.

The following queries are accessed by the adversary *MA*:

- $Execute(P_{V_A}^{t_1}, P_{V_E}^{t_2})$: *Execute* is modeled that *MA* performs the well-known attack by eavesdropping exchanged messages between participants via a public channel.
- $CorruptSC(P_{V_A}^{t_1})$: *CorruptSC* denotes the smart-card theft attack, where the *MA* is able to extract the secret parameters stored in the smart card.
- $Send(P^t, M)$: Based on this query, *MA* is able to transmit a message *M* to the instance P^t and also is able to receive accordingly.
- $Test(P^t)$: Based on this query, an unbiased coin *c* is flipped prior to the start of the experiment. The corresponding SK is fresh between V_A and V_E, and then P^t returns SK when $c = 1$ after running *Test* query and SK is new or a random nonce when $c = 0$; otherwise, it produces a $\perp$ (null value).
- $Reveal(P^t)$: Based on this query, *MA* reveals the current SK generated by its partner to the *MA*.

Hash is a random oracle, which is a one-way hash function. We utilize Zipf's law [33] to demonstrate SK security of IoV-SMAP.

Theorem 1: Suppose that $Adv_{MA}^{IoV-SMAP}$ is the advantage of the *MA* in order to break SK security for the proposed message authentication protocol (MAP). Then,

$$Adv_{MA}^{IoV-SMAP} \leq \frac{q_h^2}{|Hash|} + 2C' \cdot q_{send}^s,$$

where q_{send} and q_h are the number of *Send* and *Hash* queries, the range space of $h(\cdot)$, respectively, and Zipf's parameters [33] are C' and s.

Proof: We define the sequence of four games namely GM_i $(i \in [0, 3])$. Let $Succ_{GM_i}^{MA}$ be an event that the adversary *MA* wins the game GM_i. Then, the advantage (success probability) of *MA* for winning the GM_i is defined by $Adv_{MA,GM_i}^{IoV-SMAP} = Pr[Succ_{GM_i}^{MA}]$, where $Pr[E]$ is the probability of a random event E. All the games GM_i are described in detail as follows.

Game GM_0: GM_0 denotes the real attack with respect to the ROR model. Since the bit *c* needs to be selected at the start of GM_0. Hence, it follows from the semantic security that

$$Adv_{MA}^{IoV-SMAP} = |2 \cdot Adv_{MA,GM_0}^{IoV-SMAP} - 1| \tag{1}$$

Game GM_1: GM_1 indicates that *MA* performs an eavesdropping attack, where the exchanged messages $Msg_{V2V1} = \{M_1, M_2, M_{AE}, T_1\}$ and $Msg_{V2V2} = \{M_3, M_{EA}, T_2\}$ are intercepted using *Execute* query. Once the game ends, *MA* transmits *Test* and *Reveal* queries. The output of the *Test* and *Reveal* queries decide if *MA* gets random nonces and $SK = h(R_1||R_2||K_{VS})$ between V_A and V_E. To derive *SK*, *MA* requires the secret credentials R_1, R_2 and K_{VS}. Therefore, both the games GM_0 and GM_1 are indistinguishable. As a result, we can obtain the following result:

$$Adv_{MA,GM_1}^{IoV-SMAP} = Adv_{MA,GM_0}^{IoV-SMAP} \tag{2}$$

Game GM_2: *Send* and *Hash* queries are simulated in this active attack. GM_2 denotes an active attack, where a *MA* eavesdrops the exchanged messages Msg_{V2V1} and Msg_{V2V2}. All exchanged messages are protected using hash function $h(.)$ and also, random nonce R_1 and R_2 are utilized in the messages Msg_{V2V1} and Msg_{V2V2}. However, R_1 and R_2 are not derived from the exchanged messages due to hash function

$h(.)$. By performing the birthday paradox [34], we can get the following result:

$$|Adv^{IoV-SMAP}_{MA,GM_1} - Adv^{IoV-SMAP}_{MA,GM_2}| \leq \frac{q_h^2}{2|Hash|} \tag{3}$$

Game GM_3: In this final active game, *CorruptSC* query is simulated. MA is able to extract the secret credentials $\{Q_i, W_i, E_i\}$ from memory of the smart-card utilizing power analysis attack. Note that, $Q_i = K_{VS} \oplus h(RID_i||RPW_i)$, $W_i = h(RPW_i||K_{VS})$ and $E_i = RN_i \oplus h(PW_{v_i}||RID_i)$. GM_3 is computationally infeasible for MA to derive password PW_{V_i} of V_A correctly through *Send* query without VS's master key K_{VS} and random nonces R_1, R_2. Consequently, GM_2 and GM_3 are indistinguishable if off-line password guessing attack is not implemented. Using Zipf's law [33], we can obtain the following result:

$$|Adv^{IoV-SMAP}_{MA,GM_2} - Adv^{IoV-SMAP}_{MA,GM_3}| \leq C' \cdot q^s_{send} \tag{4}$$

When GM_0 to GM_3 are executed successfully, MA is able to guess the exact bit c. Therefore, we can obtain the following result:

$$Adv^{IoV-SMAP}_{MA,GM_3} = 1/2 \tag{5}$$

Eqs. (1), (2) and (5), we obtain the following result:

$$\begin{aligned}\frac{1}{2}Adv^{IoV-SMAP}_{MA} &= |Adv^{IoV-SMAP}_{MA,GM_0} - \frac{1}{2}| \\ &= |Adv^{IoV-SMAP}_{MA,GM_1} - \frac{1}{2}| \\ &= |Adv^{IoV-SMAP}_{MA,GM_1} - Adv^{IoV-SMAP}_{MA,GM_3}| \end{aligned} \tag{6}$$

Using the triangular inequality and Eqs. (4), (5), and (6), we obtain the following result:

$$\begin{aligned}\frac{1}{2}Adv^{IoV-SMAP}_{MA} &= |Adv^{IoV-SMAP}_{MA,GM_1} - Adv^{IoV-SMAP}_{MA,GM_3}| \\ &\leq |Adv^{IoV-SMAP}_{MA,GM_1} - Adv^{IoV-SMAP}_{MA,GM_2}| \\ &\quad + |Adv^{IoV-SMAP}_{MA,GM_2} - Adv^{IoV-SMAP}_{MA,GM_3}| \\ &\leq \frac{q_h^2}{2|Hash|} + C' \cdot q^s_{send} \end{aligned} \tag{7}$$

Finally, multiplying both sides of Eq. (7) by a factor of 2, we obtain $Adv^{IoV-SMAP}_{MA} \leq \frac{q_h^2}{|Hash|} + 2C' \cdot q^s_{send}$.

B. INFORMAL SECURITY ANALYSIS

This section proved that IoV-SMAP is able to prevent well-known attacks and provide user anonymity and authentication.

1) IMPERSONATION ATTACK

This attack assumes that a malicious adversary MA attempts to masquerade by generating a legitimate driver's login request message $\{M_1, M_2, M_{AE}, T_1\}$ and $\{V_1, V_2, V_{VI}, T_3\}$. However, MA is unable to generate the login request message because MA does not know V_i's identity ID_{V_i}, password PW_{V_i}, random nonce R_1, B_1 and VS's master key K_{VS}. Thus, IoV-SMAP is able to prevent impersonation attack because MA is unable to generate correct messages of the legitimate driver.

2) REPLAY ATTACK

MA attempts to reuse any of the previously exchanged messages $\{M_1, M_2, M_{AE}, T_1\}$, $\{M_3, M_{EA}, T_2\}$, $\{V_1, V_2, V_{VI}, T_3\}$, and $\{V_3, V_{IV}, T_4\}$ over a public channel in the V2V and V2I authentication processes. If the MA intercepts the exchanged messages in the previous session, IoV-SMAP checks the freshness of the timestamp. Furthermore, all messages in the IoV-SMAP are protected with random nonces R_1, R_2, B_1, B_2 and VS's master key K_{VS}. Consequently, IoV-SMAP is able to prevent replay attack.

3) SESSION KEY DISCLOSURE ATTACK

In the IoV-SMAP, MA must obtain random nonces (short-term secrets) R_1, R_2, B_1, B_2 and VS's master key (long-term secret) K_{VS} to generate a correct session key $SK = h(R_1||R_2||K_{VS})$ and $SK = h(B_1||B_2||K_{VS})$. However, the MA is unable to compute because K_{VS} is encrypted with VS's random nonce RN_{vs} and identity ID_{vs} using hash function. In addition, R_1, R_2, B_1, B_2 cannot be obtained because the MA does not know the K_{VS}. Thus, IoV-SMAP is secure to session key disclosure attack under the CK-adversary model as discussed in our threat model in Section I-A.

4) SMART CARD THEFT ATTACK

In the IoV-SMAP, we suppose that MA is able to steal the smart card of a legitimate driver and extract the secret credential $\{Q_i, W_i, E_i\}$ in the smart card utilizing the power analysis [13]. However, MA is unable to obtain a driver's sensitive data because the secret credentials stored in the smartcard are masked utilizing XOR and hash operations. Thus, IoV-SMAP is secure to smart card theft attack.

5) MAN-IN-THE-MIDDLE (MiTM) ATTACK

We suppose that MA is able to intercept the exchanged messages over a public channel, then a MiTM attack is possible. However, MA cannot generate the authentication request messages $\{M_{AE}, V_{VI}\}$ because MA is unable to obtain the random nonces R_1, B_1, and vehicle server's master key K_{VS}. In addition, MA is unable to generate the session key SK without random nonces $\{R_1, R_2, B_1, B_2\}$ and vehicle server's master key K_{VS}. Thus, IoV-SMAP is secure against MiTM attack.

6) ANONYMITY

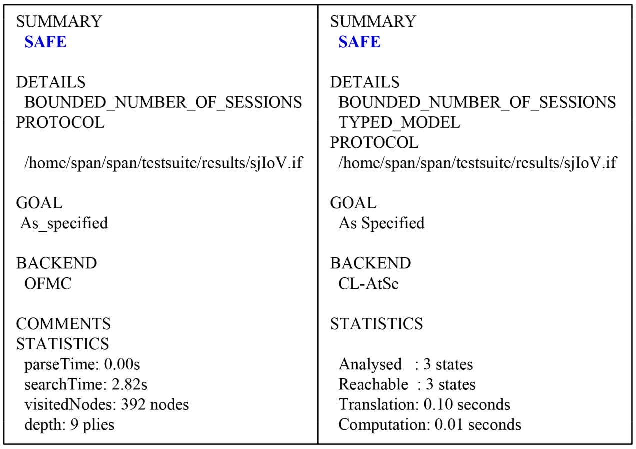
According to Section I-A, we suppose that MA is able to extract secret parameters stored in the smart card and is able to intercept the exchanged messages in the authentication process. However, MA cannot obtain the real identity of the IoV objects because transmitted messages are encrypted with master key K_{VS}, password PW_{V_i}, and random nonces N_{vs} utilizing XOR and hash operations. Therefore, IoV-SMAP provides the driver's anonymity.

7) MUTUAL AUTHENTICATION

In the IoV-SMAP, all IoV objects perform mutual authentication successfully. After getting the authentication request message $\{M_{AE}, V_{VI}\}$ from the V_i, other vehicle V_E checks $M^*_{AE} \overset{?}{=} M_{AE}$ and the IS verifies $V^*_{VI} \overset{?}{=} V_{VI}$. If the conditions hold, the V_E and IS authenticate the V_A. Upon getting the authentication response message $\{M_{EA}, V_{IV}\}$ from the V_E and IS, the V_A verifies $M^*_{EA} \overset{?}{=} M_{EA}$ and $V^*_{IV} \overset{?}{=} V_{IV}$. If the condition is valid, the V_A authenticates the V_E and the IS. Consequently, all IoV objects are mutually authenticated because the MA is unable to generate exchanged messages successfully.

VI. FORMAL SECURITY VERIFICATION USING AVISPA: SIMULATION STUDY

We simulate utilizing the AVISPA tool [20], [21] to analyze the security of IoV-SMAP against MiTM and replay attacks. The AVISPA tool implemented utilizing the ‘‘High-Level Protocol Specification Language (HLPSL)’’ [35] to generate input format (IF) of four back-ends, including ‘‘SAT-based Model Checker (SATMC)’’, ‘‘Constraint Logic-based Attack Searcher (CL-AtSE)’’, ‘‘On-the-Fly Model Checker (OFMC)’’, and ‘‘Tree automata based on Automatic Approximations for Analysis of Security Protocol (TA4SP)’’. The output format (OF) is presented the security of IoV-SMAP. To prove the security of IoV-SMAP, we first express utilizing a rule-oriented HLPSL. More details for AVISPA and HLPSL specifications can be found in [20], [21]. Various roles such as the basic specification roles for the vehicles V_A, V_E, the infrastructure IS, and the vehicle server VS, and the mandatory roles for the environment, goal, and session are implemented in HSPSL for IoV-SMAP. Because XOR operations are not supported for both TA4SP and SATMC back-ends, simulation results for these back-ends are indecisive. Thus, we show the AVISPA simulation results using OFMC and CL-AtSe in Figure 6. As a result, we prove that IoV-SMAP prevents MiTM and replay attacks.



```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL

  /home/span/span/testsuite/results/sjIoV.if

GOAL
  As_specified

BACKEND
  OFMC

COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 2.82s
  visitedNodes: 392 nodes
  depth: 9 plies
```

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/sjIoV.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 3 states
  Reachable  : 3 states
  Translation: 0.10 seconds
  Computation: 0.01 seconds
```

FIGURE 6. AVISPA simulation results using OFMC and CL-AtSe backends.

VII. PERFORMANCE ANALYSIS

To evaluate the comparative analysis on ‘‘security features’’, ‘‘computation costs’’, ‘‘communication costs’’ and ‘‘storage costs’’, this section considers the authentication process for IoV-SMAP with those of other related schemes [11], [24], [26].

A. SECURITY FEATURES

In Table 2, we present the security features of IoV-SMAP compared to existing schemes [11], [24], [26]. Referring to Table 2, existing schemes [11], [24], [26] suffer from various attacks and also their schemes is unable to provide authentication and anonymity. In contrast, IoV-SMAP prevents various attacks and provides authentication and anonymity. Thus, IoV-SMAP offers essential security requirements compared with existing schemes.

TABLE 2. Comparison of security features.

Feature	Li *et al.* [24]	Wang *et al.* [26]	Vasudev *et al.* [11]	Ours
SFT_1	○	×	×	○
SFT_2	○	×	×	○
SFT_3	×	○	×	○
SFT_4	○	○	○	○
SFT_5	○	○	×	○
SFT_6	○	○	×	○
SFT_7	×	×	○	○
SFT_8	×	×	×	○

○: “Preservation of security features”; ×: “Non-preservation of security features”; SFT_1: “Smart card theft attack”; SFT_2: “Impersonation attack”; SFT_3: “Session/secret key disclosure attack”; SFT_4: “Replay attack”; SFT_5: “MiTM attack”; SFT_6: Authentication; SFT_7: User anonymity; SFT_8: Formal (mathematical) analysis

B. COMPUTATION COSTS

We compare the computation cost of IoV-SMAP with related schemes [11], [24], [26] during the authentication process. We estimated the following parameters based on Vasudev *et al.*'s scheme [11]. T_{AE}, T_{AD}, T_S, T_{SE}, T_{SD}, and T_h denote the asymmetric encryption, asymmetric decryption, signing operation, symmetric encryption, symmetric decryption and hash function using SHA-256 hashing function, respectively. Referring to [11], we denote the computation time for various types of cryptographic operations in Table 3. XOR operation is negligible compared to other cryptographic operations because it requires low computation time. The configuration of the Desktop Computer is ‘‘Windows 10, Professional with an Intel (R) Core (TM) CPU i5-7200U, 8.1 GB memory, @2.50 GHz’’. In addition, the configuration

TABLE 3. Computation time for various cryptographic primtives [11].

Operations	Desktop Computer (DC)	Raspberriy Pi (RP)
T_{AE}	4.406 ms	866.733 ms
T_{AD}	7.761 ms	2686.533 ms
T_S	24.835 ms	709.149 ms
T_{SE}	7.761 ms	2686.533 ms
T_{SD}	0.001 ms	1800 ms
T_h	0.002 ms	0.174 ms

of Raspberry Pi is "BCM 2708 System-On-Chip (SOC) with an ARMv6-compatible processor and 8 GB SD card", and also the source code is implemented in Python 3.6.

In V2V authentication phase, the total computation costs of IoV-SMAP and Vasudev *et al.*'s scheme [11] are $17T_h$ and $6T_h + T_{SE} + T_{SD}$, respectively. According to Table 4, the total computation times of IoV-SMAP are 0.034 ms and 2.958 ms, which is implemented on the Desktop Computer and Raspberry Pi platform, respectively. Consequently, IoV-SMAP provides more efficient computation times compared with related schemes [11], [24], [26].

TABLE 4. A comparative summary: computation times.

Scheme	Based on	Computation cost (CC)	CC in DC	CC in RP
Li *et al.* [24]	V2V	T_S	24.835 ms	709.143 ms
Wang *et al.* [26]	V2V	$10T_h$	0.020 ms	1.740 ms
Vasudev *et al.* [11]	V2V, V2I	$6T_h + T_{SE} + T_{SD}$	7.774 ms	4487.577 ms
Ours	V2V	$17T_h$	0.034 ms	2.958 ms
Ours	V2I	$13T_h$	0.026 ms	2.262 ms

C. COMMUNICATION COSTS

We evaluated the communication costs of IoV-SMAP with related schemes [11], [24], [26]. According to [11], we assume that the bit-lengths of the timestamp (L_T), random number/identity (L_{ID}), symmetric encryption/decryption ($L_{SE/SD}$), asymmetric encryption/decryption ($L_{AE/AD}$), signature (L_S) and hash function (L_h) as 64 bits, 80 bits, 128 bits, 1024 bits, 1536 bits, and 256 bits, respectively. In V2V authentication process of our scheme, transmitted messages $\{M_1, M_2, M_{AE}, T_1\}$ and $\{M_3, M_{EA}, T_2\}$ require $(256 + 256 + 256 + 64) = 832$ bits and $(256 + 256 + 64) = 576$ bits, respectively. The V2I authentication process is omitted because it is the same as the V2V authentication process. Referring to Table 5, the total communication cost of IoV-SMAP is 1408 bits. Although IoV-SMAP has a higher communication cost than existing schemes [11] and it ensures better computation time and security than existing scheme [11], [24], [26].

TABLE 5. A comparative summary: communication costs.

Scheme	Based on	Communication cost	Total cost
Li *et al.* [24]	V2V	$L_T + 2L_{ID} + L_S$	1760 bits
Wang *et al.* [26]	V2V	$4L_h + 3L_T + 2L_{ID}$	1376 bits
Vasudev *et al.* [11]	V2V	$3L_h + 2L_T + L_{SE}$	1024 bits
Vasudev *et al.* [11]	V2I	$4L_h + 2L_T + L_{SE}$	1280 bits
Ours	V2V, V2I	$5L_h + 2L_T$	1408 bits

In V2V authentication process of our scheme, stored messages $\{Q_A, W_A, E_A\}$ and $\{Q_E, W_E, E_E\}$ require $(32+32+32) = 96$ bytes and $(32 + 32 + 32) = 96$ bytes, respectively. In V2I authentication process of our scheme, stored messages $\{Q_i, W_i, E_i\}$ and $\{C_i, N_{VS}\}$ require $(32+32+32) = 96$ bytes and $(32+10) = 42$ bytes, respectively. Although IoV-SMAP has the same storage overhead to Vasudev *et al.*'s scheme [11] and it provides better security and computation time than existing scheme [11], [24], [26].

TABLE 6. A comparative summary: storage overheads.

Scheme	Based on	Communication cost	Total cost
Li *et al.* [24]	V2V	$2L_T + 5L_{ID} + 2L_S$	450 bytes
Wang *et al.* [26]	V2V	$14L_h + 4L_{ID}$	488 bytes
Vasudev *et al.* [11]	V2V	$6L_h$	192 bytes
Vasudev *et al.* [11]	V2I	$4L_h + L_{ID}$	138 bytes
Ours	V2V	$6L_h$	192 bytes
Ours	V2I	$4L_h + L_{ID}$	138 bytes

D. STORAGE COSTS

We analyzed the storage costs of IoV-SMAP with existing schemes [11], [24], [26]. According to [11], we estimate that the bit-lengths of the timestamp (L_T), random number/identity (L_{ID}), symmetric encryption/decryption ($L_{SE/SD}$), asymmetric encryption/decryption ($L_{AE/AD}$), signature (L_S) and hash function (L_h) are 8 bytes, 10 bytes, 16 bytes, 128 bytes, 192 bytes, and 32 bytes, respectively.

VIII. CONCLUSION

We designed a "secure and efficient authentication scheme for IoV in smart city environment (IoV-SMAP)" to solve security threats of the existing authentication schemes. We showed that IoV-SMAP prevented various attacks, and ensured authentication and anonymity. We demonstrated the session key security of IoV-SMAP by performing formal security under the ROR model and also showed that IoV-SMAP was secure to MiTM and replay attacks by performing AVISPA simulation. We then compared the "security features", "computation costs", "communication costs" and "storage costs" of IoV-SMAP with related schemes. Consequently, IoV-SMAP significantly enhanced security and preserved the low computation cost and storage overhead utilizing only XOR and hash operations. Thus, IoV-SMAP is applicable for actual IoV environment because it is more secure and efficient than previous related schemes.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable suggestions and feedback on the paper.

REFERENCES

[1] *Save Lives—A Road Safety Technical Package*. Accessed: Jun. 16, 2020. [Online]. Available: http://apps.who.int/iris/bitstream/handle/10665/255199/9789241511704-eng.pdf

[2] *Road Traffic Injuries*. Accessed: Jun. 16, 2020. [Online]. Available: http://www.who.int/en/news-room/fact-sheets/detail/road-traffic-injuries

[3] Y. H. Park and Y. H. Park, "Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks," *Sensors*, vol. 16, no. 12, pp. 1–17, 2016.

[4] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey," *Veh. Commun.*, vol. 16, pp. 45–61, Apr. 2019.

[5] S. J. Yu, J. Y. Lee, K. K. Lee, K. S. Park, and Y. H. Park, "Secure authentication protocol for wireless sensor networks in vehicular communications," *Sensors*, vol. 18, no. 10, pp. 1–23, 2018.

[6] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and privacy in smart cities: Challenges and opportunities," *IEEE Access*, vol. 6, pp. 46134–46145, 2018.

[7] J. Y. Lee, S. J. Yu, K. S. Park, Y. H. Park, and Y. H. Park, "Secure three-factor authentication protocol for multi-gateway IoT environments," *Sensors*, vol. 19, no. 10, pp. 1–25, 2019.

[8] H. Chourabi, T. Nam, S. Walker, J. R. Gil-Garcia, S. Mellouli, K. Nahon, T. A. Pardo, and H. J. Scholl, "Understanding smart cities: An integrative framework," in *Proc. 45th Hawaii Int. Conf. Syst. Sci.*, Maui, HI, USA, Jan. 2012, pp. 1–9.

[9] 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.

[10] J. Wang, C. Jiang, Z. Han, Y. Ren, and L. Hanzo, "Internet of vehicles: Sensing-aided transportation information collection and diffusion," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 3813–3825, May 2018.

[11] H. Vasudev, D. Das, and A. V. Vasilakos, "Secure message propagation protocols for IoVs communication components," *Comput. Electr. Eng.*, vol. 82, pp. 1–15, Mar. 2020.

[12] 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.

[13] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Adv. Cryptol. (CRYPTO)*, Berlin, Germany, 1999, pp. 388–397.

[14] S. J. Yu, K. S. Park, and Y. H. Park, "A secure lightweight three-factor authentication scheme for IoT in cloud computing environment," *Sensors*, vol. 19, no. 16, pp. 1–20, 2019.

[15] Y. Park, S. Lee, C. Kim, and Y. Park, "Secure biometric-based authentication scheme with smart card revocation/reissue for wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 7, pp. 1–11, 2016.

[16] S. J. Yu, J. Y. Lee, Y. H. Park, Y. H. Park, S. W. Lee, and B. H. Chung, "A secure and efficient three-factor authentication protocol in global mobility networks," *Appl. Sci.*, vol. 10, no. 10, pp. 1–23, 2020.

[17] 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.

[18] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Proc. Int. Conf. Theory Appl. Cryptogr. Techn. (EUROCRYPT)*, Amsterdam, The Netherlands, 2002, pp. 337–351.

[19] M. Abdalla, P. A. Fouque, and D. Pointcheval, "Password-based authentication key exchange in the three-party setting," in *Proc. Public Key Cryptogr. (PKC)*, Les Diablerets, Switzerland, 2005, pp. 65–84.

[20] AVISPA. *Automated Validation of Internet Security Protocols and Applications*. Accessed: Jun. 16, 2020. [Online]. Available: http://www.avispa-project.org/

[21] *SPAN: A Security Protocol Animator for AVISPA*. Accessed: Jun. 16, 2020. [Online]. Available: http://www.avispa-project.org/

[22] N. Ruan, M. Li, and J. Li, "A novel broadcast authentication protocol for Internet of vehicles," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 6, pp. 1331–1343, Nov. 2017.

[23] L. Zhu, C. Zhang, C. Xu, X. Du, R. Xu, K. Sharif, and M. Guizani, "PRIF: A privacy-preserving interest-based forwarding scheme for social Internet of vehicles," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8804–8817, 2019.

[24] J. Li, H. Lu, and M. Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 938–948, Apr. 2015.

[25] 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.

[26] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, "2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET," *IEEE Trans. Veh. Technol.*, vol. 65, no. 2, pp. 896–911, Feb. 2016.

[27] R. Amin, P. Lohani, M. Ekka, S. Chourasia, and S. Vollala, "An enhanced anonymity resilience security protocol for vehicular ad-hoc network with Scyther simulation," *Comput. Electr. Eng.*, vol. 82, pp. 1–18, 2020.

[28] 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.

[29] B. Ying and A. Nayak, "Anonymous and lightweight authentication for secure vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10626–10636, Dec. 2017.

[30] C.-M. Chen, B. Xiang, Y. Liu, and K.-H. Wang, "A secure authentication protocol for Internet of vehicles," *IEEE Access*, vol. 7, pp. 12047–12057, 2019.

[31] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin, and X. Liu, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

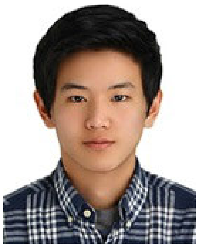
[32] W. E. May. (Apr. 1995). Secure Hash Standard. FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce. Accessed: Aug. 2019. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[33] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2776–2791, Nov. 2017.

[34] V. Boyko, P. Mackenzie, and S. Patel, "Provably secure password-authenticated key exchange using Diffie-Hellman," in *Proc. Int. Conf. Theory Appl. Crypto. Tech. Adv. Cryptol. (EUROCRYPT)*, Bruges, Belgium, 2000, pp. 156–171.

[35] D. V. Oheimb, "The high-level protocol specification Lanuage HLPSL developed in the EU project AVISPA," in *Proc. APPSEM Workshop*, Tallinn, Finland, 2005, pp. 1–17.

SUNGJIN YU received the B.S. degree in electronics engineering from Daegu University, in 2017, and the M.S. degree from Kyungpook National University, Daegu, South Korea, in 2019, where he is currently pursuing the Ph.D. degree in electronics engineering. His research interests include blockchain, VANET, information security, post-quantum cryptography, and authentication.



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

KISUNG PARK received the B.S. and M.S. degrees in electronics engineering from Kyungpook National University, Daegu, South Korea, in 2015 and 2017, respectively, where he is currently pursuing the Ph.D. degree with the School of Electronics Engineering. He is currently a Researcher with the Electronics and Telecommunications Research Institute (ETRI), Daejeon, South Korea. His research interests include blockchain, authentication, anonymous credentials, the Internet of Things, decentralized identifier, information security, post-quantum cryptography, and VANET.

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 is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. His current research interests include cryptography, wireless sensor network security, hierarchical access control, security in vehicular ad hoc networks, smart grid, the Internet of Things (IoT), cyber-physical systems (CPS) and cloud computing, and remote user authentication. He has authored over 235 papers in international journals and conferences in the above areas, including over 200 reputed journal articles. Some of his research findings are published in top cited journals, such as the IEEE Transactions on Information Forensics and Security, the IEEE Transactions on Dependable and Secure Computing, the IEEE Transactions on Smart Grid, the IEEE Internet of Things Journal, the IEEE Transactions on Industrial Informatics, the IEEE Transactions on Vehicular Technology, the IEEE Transactions on Consumer Electronics, the IEEE Journal of Biomedical and Health Informatics (formerly the IEEE Transactions on Information Technology in Biomedicine), *IEEE Consumer Electronics Magazine*, IEEE Access, *IEEE Communications Magazine*, *Future Generation Computer Systems*, *Computers and Electrical Engineering*, *Computer Methods and Programs in Biomedicine*, *Computer Standards and Interfaces*, *Computer Networks*, *Expert Systems with Applications*, and the *Journal of Network and Computer Applications*. He has served as a Program Committee Member in many international conferences. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He has served as one of the Technical Program Committee Chairs of the first International Congress on Blockchain and Applications (BLOCKCHAIN 2019), Avila, Spain, in June 2019, and the second International Congress on Blockchain and Applications (BLOCKCHAIN 2020), L'Aquila, Italy, in October 2020. He is on the Editorial Board of the IEEE Systems Journal, *Computer Communications* (Elsevier), *IET Communications*, the *KSII Transactions on Internet and Information Systems*, and the *International Journal of Internet Technology and Secured Transactions* (Inderscience). He is also a Guest Editor of the Special Issue on Big data and the IoT in E-Healthcare and for ICT Express (Elsevier) and the Special Issue on Blockchain Technologies and Applications for the 5G Enabled IoT of *Computers and Electrical Engineering* (Elsevier).

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 Electronics 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 Electronics Engineering, Kyungpook National University. His research interests include multimedia, computer networks, and information security.