IoVCom: Reliable Comprehensive Communication System for Internet of Vehicles

Trupil Limbasiya, *Student Member, IEEE* and Debasis Das, *Member, IEEE*

Abstract—By 2020, around 25 billion “things” will be connected to the Internet for a better society using different technological systems. Vehicle users have better experience by collaborating the Internet of Things (IoT) and vehicular ad-hoc network (VANET) architectures, and this emerging field is called the Internet of vehicles (IoV). Therefore, the IoV architecture will play an important role in the industry, research organization, and academics for various public and commercial applications. However, the IoV structure should ensure secure and efficient performance for vehicular communications, else an attacker may interfere in the system. In this paper, we propose protected comprehensive data dissemination protocols (say IoVCom) based on one-way hash function and elliptic curve cryptography (ECC) for the IoV structure. Next, we analyze security strengths of the IoVCom against various security attacks and discuss performance results in terms of communication overhead, computation time, storage cost, and energy consumption.

Index Terms—Attack, Authentication, Communication, Data, IoV.

1 Introduction

Mostly, people use road transportation for traveling and thus, a number of vehicles increases day-by-day. Hence, it is tough to provide different resources (e.g., road space, fuel, traffic management, etc.) efficiently to all vehicles. Presently, all systems are moving toward the development of smart city applications, and smart transportation is the most powerful pillar inside a smart city [1], [2]. Vehicular ad-hoc network (VANET) is designed to exchange vital information using dedicated short-range communication (DSRC) standard on the road [3] with two types of communications, as vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). It is used in safety and non-safety applications such as present location, traffic, road safety, and driver assistance/comfort [4], [5]. Hence, public key infrastructure methods (in Europe) and security credential management system (in the USA) are developed for VANET. However, VANET has some limitations for commercialization and future market opportunities, i.e., fixed storage, limited computational power, local data knowledge only, conditionally decision capability, short-range communication, non-collaborative, and bounded connectivity [6], [7].

The explosion of different smart devices, systems, and technologies has created an outstanding platform (known as the Internet of Things (IoT)) by connecting every “thing” to the Internet for better experience [8]. The IoT system collects data from different devices to perform a structured analysis and then, it shares the most relevant data with appropriate receivers to fulfill their needs. Hence, this concept has transformed mostly all industries into the IoT world.

V2X communications came into the picture to transfer messages between a vehicle and nearby devices using the DSRC-cellular hybrid architecture, and nodes (static and dynamic) are organized in flat and hierarchical structures. However, it is a challenging task to decide the node level (e.g., fixed/dynamic) in the hierarchical structure and data transmission type (e.g., data-centric/performance-centric) for the flat architecture. Besides, V2X communication has different limitations such as mobility management, preference to the network selection (e.g., DSRC/cellular), implementation cost, and stable clusters forming for a long time [9], [10]. Hence, it confines a global network to provide different services by involving intelligent systems (in a vehicle) and different cyber-physical systems (mobile device, vehicle, sensor, road-side-unit, etc.) for smart city users.

1.1 The IoV Architecture Overview

In the fast-growing world, we need a dominant structure to manage various devices and applications. Thus, the combined concept of VANET and IoT came into the picture as the Internet of Vehicles (IoV) [11]. This evolution is implemented based on the concept of device-to-device communication for the benefits of a society [12]. Hence, the IoV framework is a driving force with the capability to enrich the user experience, safety, human ability, and vehicle usage in the automotive society. It consists of modern vehicles, which are integrated with a two-way RF (radio frequency) equipment and is a combination of multiple technologies by having the potentiality for communication, environmental protection, safety, and energy conservation. The integration of inter-vehicle network, intra-vehicle network, and mobile network achieves multiple advantages. Some of them are as real-time vehicle monitoring and operation, alerts to the driver and relatives, remote control of the vehicle, optimization of routes and driving expenses, software update, safety systems, automatic emergency calls in case of an accident, real-time traffic data, entertainment for passengers, store location, and environmental conditions [13], [14].

- *T. Limbasiya is with the Department of Computer Science and Information Systems, Birla Institute of Technology & Science (BITS) Pilani, K. K. Birla Goa Campus, Goa-403726, India (email: limbasiyatrupil@gmail.com).*
- *D. Das is with the Department of Computer Science and Engineering, Indian Institute of Technology (IIT) Jodhpur, Rajasthan-342037, India (email: debasis@iitj.ac.in).*

Manuscript received Month XX, 20XX; revised Month XX, 20XX.

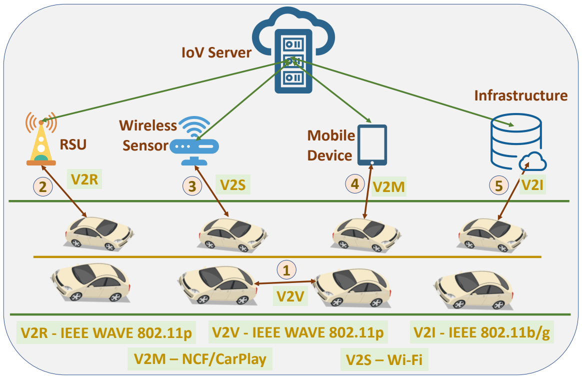


Figure 1: The generalized IoV communication architecture

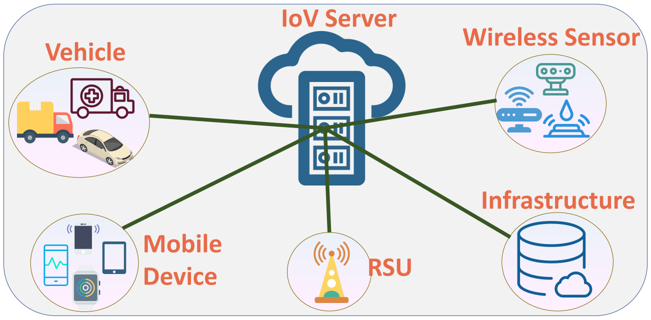


Figure 2: The registration connection with the IoV server

IoV applications can be broadly classified into two ways, (1) business oriented (2) safety-related. Business-oriented applications include car-sharing, insurance, infotainment, etc. Safety-related applications are navigation, remote telematics, diagnostic, traffic efficiency, co-operative message transfer, post-crash notification, enhancing traffic safety, co-operate to help other vehicles, real-time traffic, etc. One of the key features of the IoV is its different communications (see Figure 1), and it is systematized as V2V (vehicle-to-vehicle), V2R (vehicle-to-roadside unit), V2S (vehicle-to-wireless sensor), V2M (vehicle-to-mobile device), and V2I (vehicle-to-infrastructure). However, these communications are carried out using different wireless access technologies (WAT). In general, the WAT include Wi-Fi for V2S, Wi-Fi 802.11b/g for V2I, NCF/CarPlay for V2M, and IEEE WAVE 802.11p for V2V and V2R [7]. Therefore, it is necessary to implement all these different communication technologies in the IoV structure, and it increases the cost of the project [15]. Further, different IoV components (vehicle, mobile device, road-side-unit (RSU), wireless sensor, and infrastructure) are essential for various smart city applications as discussed recently. An RSU has limited memory space, and it is practiced in a city environment for short-range data transmissions. Generally, an infrastructure is placed in rural areas with long communication range and more storage capacity rather than an RSU. Multi-party data transmission comes into the picture to exchange information and to deal with different devices under one system collectively. Initially, IoV components should legally register with the IoV server once before exchanging relevant information with other components. Figure 2 shows the outline of a direct link between these devices and the IoV server. In general, the registration process happens through a secure infrastructure (e.g., SSL/TLS protocol) [16], [17], [28]. The IoV server is the central components in the IoV architecture.

The dream of intelligent transportation and autonomous car systems can be practiced using the IoV framework, but packets are sent over a public channel in vehicular communications and thus, an adversary has an opportunity to apply different attacks. Hence, it is vital to preserve fundamental security requirements, i.e., authentication, integrity, confidentiality, access control, non-repudiation, and availability [11], [18]. Moreover, the IoV framework mainly deals with the intelligent transportation systems, and if the communication system is not protected against varied threats, e.g., Sybil, modification, impersonation, illusion, replay, and collision induction, then it leads to critical problems in the security layer [19]. Therefore, the performance is degraded in the communication system, and it affects other smart systems because the IoV system is connected to different ubiquitous devices. Ultimately, secure data transmission is an essential component in public circumstances, and it is also a significant challenge in the IoV framework. The key agreement concept plays a vital role to identify the correctness of users and data for reliable communications over a public channel [20].

1.2 Related Works

In 2014, Wan et al. [21] firstly, proposed a three-layer IoV architecture using vehicle, location, and cloud, but limited communication facility is available in this system. Therefore, a new architecture [7] was designed with five layers, i.e., perception, business, artificial intelligence, coordination, and application, which is considered as an ideal architecture for IoV. Further, these layers are responsible for all five types of communications (V2V, V2I, V2R, V2S, and V2M). Researchers [7], [21] suggested the IoV layered structure, but they did not discuss possible security issues.

Researchers [17], [22], [23], [24] worked on privacy-preserving VANET communication systems. However, the security depends only on the private key of the trusted authority in all these schemes, and it may lead to some security flaws. Lyu et al. [25] proposed a lightweight V2V data verification system using private key cryptography and mentioned that it is resistant to a computation-based DoS (denial of service) attack and reduced the packet loss ratio. In [25], they shortened a re-keyed message authentication code (MAC) for signatures without compromising security, but they failed to deal with privacy issues, and its communication scope is limited to V2V. Vijayakumar et al. [26] suggested a dual authentication and key management method using the hash code and biometric identity to avoid malicious users to use the secret key for VANET applicants. The main limitation of the scheme [26] is that other vehicles or intruders can track the vehicles' location. Cui et al. [27] proposed a message authentication protocol to improve performance results in VANETs, but the execution cost is high and this scheme is vulnerable to impersonation, man-in-the-middle, illusion, modification, and plain-text attacks. Ultimately, most of these protocols need high execution time, communication overhead, and storage cost. Thus, these schemes consume more energy during the implementation.

Since the IoV is a combination of the IoT and VANET, we discuss possible security and performance problems of relevant authentication schemes. Liu et al. [28] came up with an efficient privacy-preserving authentication and key establishment technique using symmetric/asymmetric encryption, signature, exponential, and one-way hash for a V2V communication in the IoV paradigm. However, the performance of this scheme is not robust for storage, communication cost, and execution time due to high-cost operations. Hence, the scheme in [28] is weak in faster computation for IoV applications. Sun et al. [29] proposed a conditional privacy-preserving verification technique using a signature to increase system efficiency in VANETs, but this model needs high communication cost. E3PAKE (Extended Three Party Password-based Authenticated Key Exchange) [30] was proposed to deal with different concerns, i.e., high transmission/verification time, invalid service request, and verification failure. However, they [30] did not analyze different security attacks for communications.

Liu et al. [31] suggested a batch verification scheme for IoV to reduce the message verification time, but it takes a high amount time to check the correctness of messages at the receiver side because they used high-cost operations (bi-linear pairing and elliptic curve) in the message confirmation scheme. Besides, this protocol is vulnerable to man-in-the-middle, replay, and plain-text attacks. Hence, the scheme [31] is not trustworthy and competent for vehicle users to transmit messages over a common channel.

Wang et al. [32] proposed a data transmission scheme using different cryptographic functions (bi-linear pairing, elliptic curve, one-way hash, and exponential) to deal with authentication and privacy issues in VANETs. However, this communication method cannot withstand against modification, impersonation, and illusion attacks. Besides, the computational cost is very high due to the usage of bi-linear pairing and exponential operations. Moreover, the communication overhead and storage cost are also high for VANET applications. For all these reasons, the method [32] is not reliable for vehicular communications. Recently, Zhang et al. [33] designed an authentication method using a Chinese remainder theorem for VANETs to improve the performance results during the implementation. However, this scheme is vulnerable to man-in-the-middle and plain-text attacks. Further, the impact of Sybil and collision induction attacks is also high during data transmission. Besides, the computational cost is comparatively high. Therefore, the protocol [33] is not efficient for vehicular communications, and it does not preserve message confidentiality.

1.3 Motivations and Contributions

From the literature review, we understand that most of the schemes are vulnerable to various threats, e.g., modification, masquerade, camouflage, replay, key establishment, man-in-the-middle, etc. [19], [34], [35], [36]. To the best of our knowledge, no researchers have designed an exhaustive secure communication system to provide all five types of communication together for the IoV structure. Besides, smart transportation is an important pillar in smart city applications and therefore, it is necessary to implement all five types of IoV communications (refer Figure 1) securely and efficiently. Hence, the IoV communication system is a vital part of a knowledge city and is a unified network system to connect vehicle applicants, automotive and ubiquitous technological systems concurrently. Moreover, a huge amount of data is transferred between ubiquitous devices in the IoV architecture and accordingly, the communication system consumes high energy to execute essential operations. Motivated by these reasons, we find that there is a need to have secure and efficient data dissemination methods for IoV that can resist different security attacks and provide a better user experience. Keeping focused on these aspects, we propose novel comprehensive data transmission protocols with the following key features.

- Design a dependable system with five communications (V2S, V2V, V2I, V2M, and V2R) using one-way hash and elliptic curve operations to achieve mutual authentication between IoV entities (vehicle, RSU, mobile device, wireless sensor, and infrastructure).
- Resists various security attacks, e.g., Sybil, collision induction, modification, illusion, impersonation, replay, password guessing, man-in-the-middle, and plain-text.
- Attains better results in different performance measures such as execution time, energy consumption, storage cost, and communication overhead.

Hence, the proposed communication system can be mounted easily for the IoV architecture effectively. The central focus of the paper is to have a secure and effective communication from a vehicle to all IoV components around the world using advanced technology.

1.4 Organization of the Paper

The paper is structured as follows. Preliminaries are described in Section 2. We present a novel secure exhaustive communication schemes (IoVCom) in Section 3. Section 4 discusses performance results and security evaluations for the IoVCom. Conclusions and future works are given in Section 5.

2 PRELIMINARIES

In this section, we describe one-way hash function and elliptic curve cryptosystem, which are used in the design of the IoVCom. After that, we discuss different points on security and performance in the threat model.

2.1 One-way Hash

It is a cryptographic operation as $h : \{0,1\}^* \rightarrow \{0,1\}^k$ in which it takes an input of random size $x \epsilon \{0,1\}^k$ and then, it gives an output of the fixed size hash value as $h(x)$. Here, k is a block size. Further, it is computationally impracticable to obtain x from a given hash value $y = h(x)$ as one-way hash is an irreversible function.

2.2 Elliptic Curve Cryptosystem

An elliptic curve (EC) is defined as $E_p(a,b)$ over $y^2 = x^3 + ax + b$ mod p to generate point values. Here, a, b ϵF_p; p is a 256-bit large prime integer value; and P is a generator for $E_p(a,b)$ for an EC group G with an order of q. The EC scalar multiplication is defined as $n \cdot P = P + P + ... + P$, where $n \epsilon Z_q^*$. It is hard to compute n due to the elliptic curve discrete logarithm problem even though P is known [37].

2.3 Threat Model

Data is sent over a public channel during the communication phase in the IoV architecture and thus, we assume some considerations for security and performance aspects in the threat model as following [22], [33], [38].

- An adversary ($\mathcal{A}$) knows the communication protocol completely and s/he can compute different values if and only if $\mathcal{A}$ has all necessary credentials.
- Consider two authorized users, A and B. In this, if A can perform some illegal activities by having credentials (e.g., on-board-unit, public channel parameters) of B, then A is an adversary for B by playing two roles (legal user and attacker). However, $\mathcal{A}$ cannot extract data from a tamper-proof-device (*TPD*) [22], [25].
- A legitimate user can act an adversary to send multiple requests using different illegal identities to communicate with other IoV components. Here, the motivation of an attacker is to keep IoV devices busy so that on-time resources cannot be given to other authorized users.
- The session key is used to exchange information between two devices. This key is temporary, and it is calculated correctly if both (sender and receiver) agree on shared values, and they have all essential parameters.
- We consider an equation, $\mathbb{X} = \mathbb{Y} \oplus \mathbb{Z}$. Here, $\mathcal{A}$ can obtain $\mathbb{X}$ if and only if $\mathcal{A}$ knows $\mathbb{Z}$ and $\mathbb{Y}$. However, $\mathcal{A}$ cannot get $\mathbb{X}$ or $\mathbb{Y}$ or $\mathbb{Z}$ if s/he has only one value ($\mathbb{Y}$ or $\mathbb{Z}$ or $\mathbb{X}$).
- $\mathcal{A}$ can guess one credential at the same time. It means that $\mathcal{A}$ can proceed in the computation with only one parameter (e.g., user password, random nonce or relevant credential) as a guessable value. Next, it is not feasible to guess more than one parameter/nonce together correctly in polynomial time.
- In the IoV architecture, we have two kinds of a communication channel (public/insecure/open and private/secure). $\mathcal{A}$ cannot get any data from the private channel, but s/he can capture sent messages over an insecure medium. Hence, $\mathcal{A}$ can do re-transmission, deletion, interception, modification, and rerouting on data in a public environment [16], [17], [28].
- All cryptographic primitives (symmetric/asymmetric, one-way hash, elliptic curve, and bi-linear pairing) are secure, and $\mathcal{A}$ cannot break these algorithms.

3 The Proposed Protocol: IoVCom

We propose a reliable comprehensive data transmission system (named as IoVCom) with different five types of communications (V2V, V2R, V2S, V2M, and V2I) for IoV to exchange data with each other directly. The IoVCom provides all IoV communications as shown in Figure 1 and thus, it reliably connects to ubiquitous devices for any type of information through smart city applications. The proposed method consists of two phases as (1) registration and setup (2) data transmission. Generally, the registration and setup phase is carried out over a secure infrastructure (e.g. the transport layer security (TLS) protocol), and data transmission phase is performed through a public channel [16], [17], [28]. We use different notations in the paper, and they are described in Table 1.

Table 1: List of different symbols

Notations	Descriptions
V_a	Vehicle user a
M_b	Mobile user b
RSU_c	Road-side-unit c
S_d	Wireless Sensor d
I_e	Infrastructure e
S_{IoV}	IoV server
ID_X	Identity of X entity
PW_{V_a}/PW_{M_b}	Password for V_a/M_b
$p_i/q_i/r_i/s_i$	Random numbers
K_S	A key of S
TPD_X	Tamper-proof device for X entity
M_{XX}	Request message from X to X
$\mathcal{MXX}$	Response message for M_{XX}
$\mathcal{C}_{\mathcal{XY}}$	Communication count among X and Y
$\mathcal{A}$	An attacker/adversary
SC_{M_b}	Smart-chip for M_b
$\oplus$	Bit-wise XOR operation
$\|$	Concatenation operation
$h(\cdot)$	One-way hash function
Δt_x	A threshold delay fixed for time x
t_y	Current time-stamp generated at time y

X is considered as any type of user from $V_a/M_b/RSU_c/S_d/I_e$.

3.1 The IoVCom: Registration and Setup

This phase is practiced once to become a legitimate user and deploy necessary devices as all IoV communications are carried out between only authorized components. Therefore, this step is an essential part of the proposed IoV communication system at the first-time usage. In this operation, two registration techniques and three device setup procedures are performed by the IoV server (S_{IoV}) as shown in Figure 2. The server key (K_S) is randomly chosen of 128-bit by the IoV server, and the RSU secret key (SK_{RSU}) is computed as $h(s_i||K_S||\mathcal{T})$, where s_i is a random nonce and $\mathcal{T}$ is the current time-stamp. The RSU public key is calculated as $Pub_{RSU} = Pri_{RSU} \cdot P$, and it is the same for all RSUs. Pri_{RSU} is the RSU private key, and it remains the same for all RSUs. Further, the private and public keys (of the infrastructure) are Pri_{I_e} and $Pub_{I_e} = Pri_{I_e} \cdot P$ respectively. Here, Pri_{RSU} and Pri_{I_e} are 128-bit random nonce, and P is a generator on the elliptic curve of order q.

3.1.1 *Vehicle Registration*

If a vehicle user (V_a) wants to exchange vital information with other IoV components in the IoV system, then s/he should register his/her vehicle with S_{IoV} as follows. The proposed vehicle registration phase is shown in Figure 3.

1) V_a selects own ID_{V_a}, PW_{V_a}, p_i and does $P_{V_a} = h(ID_{V_a}||PW_{V_a})$, $Q_{V_a} = P_{V_a} \oplus p_i$. Then, V_a sends $\{ID_{V_a}, P_{V_a}, Q_{V_a}\}$ to S_{IoV}.
2) S_{IoV} computes $R_{V_a} = P_{V_a} \oplus Q_{V_a} \oplus ID_{V_a}$, $T_{V_a} = K_S \oplus R_{V_a} \oplus \mathcal{C}_{\mathcal{MV}}$, $U_{V_a} = \mathcal{C}_{\mathcal{VS}} \oplus R_{V_a} \oplus K_S$, $V_{V_a} = K_S \oplus R_{V_a} \oplus \mathcal{C}_{\mathcal{VI}}$, $Z_{V_a} = K_S \oplus R_{V_a} \oplus \mathcal{C}_{\mathcal{VV}}$, and $X_{V_a} = K_S \oplus Q_{V_a}$. S_{IoV} saves V_{V_a}, T_{V_a}, U_{V_a}, Z_{V_a}, $\mathcal{C}_{\mathcal{VV}}$, $\mathcal{C}_{\mathcal{VI}}$, $\mathcal{C}_{\mathcal{MV}}$, $\mathcal{C}_{\mathcal{VS}}$, SK_{RSU}, Pub_{RSU}, Pub_{I_e} in TPD_{V_a} and installs it into vehicle. Here, R_{V_a}, S_{V_a}, T_{V_a}, U_{V_a}, X_{V_a}, and Z_{V_a} are simply computed values. Besides, S_{IoV} stores $List_{ID_{V_a}}$, $List_{X_{V_a}}$, $List_{\mathcal{C}_{\mathcal{MV}}}$, $List_{\mathcal{C}_{\mathcal{VS}}}$, $List_{\mathcal{C}_{\mathcal{VI}}}$, and $List_{\mathcal{C}_{\mathcal{VV}}}$ in the database.
3) V_a computes $W_{V_a} = p_i \oplus h(PW_{V_a}||P_{V_a})$ and saves Q_{V_a}, W_{V_a} into TPD_{V_a}.

$\mathbf{V_a}$ **$\mathbf{S_{IoV}}$**

Vehicle Registration:

Selects ID_{V_a}, PW_{V_a}, and p_i
Computes...
$P_{V_a} = h(ID_{V_a}||PW_{V_a})$
$Q_{V_a} = P_{V_a} \oplus p_i$

$\xrightarrow{\{\text{ID}_{V_a}, P_{V_a}, Q_{V_a}\}}$

Computes...
$R_{V_a} = P_{V_a} \oplus Q_{V_a} \oplus ID_{V_a}$
$T_{V_a} = K_S \oplus R_{V_a} \oplus \mathcal{C}_{\mathcal{MV}}$
$U_{V_a} = K_S \oplus R_{V_a} \oplus \mathcal{C}_{\mathcal{VS}}$
$V_{V_a} = K_S \oplus R_{V_a} \oplus \mathcal{C}_{\mathcal{VI}}$
$Z_{V_a} = K_S \oplus R_{V_a} \oplus \mathcal{C}_{\mathcal{VV}}$
$X_{V_a} = K_S \oplus Q_{V_a}$
TPD_{V_a} consists...
$\{T_{V_a}, U_{V_a}, V_{V_a}, Z_{V_a}, \mathcal{C}_{\mathcal{VV}}, \mathcal{C}_{\mathcal{MV}}, \mathcal{C}_{\mathcal{VS}}, \mathcal{C}_{\mathcal{VI}}, Pub_{I_e}, SK_{RSU}, Pub_{RSU}\}$

$\xleftarrow{\{\text{TPD}_{V_a}\}}$

Calculates...
$W_{V_a} = p_i \oplus h(PW_{V_a}||P_{V_a})$
Saves Q_{V_a}, W_{V_a} in TPD_{V_a}

Figure 3: IoVCom: Vehicle Registration Phase

3.1.2 Mobile user Registration

A mobile user (M_b) can communicate with a vehicle user (V_a) using his/her portable device directly to get different statistics. To become a legitimate mobile user, M_b should perform following steps with S_{IoV}. A mobile user registration process is presented in Figure 4.

1) M_b chooses ID_{M_b}, PW_{M_b}, q_i and computes $P_{M_b} = h(ID_{M_b}||PW_{M_b})$, $Q_{M_b} = P_{M_b} \oplus q_i$. Now, M_b sends $\{ID_{M_b}, P_{M_b}, Q_{M_b}\}$ to S_{IoV}.
2) S_{IoV} does $R_{M_b} = P_{M_b} \oplus Q_{M_b} \oplus ID_{M_b}$, $T_{M_b} = K_S \oplus R_{M_b} \oplus \mathcal{C}_{\mathcal{MV}}$, $X_{M_b} = K_S \oplus Q_{M_b}$. Further, SC_{M_b} consists of T_{M_b}, $List_{ID_{V_a}}$, $List_{\mathcal{C}_{\mathcal{MV}}}$ and S_{IoV} installs this SC_{M_b} into a mobile of M_b. SC_{M_b} is a smart-chip memory. After that, M_b does $W_{M_b} = q_i \oplus h(PW_{M_b}||P_{M_b})$ and saves Q_{M_b}, W_{M_b} in the SC_{M_b}.

3.1.3 Road-side-unit Setup

A road-side-unit (RSU_c) can transfer data to V_a after the deployment by the the IoV server (S_{IoV}). Hence, RSU_c should perform the following steps. An RSU setup procedure is displayed in Figure 5.

1) RSU_c chooses ID_{RSU_c} and sends it to S_{IoV}.
2) S_{IoV} allows to become a legitimate RSU_c in case of ID_{RSU_c} is not matched with other RSU's identity. Further, S_{IoV} gets RSU keys (Pri_{RSU} and SK_{RSU}) from the database and stores Pri_{RSU} and SK_{RSU} into TPD_{RSU_c}. After that, S_{IoV} enrolls this RSU and deploys it on the road by installing TPD_{RSU_c} in it.

3.1.4 Wireless Sensor Setup

A wireless sensor (S_d) deployment is done by S_{IoV} as follows to provide important information to V_a on the road, and it is also represented in Figure 6.

$\mathbf{M_b}$ **$\mathbf{S_{IoV}}$**

Mobile User Registration:

Chooses ID_{M_b}, PW_{M_b}, q_i
Computes...
$P_{M_b} = h(ID_{M_b}||PW_{M_b})$
$Q_{M_b} = P_{M_b} \oplus q_i$

$\xrightarrow{\{\text{ID}_{M_b}, P_{M_b}, Q_{M_b}\}}$

$R_{M_b} = ID_{M_b} \oplus P_{M_b} \oplus Q_{M_b}$
$T_{M_b} = R_{M_b} \oplus K_S \oplus \mathcal{C}_{\mathcal{MV}}$
$X_{M_b} = K_S \oplus Q_{M_b}$
$SC_{M_b} = \{T_{M_b}, List_{ID_{V_a}}, List_{\mathcal{C}_{\mathcal{MV}}}\}$

$\xleftarrow{\{\text{SC}_{M_b}\}}$

Calculates...
$W_{M_b} = q_i \oplus h(PW_{M_b}||P_{M_b})$
SC_{M_b} consists...
$\{Q_{M_b}, W_{M_b}, T_{M_b}, List_{ID_{V_a}}, List_{\mathcal{C}_{\mathcal{MV}}}\}$

Figure 4: IoVCom: Mobile User Registration Phase

$\mathbf{RSU_c}$ **$\mathbf{S_{IoV}}$**

Road-side-unit Setup:

Selects ID_{RSU_c}

$\xrightarrow{\{\text{ID}_{RSU_c}\}}$

Checks availability of ID_{RSU_c}
Saves Pri_{RSU} and SK_{RSU} in TPD_{RSU_c}
Deployment of RSU_c with TPD_{RSU_c}

$\xleftarrow{\{\text{TPD}_{RSU_c}\}}$

Figure 5: IoVCom: Road-side-unit Setup

1) S_d selects ID_{S_d} and transfers to S_{IoV}.
2) S_{IoV} accepts ID_{S_d} if this identity is not available in the database. Next, S_{IoV} gets X_{V_a} from the database and computes $Y_{V_a} = X_{V_a} \oplus ID_{S_d}$. S_{IoV} stores $List_{ID_{V_a}}$, $List_{Y_{V_a}}$, $List_{\mathcal{C}_{\mathcal{VS}}}$ into TPD_{S_d} and puts it into S_d.

$\mathbf{S_d}$ **$\mathbf{S_{IoV}}$**

Wireless Sensor Setup:

Selects ID_{S_d}

$\xrightarrow{\{\text{ID}_{S_d}\}}$

Checks availability of ID_{S_d}
Computes...
$X_{V_a} = K_S \oplus Q_{V_a}$
$Y_{V_a} = X_{V_a} \oplus ID_{S_d}$
$TPD_{S_d} = \{List_{ID_{V_a}}, List_{Y_{V_a}}, List_{\mathcal{C}_{\mathcal{VS}}}\}$
Installation of S_d with TPD_{S_d}

$\xleftarrow{\{\text{TPD}_{S_d}\}}$

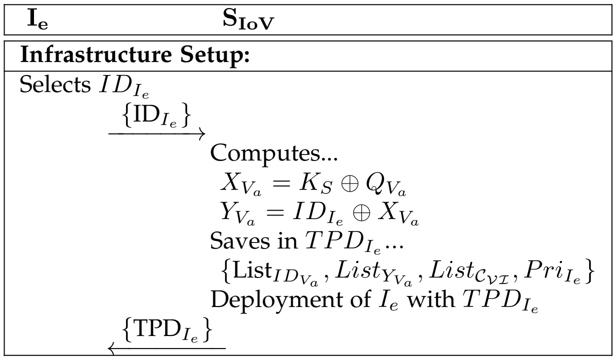
Figure 6: IoVCom: Wireless Sensor Setup

3.1.5 Infrastructure Setup

An infrastructure (I_e) should be registered with the *IoV* server (S_{IoV}) before delivering any information to V_a, and it should perform following necessary steps. The basic setup process for infrastructure is shown in Figure 7.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2019.2963191, IEEE Transactions on Dependable and Secure Computing

1) I_e selects ID_{I_e} and sends it to S_{IoV}.
2) S_{IoV} registers I_e if it has sent an unique identity (ID_{I_e}). After that, S_{IoV} retrieves X_{V_a} from the database and calculates $Y_{V_a} = X_{V_a} \oplus ID_{I_e}$.
3) S_{IoV} puts $List_{ID_{V_a}}, List_{Y_{V_a}}, List_{\mathcal{C}_{\mathcal{VI}}}$, Pri_{I_e} into TPD_{I_e} and initializes I_e by installing TPD_{I_e} in it.


$\mathbf{I_e}$ $\mathbf{S_{IoV}}$

Infrastructure Setup:

Selects ID_{I_e}

$\xrightarrow{\{\mathrm{ID}_{I_e}\}}$

Computes...

$X_{V_a} = K_S \oplus Q_{V_a}$

$Y_{V_a} = ID_{I_e} \oplus X_{V_a}$

Saves in TPD_{I_e}...

$\{\mathrm{List}_{ID_{V_a}}, List_{Y_{V_a}}, List_{\mathcal{C}_{\mathcal{VI}}}, Pri_{I_e}\}$

Deployment of I_e with TPD_{I_e}

$\xleftarrow{\{\mathrm{TPD}_{I_e}\}}$

Figure 7: IoVCom: Infrastructure Setup

3.2 The IoVCom: Data Transmission Schemes

After completing the registration and setup phases, IoV entities ($V_a/M_b/RSU_c/S_d/I_e$) can directly communicate with each other via a common channel to get better experience by using the IoV system (see Figure 1). The vehicular smart system (VSS) is available in each vehicle to calculate different values on behalf of V_a, and it includes an on-board-unit (*OBU*) and a *TPD*. Each IoV communication phase is described in-detail as follows.

3.2.1 *Vehicle-to-Vehicle*

V2V communication is practiced to transmit data between two vehicles as follows, and it is shown in Figure 8.

1) V_a puts ID'_{V_a} and PW'_{V_a} into VSS, and it calculates $P'_{V_a} = h(ID'_{V_a}||PW'_{V_a})$, $p'_i = Q_{V_a} \oplus P'_{V_a}$, $W'_{V_a} = h(PW'_{V_a}||P'_{V_a}) \oplus p'_i$. Further, it confirms V_a by $W'_{V_a} \overset{?}{=} W_{V_a}$. If true, then only it proceeds to the next step. In other cases, VSS ends the session directly.
2) VSS enumerates $R'_{V_a} = P'_{V_a} \oplus Q_{V_a} \oplus ID'_{V_a}$, $K_S = Z_{V_a} \oplus \mathcal{C}_{\mathcal{VV}} \oplus R'_{V_a}$, $M_1 = M_{VaVi} \oplus K_S \oplus \mathcal{C}_{\mathcal{VV}}$, $M_2 = M_1 \oplus t_1 \oplus ID_{V_i}$, $M_3 = h(M_{VaVi}||M_2||\mathcal{C}_{\mathcal{VV}})$ and transfers a request $\{ID'_{V_a}, M_2, M_3, t_1\}$ to V_i. Here, M_{VaVi} is a request message from V_a to V_i.
3) V_i puts ID'_{V_i} and PW'_{V_i} into VSS to calculate $P'_{V_i} = h(ID'_{V_i}||PW'_{V_i})$, $p'_i = Q_{V_i} \oplus P'_{V_i}$, $W'_{V_i} = p'_i \oplus h(PW'_{V_i}||P'_{V_i})$. Then, it confirms V_i by $W'_{V_i} \overset{?}{=} W_{V_i}$. If it is true, then only it proceeds to the next step. In other cases, VSS ends the session directly.
4) V_i calculates $t_2 - t_1 \leq \Delta t_1$. If correct, it proceeds for $M'_1 = M_2 \oplus t_1 \oplus ID'_{V_i}$, $M'_{VaVi} = M'_1 \oplus K_S \oplus \mathcal{C}_{\mathcal{VV}}$, and $M'_3 = h(M'_{VaVi}||M_2||\mathcal{C}_{\mathcal{VV}})$. If $M'_3 = M_3$, then V_i increases $\mathcal{C}_{\mathcal{VV}}$ by 1 and calculates $M_4 = M'_{VaVi} \oplus \Delta t_1 \oplus \mathcal{MVV} \oplus ID'_{V_a}$, $M_5 = h(\mathcal{MVV}||M'_{VaVi}||\Delta t_1||ID'_{V_a})$. Here, $\mathcal{MVV}$ is a response message for M_{VaVi}. Further, V_i replies as $\{M_4, M_5, t_2\}$ to V_a.
5) VSS confirms the validity by computing Δt_2 at V_a end. If valid, then it computes $\Delta t_1 = t_2 - t_1$, $\mathcal{MVV}' = M_4 \oplus \Delta t_1 \oplus M_{VaVi}$, $M'_5 = h(\mathcal{MVV}'||M_{VaVi}||\Delta t_1||ID'_{V_a})$. Now, it confirms the correctness of M'_5 in order to proceed further. If it holds, then VSS increases $\mathcal{C}_{\mathcal{VV}}$, accepts $\mathcal{MVV}'$. Next, VSS does $M_6 = h(\mathcal{MVV}'||M_{VaVi}||\mathcal{C}_{\mathcal{VV}}||\Delta t_2)$ and sends $\{M_6, t_3\}$ to V_i.
6) At V_i end, there are two possibilities.
(a) No $\{M_6, t_3\}$ from VSS or delay on $\{M_6, t_3\}$
(b) No interruption on $\{M_6, t_3\}$
For the first case, V_i reduces $\mathcal{C}_{\mathcal{VR}}$ by 1. In the second case, it confirms the expiry of $\{M_6, t_3\}$. If it is valid, then only V_i goes for $\Delta t_2 = t_3 - t_2$, $M'_6 = h(\mathcal{MVV}||M'_{VaVi}||\mathcal{C}_{\mathcal{VV}}||\Delta t_2)$ and checks $M'_6 \overset{?}{=} M_6$. If true, V_i considers that $\mathcal{MVV}$ was delivered to V_a correctly. Otherwise, V_i decreases $\mathcal{C}_{\mathcal{VV}}$ by 1.

3.2.2 *Vehicle-to-Mobile*

This communication phase is practiced to exchange information between a mobile user (M_b) and V_a. V2M communication is shown in Figure 9.

1) M_b inserts ID'_{M_b}, PW'_{M_b}; The mobile device system (MDS) calculates $P'_{M_b} = h(ID'_{M_b}||PW'_{M_b})$, $q'_i = Q_{M_b} \oplus P'_{M_b}$, $W'_{M_b} = q'_i \oplus h(PW'_{M_b}||P'_{M_b})$. If both ($W'_{M_b}$ and W_{M_b}) are equal, then it proceeds to the next step. Otherwise, MDS rejects M_b instantly.
2) MDS calculates $R'_{M_b} = P'_{M_b} \oplus Q_{M_b} \oplus ID'_{M_b}$, $K_S = T_{M_b} \oplus \mathcal{C}_{\mathcal{MV}} \oplus R'_{M_b}$, $M_1 = M_{MV} \oplus K_S \oplus ID_{V_a}$, $M_2 = M_1 \oplus t_1 \oplus \mathcal{C}_{\mathcal{MV}}$, $M_3 = h(M_{MV}||\mathcal{C}_{\mathcal{MV}}||M_2)$ and transfers a request $\{ID'_{M_b}, M_2, M_3, t_1\}$ to V_a. Here, M_{MV} is a message request from M_b to V_a.
3) This step is same as step-1 (of section 3.2.1).
4) VSS on behalf of V_a confirms the validity of $\{ID'_{M_b}, M_2, M_3, t_1\}$ through Δt_1. If true, VSS does $M'_1 = M_2 \oplus t_1 \oplus \mathcal{C}_{\mathcal{MV}}$, $M'_{MV} = M'_1 \oplus K_S \oplus ID_{V_a}$, $M'_3 = h(M'_{MV}||\mathcal{C}_{\mathcal{MV}}||M_2)$ and checks $M'_3 \overset{?}{=} M_3$. If it holds, then VSS increases $\mathcal{C}_{\mathcal{MV}}$ by 1 and computes $M_4 = M'_{MV} \oplus \Delta t_1 \oplus \mathcal{MVM}$, $M_5 = h(\mathcal{MVM}||M'_{MV}||\Delta t_1||ID'_{V_a})$, where $\mathcal{MVM}$ is a response for M_{MV}. VSS sends $\{M_4, M_5, t_2\}$ to MDS.
5) MDS checks the validity of $\{M_4, M_5, t_2\}$ through Δt_2. If valid, MDS does $\Delta t_1 = t_2 - t_1$, $\mathcal{MVM}' = M_4 \oplus \Delta t_1 \oplus M_{MV}$, $M'_5 = h(\mathcal{MVM}'||M_{MV}||\Delta t_1||ID'_{V_a})$ to confirm the exactness of M'_5.
6) If it holds, then it increases $\mathcal{C}_{\mathcal{VR}}$, accepts $\mathcal{MVM}'$, and calculates $M_6 = h(\mathcal{MVM}'||M_{MV}||\mathcal{C}_{\mathcal{MV}}||\Delta t_2)$. After that, MDS sends $\{M_6, t_3\}$ to VSS.
7) At V_a end, there are two possibilities.
(a) No $\{M_6, t_3\}$ from MDS or interval on $\{M_6, t_3\}$
(b) No interruption on $\{M_6, t_3\}$
In the first case, VSS reduces $\mathcal{C}_{\mathcal{MV}}$ by 1. For another case - (b), it checks the validity of $\{M_6, t_3\}$ by Δt_3 and if valid, then VSS does $\Delta t_2 = t_3 - t_2$, $M'_6 = h(\mathcal{MVM}||M'_{MV}||\mathcal{C}_{\mathcal{MV}}||\Delta t_2)$ and confirms $M'_6 \overset{?}{=} M_6$. If correct, VSS believes that $\mathcal{MVM}$ was delivered to M_b only. Otherwise, VSS decreases $\mathcal{C}_{\mathcal{MV}}$ by 1.

3.2.3 *Vehicle-to-RSU*

Generally, RSUs are located on the road, and vehicles always move on the road. Thus, a vehicle user should get vital information from an RSU when s/he comes within the

$\mathbf{V_a}$ **$\mathbf{V_i}$**

Vehicle-to-Vehicle (V2V)

Inserts ID'_{V_a} & PW'_{V_a}
Computes...
$P'_{V_a} = h(ID'_{V_a}||PW'_{V_a})$
$p'_i = Q_{V_a} \oplus P'_{V_a}$
$W'_{V_a} = p'_i \oplus h(PW'_{V_a}||P'_{V_a})$
Checks $W'_{V_a} \overset{?}{=} W_{V_a}$
$R'_{V_a} = P'_{V_a} \oplus Q_{V_a} \oplus ID'_{V_a}$
$K_S = Z_{V_a} \oplus \mathcal{C}_{\mathcal{VV}} \oplus R'_{V_a}$
$M_1 = M_{VaVi} \oplus K_S \oplus \mathcal{C}_{\mathcal{VV}}$
$M_2 = M_1 \oplus t_1 \oplus ID_{V_i}$
$M_3 = h(M_{VaVi}||M_2||\mathcal{C}_{\mathcal{VV}})$

$\xrightarrow{\{ID'_{V_a}, M_2, M_3, t_1\}}$

Inserts ID'_{V_i} & PW'_{V_i}
Computes & Checks $W'_{V_i} \overset{?}{=} W_{V_i}$
Checks $t_2 - t_1 \leq \Delta t_1$
Calculates...
$M'_1 = M_2 \oplus t_1 \oplus ID'_{V_i}$
$M'_{VaVi} = M'_1 \oplus K_S \oplus \mathcal{C}_{\mathcal{VV}}$
$M'_3 = h(M'_{VaVi}||M_2||\mathcal{C}_{\mathcal{VV}})$
Confirms $M'_3 \overset{?}{=} M_3$
Increases $\mathcal{C}_{\mathcal{VV}}$ & computes...
$M_4 = \mathcal{MVV} \oplus \Delta t_1 \oplus M'_{VaVi} \oplus ID'_{V_a}$
$M_5 = h(\mathcal{MVV}||M'_{VaVi}||\Delta t_1||ID'_{V_a})$

$\xleftarrow{\{M_4, M_5, t_2\}}$

Checks $t_3 - t_2 \leq \Delta t_2$
Calculates...
$\Delta t_1 = t_2 - t_1$
$\mathcal{MVV}' = M_4 \oplus \Delta t_1 \oplus M_{VaVi}$
$M'_5 = h(\mathcal{MVV}'||M_{VaVi}||\Delta t_1||ID'_{V_a})$
Verifies $M'_5 \overset{?}{=} M_5$
If wrong, discards $\mathcal{MVV}'$ & disconnects
else considers $\mathcal{MVV}'$ & increases $\mathcal{C}_{\mathcal{VV}}$
Calculates...
$M_6 = h(\mathcal{MVV}'||M_{VaVi}||\mathcal{C}_{\mathcal{VV}}||\Delta t_2)$

$\xrightarrow{\{M_6, t_3\}}$

① No $\{M_5, t_3\}$ in Δt_3, Reduces $\mathcal{C}_{\mathcal{VV}}$
② Checks $t_4 - t_3 \leq \Delta t_3$
Calculates...
$\Delta t_2 = t_3 - t_2$
$M'_6 = h(\mathcal{MVV}||M'_{VaVi}||\mathcal{C}_{\mathcal{VV}}||\Delta t_2)$
Confirms $M'_6 \overset{?}{=} M_6$
If correct, no change in $\mathcal{C}_{\mathcal{VV}}$
else, reduces $\mathcal{C}_{\mathcal{VV}}$

Figure 8: IoVCom: V2V Communication

$\mathbf{M_B}$ **$\mathbf{V_a}$**

Vehicle-to-Mobile (V2M)

Inserts ID'_{M_b} & PW'_{M_b}
Computes...
$P'_{M_b} = h(ID'_{M_b}||PW'_{M_b})$
$q'_i = Q_{M_b} \oplus P'_{M_b}$
$W'_{M_b} = q'_i \oplus h(PW'_{M_b}||P'_{M_b})$
Checks $W'_{M_b} \overset{?}{=} W_{M_b}$
$R'_{M_b} = P'_{M_b} \oplus Q_{M_b} \oplus ID'_{M_b}$
$K_S = T_{M_b} \oplus \mathcal{C}_{\mathcal{MV}} \oplus R'_{M_b}$
$M_1 = M_{MV} \oplus K_S \oplus ID_{V_a}$
$M_2 = M_1 \oplus t_1 \oplus \mathcal{C}_{\mathcal{MV}}$
$M_3 = h(M_{MV}||\mathcal{C}_{\mathcal{MV}}||M_2)$

$\xrightarrow{\{ID'_{M_b}, M_2, M_3, t_1\}}$

Inserts ID'_{V_a} & PW'_{V_a}
Computes P'_{V_a}, p'_i, & W'_{V_a}
Checks $W'_{V_a} \overset{?}{=} W_{V_a}$
Checks $t_2 - t_1 \leq \Delta t_1$
Calculates...
$M'_1 = t_1 \oplus M_2 \oplus \mathcal{C}_{\mathcal{MV}}$
$M'_{MV} = M'_1 \oplus K_S \oplus ID_{V_a}$
$M'_3 = h(M'_{MV}||\mathcal{C}_{\mathcal{MV}}||M_2)$
Confirms $M'_3 \overset{?}{=} M_3$
Increases $\mathcal{C}_{\mathcal{MV}}$ & enumerates...
$M_4 = \mathcal{MVM} \oplus \Delta t_1 \oplus M'_{MV}$
$M_5 = h(\mathcal{MVM}||M'_{MV}||\Delta t_1||ID'_{V_a})$

$\xleftarrow{\{M_4, M_5, t_2\}}$

Checks $t_3 - t_2 \leq \Delta t_2$
Calculates...
$\Delta t_1 = t_2 - t_1$
$\mathcal{MVM}' = M_4 \oplus \Delta t_1 \oplus M_{MV}$
$M'_5 = h(\mathcal{MVM}'||M_{MV}||\Delta t_1||ID_{V_a})$
Verifies $M'_5 \overset{?}{=} M_5$
If false, discards $\mathcal{MVM}'$ & disconnects
else considers $\mathcal{MVM}'$ & increases $\mathcal{C}_{\mathcal{MV}}$
Calculates...
$M_6 = h(\mathcal{MVM}'||M_{MV}||\mathcal{C}_{\mathcal{MV}}||\Delta t_2)$

$\xrightarrow{\{M_6, t_3\}}$

① No $\{M_5, t_3\}$ in Δt_3
Reduces $\mathcal{C}_{\mathcal{MV}}$
② Checks $t_4 - t_3 \leq \Delta t_3$
Calculates...
$\Delta t_2 = t_3 - t_2$
$M'_6 = h(\mathcal{MVM}||M'_{MV}||\mathcal{C}_{\mathcal{MV}}||\Delta t_2)$
Confirms $M'_6 \overset{?}{=} M_6$
If true, no change in $\mathcal{C}_{\mathcal{MV}}$
else, reduces $\mathcal{C}_{\mathcal{MV}}$

Figure 9: IoVCom: V2M Communication

communication range of an RSU. Therefore, an RSU sends meaningful messages to vehicles using DSRC standard regularly, but a vehicle user should verify the obtained messages (from nearby RSUs) to confirm integrity (of messages) and authorization (of an RSU sender). Hence, we propose a V2R communication protocol for vehicle users as follows. Figure 10 shows the proposed V2R communication.

1) RSU_c calculates $\alpha_i = h(ID_{RSU_c} \oplus h(Pri_{RSU}||t_1))$, $\beta_i = \alpha_i \oplus \mathcal{MRV} \oplus SK_{RSU}$, $\sigma_i = Pri_{RSU} \cdot (\alpha_i \oplus h(\mathcal{MRV}||t_1))$, and broadcasts $\{\alpha_i, \beta_i, \sigma_i, t_1\}$ to nearby vehicles on every 100-300 milliseconds using DSRC [3]. Here, Pri_{RSU} is the RSU private key, and it remains the same for all RSUs; $\mathcal{MRV}$ is roadside information; Pub_{RSU} is the RSU public key; SK_{RSU} is the secret key for RSUs, which is saved in TPD_{RSU_c} during the RSU setup.
2) This is same as step-1 (of section 3.2.1).
3) VSS (of a vehicle V_a) calculates $t_2 - t_1 \leq \Delta t_1$. If it is true, then VSS computes $\mathcal{MRV}' = \beta_i \oplus \alpha_i \oplus SK_{RSU}$ and $\sigma_i \cdot P = Pub_{RSU}(\alpha_i \oplus h(\mathcal{MRV}'||t_1))$, where SK_{RSU} and Pub_{RSU} are already available in TPD_{V_a}. Moreover, if $\sigma_i \cdot P$ holds, then only VSS considers $\mathcal{MRV}'$ as a legal message.

$\mathbf{V_a}$	$\mathbf{RSU_c}$
Vehicle-to-RSU (V2R)	
	Calculates... $\alpha_i = h(ID_{RSU_c} \oplus h(Pri_{RSU}\|\|t_1))$ $\beta_i = \alpha_i \oplus \mathcal{MRV} \oplus SK_{RSU}$ $\sigma_i = Pri_{RSU} \cdot (\alpha_i \oplus h(\mathcal{MRV}\|\|t_1))$
$\xleftarrow{\{\alpha_i, \beta_i, \sigma_i, t_1\}}$	
Checks $t_2 - t_1 \leq \Delta t_1$ Inserts ID'_{V_a} & PW'_{V_a} Computes... $P'_{V_a} = h(ID'_{V_a}\|\|PW'_{V_a})$ $p'_i = Q_{V_a} \oplus P'_{V_a}$ $W'_{V_a} = p'_i \oplus h(PW'_{V_a}\|\|P'_{V_a})$ Checks $W'_{V_a} \overset{?}{=} W_{V_a}$ $\mathcal{MRV}' = \beta_i \oplus \alpha_i \oplus SK_{RSU}$ $\sigma_i \cdot P = Pub_{RSU}(\alpha_i \oplus h(\mathcal{MRV}'\|\|t_1))$ Checks $\sigma_i \cdot P \overset{?}{=} True$ If wrong, discards $\mathcal{MRV}'$ If true, considers $\mathcal{MRV}'$	

Figure 10: IoVCom: V2R Communication

3.2.4 Vehicle-to-Wireless Sensor

If V_a is interested to obtain some data from a wireless sensor (S_d), then V_a should perform the following steps by sending a request message (M_{VS}) to S_d. After that, S_d sends a response message ($\mathcal{MSV}$) for MVS to V_a. V2S communication is shown in Figure 11.

1) This is same as step-1 (of section 3.2.1).
2) VSS calculates $R'_{V_a} = P'_{V_a} \oplus Q_{V_a} \oplus ID'_{V_a}$, $K_S = S_{V_a} \oplus \mathcal{C_{VS}} \oplus R'_{V_a}$, $M_1 = M_{VS} \oplus K_S \oplus Q_{V_a}$, $M_2 = K_S \oplus Q_{V_a} \oplus t_1 \oplus \mathcal{C_{VS}}$, $M_3 = h(M_{VS}||M_2||\mathcal{C_{VS}})$ and sends $\{ID'_{V_a}, M_1, M_3, t_1\}$ to S_d.
3) S_d performs $t_2 - t_1 \leq \Delta t_1$. If valid, S_d proceeds for $M'_{VS} = M_1 \oplus X_{V_a}$, $M'_2 = t_1 \oplus X_{V_a} \oplus \mathcal{C_{VS}}$, $M'_3 = h(M'_{VS}||M_2||\mathcal{C_{VS}})$. If $M'_3 = M_3$, then S_d increases $\mathcal{C_{VS}}$ by 1 and computes $M_4 = \Delta t_1 \oplus M'_{VS} \oplus \mathcal{MSV} \oplus X_{V_a}$, $M_5 = h(\mathcal{MSV}||M'_{VS}||X_{V_a}||ID'_{V_a})$. Now, S_d responses as $\{M_4, M_5, t_2\}$ to VSS.
4) VSS confirms the validity of $\{M_4, M_5, t_2\}$ by computing Δt_2. If it is valid, then VSS calculates $\Delta t_1 = t_2 - t_1$, $\mathcal{MSV}' = M_4 \oplus \Delta t_1 \oplus M_{VS} \oplus K_S \oplus Q_{V_a}$, $M'_5 = h(\mathcal{MSV}'||M_{VS}||(K_S \oplus Q_{V_a})||ID'_{V_a})$. After that, it confirms the correctness of M'_5 for further process.
5) If it holds, then it increases $\mathcal{C_{VS}}$ by 1, accepts $\mathcal{MSV}'$, and computes $M_6 = h(\mathcal{MSV}'||M_{VS}||\mathcal{C_{VS}}||\Delta t_2)$. Then, VSS sends $\{M_6, t_3\}$ to S_d.
6) At S_d end, there are two possibilities.
(a) No $\{M_6, t_3\}$ from VSS or interval on $\{M_6, t_3\}$
(b) No interruption on $\{M_6, t_3\}$
For case - (a), S_d reduces $\mathcal{C_{VS}}$ by 1. In the second case, it verifies the expiry of $\{M_6, t_3\}$. If it is within Δt_3, then S_d computes $\Delta t_2 = t_3 - t_2$, $M'_6 = h(\mathcal{MSV}||M'_{VS}||\mathcal{C_{VS}}||\Delta t_2)$ and checks $M'_5 \overset{?}{=} M_5$. If correct, S_d believes that $\mathcal{MSV}$ was delivered to VSS correctly. Otherwise, S_d decreases $\mathcal{C_{VS}}$ by 1.

3.2.5 Vehicle-to-Infrastructure

To obtain information from the infrastructure (I_e), VSS should perform following steps in the interest of V_a. We consider an EC as $y^2 = x^3 + ax + b$ mod p to generate the private and public keys as Pri_{I_e} (128-bit random nonce) and $Pub_{I_e} = Pri_{I_e} \cdot P$ respectively. V2I communication is shown in Figure 12.

$\mathbf{V_a}$	$\mathbf{S_d}$
Vehicle-to-Wireless Sensor (V2S)	
Inserts ID'_{V_a}&PW'_{V_a} Computes... $P'_{V_a} = h(ID'_{V_a}\|\|PW'_{V_a})$ $p'_i = Q_{V_a} \oplus P'_{V_a}$ $W'_{V_a} = p'_i \oplus h(PW'_{V_a}\|\|P'_{V_a})$ Checks $W'_{V_a} \overset{?}{=} W_{V_a}$ $R'_{V_a} = P'_{V_a} \oplus Q_{V_a} \oplus ID'_{V_a}$ $K_S = S_{V_a} \oplus \mathcal{C_{VS}} \oplus R'_{V_a}$ $M_1 = M_{VS} \oplus K_S \oplus Q_{V_a}$ $M_2 = K_S \oplus Q_{V_a} \oplus t_1 \oplus \mathcal{C_{VS}}$ $M_3 = h(M_{VS}\|\|M_2\|\|\mathcal{C_{VS}})$	
$\xrightarrow{\{ID'_{V_a}, M_1, M_3, t_1\}}$	
	Checks $t_2 - t_1 \leq \Delta t_1$ Calculates... $M'_{VS} = M_1 \oplus X_{V_a}$ $M'_2 = t_1 \oplus X_{V_a} \oplus \mathcal{C_{VS}}$ $M'_3 = h(M'_{VS}\|\|M_2\|\|\mathcal{C_{VS}})$ Confirms $M'_3 \overset{?}{=} M_3$ Increases $\mathcal{C_{VS}}$ & enumerates... $M_4 = \mathcal{MSV} \oplus \Delta t_1 \oplus M'_{VS} \oplus X_{V_a}$ $M_5 = h(\mathcal{MSV}\|\|M'_{VS}\|\|X_{V_a}\|\|ID'_{V_a})$
$\xleftarrow{\{M_4, M_5, t_2\}}$	
Checks $t_3 - t_2 \leq \Delta t_2$ Calculates... $\Delta t_1 = t_2 - t_1$ $\mathcal{MSV}' = M_4 \oplus \Delta t_1 \oplus M_{VS} \oplus K_S \oplus Q_{V_a}$ $M'_5 = h(\mathcal{MSV}'\|\|M_{VS}\|\|(K_S \oplus Q_{V_a})\|\|ID'_{V_a})$ Verifies $M'_5 \overset{?}{=} M_5$ If false, discards $\mathcal{MSV}'$ & disconnects else considers $\mathcal{MSV}'$ & increases $\mathcal{C_{VS}}$ Calculates... $M_6 = h(\mathcal{MSV}'\|\|M_{VS}\|\|\mathcal{C_{VS}}\|\|\Delta t_2)$	
$\xrightarrow{\{M_6, t_3\}}$	
	① No $\{M_5, t_3\}$ in Δt_3 Reduces $\mathcal{C_{VS}}$ ② Checks $t_4 - t_3 \leq \Delta t_3$ Calculates... $\Delta t_2 = t_3 - t_2$ $M'_6 = h(\mathcal{MSV}\|\|M'_{VS}\|\|\mathcal{C_{VS}}\|\|\Delta t_2)$ Confirms $M'_6 \overset{?}{=} M_6$ If true, no change in $\mathcal{C_{VS}}$ else, reduces $\mathcal{C_{VS}}$

Figure 11: IoVCom: V2S Communication

1) This is same as step-1 (of section 3.2.1).
2) VSS does $R'_{V_a} = P'_{V_a} \oplus Q_{V_a} \oplus ID'_{V_a}$, $K_S = S_{V_a} \oplus \mathcal{C_{VI}} \oplus R'_{V_a}$, $M_1 = r_i \cdot P$, $\overline{M_{VI}} = (M_{VI}||ID'_{V_a}) \oplus t_1$, $M_2 = \overline{M_{VI}} + r_i \cdot Pub_{I_e}$, $M_3 = h(Q_{V_a} \oplus \mathcal{C_{VI}} \oplus K_S \oplus \overline{M_{VI}})$, where r_i is a random nonce and M_{VI} is a request message by V_a. After that, VSS sends $\{M_1, M_2, M_3, t_1\}$ to I_e.
3) I_e calculates $t_2 - t_1 \leq \Delta t_1$. If true, I_e proceeds for $\overline{M_{VI}} = M_2 - Pri_{I_e} \cdot M_1$, $M_{VI}||ID'_{V_a} = t_1 \oplus \overline{M_{VI}}$, $M'_3 = h(X_{V_a} \oplus M_{VI} \oplus \mathcal{C_{VI}})$. The infrastructure receives

a large number of query messages from vehicle users to provide vital information and thus, it is difficult to verify each query message separately. Therefore, the infrastructure performs this step using batch verification concept to check more than one message quickly at the same time, and it is as follows. Here, i is a query message number from a vehicle.

$$\sum_{i=1}^{n} \overline{M_{VI_i}} = \sum_{i=1}^{n} M_{2_i} - Pri_{I_e} \cdot \sum_{i=1}^{n} M_{1_i}$$

4) Now, I_e checks $M_3' \stackrel{?}{=} M_3$. If correct, then I_e increases $\mathcal{C_{VI}}$ by 1 and computes $M_4 = M_{VI}' \oplus \Delta t_1 \oplus \mathcal{MIV} \oplus X_{V_a}$, $M_5 = h(\mathcal{MIV}||M_{VI}||X_{V_a}||ID_{V_a}')$, where $\mathcal{MIV}$ is a response message for M_{VI_i}. After that, I_e replies as $\{M_4, M_5, t_2\}$ to VSS.
5) VSS confirms the validity of $\{M_4, M_5, t_2\}$ through Δt_2. If valid, then VSS calculates $\Delta t_1 = t_2 - t_1$, $\mathcal{MIV}' = M_4 \oplus \Delta t_1 \oplus M_{VI} \oplus K_S \oplus Q_{V_a}$, $M_5' = h(\mathcal{MIV}'||M_{VI}||(K_S \oplus Q_{V_a})||ID_{V_a})$. After that, it confirms the correctness of M_5' to proceed further.
6) If holds, VSS increases $\mathcal{C_{VI}}$, accepts $\mathcal{MIV}'$, does $M_6 = h(\mathcal{MIV}'||M_{VI}||\mathcal{C_{VI}}||\Delta t_2)$, and sends $\{M_6, t_3\}$ to I_e.
7) At I_e end, there are two possibilities.
(a) No $\{M_6, t_3\}$ from VSS or delay on $\{M_6, t_3\}$
(b) No interruption on $\{M_6, t_3\}$
For (a), I_e decreases $\mathcal{C_{VI}}$ by 1. In case - (b), I_e receives $\{M_6, t_3\}$ then, it confirms validity of $\{M_6, t_3\}$. If valid, then only I_e computes Δt_2, $M_6' = h(\mathcal{MIV}||M_{VI}'||\mathcal{C_{VI}}||\Delta t_2)$ and checks $M_5' \stackrel{?}{=} M_5$. If it is correct, I_e believes that $\mathcal{MIV}$ was delivered to VSS successfully. Otherwise, I_e decreases $\mathcal{C_{VI}}$ by 1.

4 Analysis of the Proposed Scheme

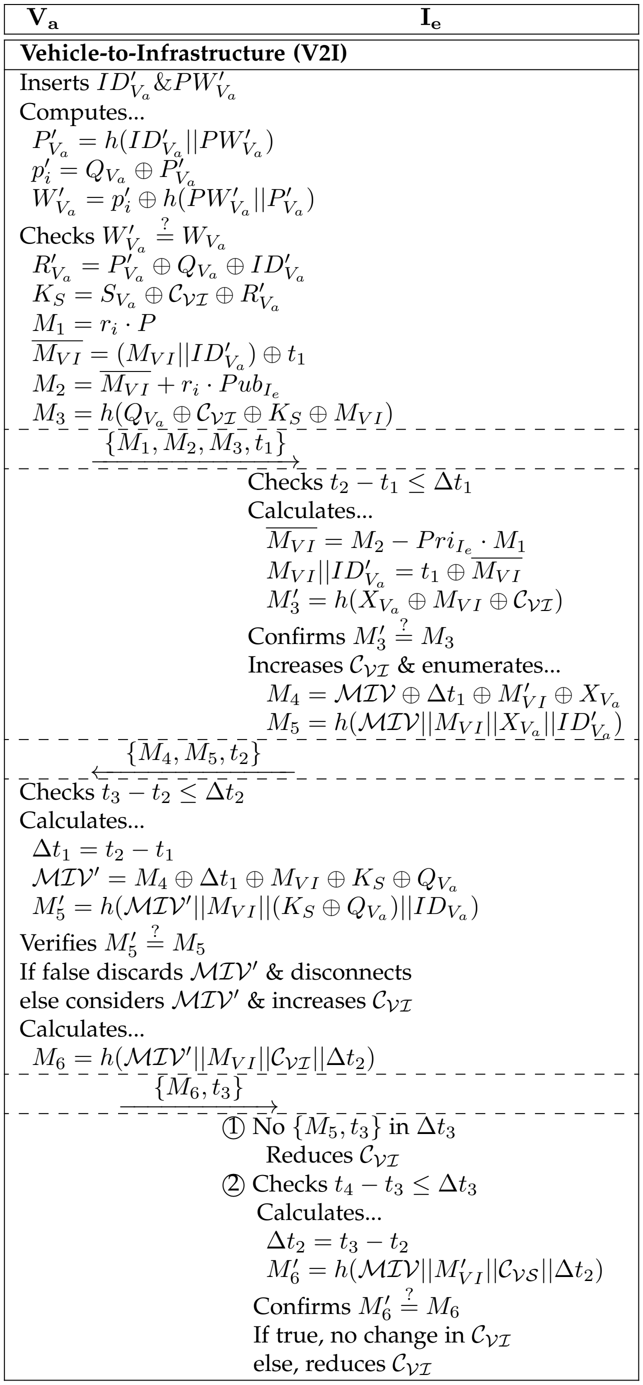
We analyze various communications (V2V, V2M, V2S, V2R, and V2I) of the proposed system in terms of security and performance in this section. Hence, it confirms the security strengths and performance efficiency of the IoVCom for smart transportation communications.

4.1 Security Proof and Analysis

Generally, an adversary may attempt to apply different attacks to gain information or access the IoV system illegally and thus, it is essential to check security strengths of the IoV communication system. Hence, we explain how the suggested schemes resist various attacks to understand security robustness based on the threat model (refer Section 2.3). Firstly, we discuss the security proof based on the random oracle model for the IoVCom and after that, we describe different security attributes.

Definition: An attacker ($\mathfrak{A}_{\mathfrak{A}}$) knows transmitted messages over a public communication channel and thus, s/he can play with this data (of sent messages). Here, $\mathfrak{A}_{\mathfrak{A}}$ acts as a non-registered person of the system.

Theorem: The suggested protocol can withstand against $\mathfrak{A}_{\mathfrak{A}}$'s adaptive malicious activities based on a one-way hash function in the random oracle model.



V_a **I_e**

Vehicle-to-Infrastructure (V2I)

Inserts $ID_{V_a}' \& PW_{V_a}'$
Computes...
$P_{V_a}' = h(ID_{V_a}'||PW_{V_a}')$
$p_i' = Q_{V_a} \oplus P_{V_a}'$
$W_{V_a}' = p_i' \oplus h(PW_{V_a}'||P_{V_a}')$
Checks $W_{V_a}' \stackrel{?}{=} W_{V_a}$
$R_{V_a}' = P_{V_a}' \oplus Q_{V_a} \oplus ID_{V_a}'$
$K_S = S_{V_a} \oplus \mathcal{C_{VI}} \oplus R_{V_a}'$
$M_1 = r_i \cdot P$
$\overline{M_{VI}} = (M_{VI}||ID_{V_a}') \oplus t_1$
$M_2 = \overline{M_{VI}} + r_i \cdot Pub_{I_e}$
$M_3 = h(Q_{V_a} \oplus \mathcal{C_{VI}} \oplus K_S \oplus M_{VI})$

$\xrightarrow{\{M_1, M_2, M_3, t_1\}}$

Checks $t_2 - t_1 \leq \Delta t_1$
Calculates...
$\overline{M_{VI}} = M_2 - Pri_{I_e} \cdot M_1$
$M_{VI}||ID_{V_a}' = t_1 \oplus \overline{M_{VI}}$
$M_3' = h(X_{V_a} \oplus M_{VI} \oplus \mathcal{C_{VI}})$
Confirms $M_3' \stackrel{?}{=} M_3$
Increases $\mathcal{C_{VI}}$ & enumerates...
$M_4 = \mathcal{MIV} \oplus \Delta t_1 \oplus M_{VI}' \oplus X_{V_a}$
$M_5 = h(\mathcal{MIV}||M_{VI}||X_{V_a}||ID_{V_a}')$

$\xleftarrow{\{M_4, M_5, t_2\}}$

Checks $t_3 - t_2 \leq \Delta t_2$
Calculates...
$\Delta t_1 = t_2 - t_1$
$\mathcal{MIV}' = M_4 \oplus \Delta t_1 \oplus M_{VI} \oplus K_S \oplus Q_{V_a}$
$M_5' = h(\mathcal{MIV}'||M_{VI}||(K_S \oplus Q_{V_a})||ID_{V_a})$
Verifies $M_5' \stackrel{?}{=} M_5$
If false discards $\mathcal{MIV}'$ & disconnects
else considers $\mathcal{MIV}'$ & increases $\mathcal{C_{VI}}$
Calculates...
$M_6 = h(\mathcal{MIV}'||M_{VI}||\mathcal{C_{VI}}||\Delta t_2)$

$\xrightarrow{\{M_6, t_3\}}$

① No $\{M_5, t_3\}$ in Δt_3
Reduces $\mathcal{C_{VI}}$
② Checks $t_4 - t_3 \leq \Delta t_3$
Calculates...
$\Delta t_2 = t_3 - t_2$
$M_6' = h(\mathcal{MIV}||M_{VI}'||\mathcal{C_{VS}}||\Delta t_2)$
Confirms $M_6' \stackrel{?}{=} M_6$
If true, no change in $\mathcal{C_{VI}}$
else, reduces $\mathcal{C_{VI}}$

Figure 12: IoVCom: V2I Communication

Proof: As per the *Definition*, $\mathfrak{A}_{\mathfrak{A}}$ knows ID_{V_a}', ID_{M_b}', M_1, M_2, M_3, M_4, M_5, M_6, t_1, t_2, t_3 and accordingly, s/he attempts to perform different malicious activities. For this, an adversary needs to compute all necessary values to proceed further. Hence, s/he should know M_{VaVi}, $\mathcal{C_{VV}}$, K_S, M_{MV}, $\mathcal{C_{MV}}$, Pri_{RSU}, $\mathcal{C_{VR}}$, M_{VS}, and $\mathcal{C_{VS}}$, but $\mathfrak{A}_{\mathfrak{A}}$ is unable to get these parameters anyhow. Thus, $\mathfrak{A}_{\mathfrak{A}}$ fails to carry out any type of illegal activities in the IoVCom.

Next, we illustrate strengths of the proposed mechanism against various security attacks as follows.

1) ***Modification:*** If an attacker ($\mathcal{A}$) wants to change data illegally in the proposed method, then s/he should

calculate M_2/M_1 and M_3 correctly. Hence, $\mathcal{A}$ should know $\mathcal{C}_{\mathcal{MV}}$, $\mathcal{C}_{\mathcal{VV}}$, $\mathcal{C}_{\mathcal{VR}}$, $\mathcal{C}_{\mathcal{VS}}$, $\mathcal{C}_{\mathcal{VI}}$, K_S, but $\mathcal{A}$ has no knowledge on these values because $\mathcal{C}_{\mathcal{MV}}$, $\mathcal{C}_{\mathcal{VV}}$, $\mathcal{C}_{\mathcal{VR}}$, $\mathcal{C}_{\mathcal{VS}}$, $\mathcal{C}_{\mathcal{VI}}$ are stored in a *TPD* (installed into a vehicle) of V_a, and $\mathcal{A}$ cannot reveal any value from a *TPD*. The IoV server only knows K_S. If $\mathcal{A}$ wants to get K_S, then s/he should know Z_{V_a}, R_{V_a}, Q_{V_a}, $\mathcal{C}_{\mathcal{VV}}$, but $\mathcal{A}$ does not know PW_{V_a}, p_i and these confidential credentials are not saved anywhere. Moreover, it is generally not feasible to guess two values at the same time in polynomial time. Hence, $\mathcal{A}$ fails to calculate M_2/M_1 and M_3.

During V_i to V_{V_a} response message (M_4, M_5, T_2), $\mathcal{A}$ requires M_{XX}, $\mathcal{MXX}$, and X_{V_a} to compute M_4 and M_5. Here, M_{XX} dictates a message from X (vehicle) to X (other IoV component: vehicle, wireless sensor, infrastructure, mobile device, and RSU) IoV component and $\mathcal{MXX}$ denotes a message from $\mathcal{X}$ (vehicle) to $\mathcal{X}$ (other IoV component: vehicle/wireless sensor/infrastructure/mobile device/RSU). M_{XX} is known to V_a and the original receiver. Further, $\mathcal{MXX}$ is only known to the original receiver of $ID'_{V_a}, M_1/M_2, M_3, t_1$ at this stage. Therefore, $\mathcal{A}$ cannot proceed for further computation without having all essential values. Similarly, $\mathcal{A}$ does not know M_{XX} and $\mathcal{CXX}$ for calculating M_6. Ultimately, $\mathcal{A}$ cannot change M_{XX} or $\mathcal{MXX}$. For all these reasons, a modification attack is not feasible in the proposed system.

2) ***Plain-text:*** If $\mathcal{A}$ can understand a replied message, then a plain-text attack is applicable in the system. Generally, an adversary has two ways to perform this attack as (1) $\mathcal{A}$ can know relevant information if a sender sends it in a simple form and (2) $\mathcal{A}$ can compute and derive this information after having public channel parameters.

In the first case as per the IoVCom, $\mathcal{A}$ cannot get any information from an insecure communication channel directly because V_a, M_b, RSU_C, S_d, and I_e do not send M_{XX} or $\mathcal{MXX}$ publicly. $V_a/M_b/RSU_C/S_d/I_e$ transmits ID'_{V_a}, M_1/M_2, M_3, M_4, M_5, M_6, α_i, β_i, σ_i, t_1, t_2, t_3 over a common channel to start a communication temporary, and all these values $(M_1/M_2, M_3, M_4, M_5, M_6$, α_i, β_i, and $\sigma_i)$ are computed using a one-way hash operation. Thus, $\mathcal{A}$ is unable to get any information from these parameters. Besides, t_1, t_2, t_3 are current time-stamps, and they are invalid after $\Delta t_1/\Delta t_2/\Delta t_3$ (Latency is discussed in Section 4.2.1.) [39].

In the second case, $\mathcal{A}$ knows ID'_{V_a}, α_i, β_i, σ_i, M_1/M_2, M_3, M_4, M_5, M_6, t_1, t_2, t_3 and thus, s/he may try to extract some information using these values. We consider that $\mathcal{A}$ wants to know two messages (request:M_{XX} and response:$\mathcal{MXX}$). To get M_{XX}, $\mathcal{A}$ should have M_1, K_S, and $\mathcal{CXX}$, but $\mathcal{A}$ knows none of these credentials accurately (refer Section 4.1.1 - modification attack). Without knowing required variables, it is very hard to obtain M_{XX} correctly. Next, $\mathcal{A}$ wants to get $\mathcal{MXX}$ and s/he does not know M_{XX} according to previous explanation. Therefore, $\mathcal{A}$ should have $M_4, \Delta t_1$, and M_{XX} to decipher $\mathcal{MXX}$. We assume that Δt_1 and M_4 are available to $\mathcal{A}$ after listening $\{ID'_{V_a}/ID'_{M_b}, M_2, M_3, t_1\}$ and $\{M_4, M_5, t_2\}$. However, M_{XX} is unknown to $\mathcal{A}$ because $\mathcal{A}$ does not have essential values (M_{XX}, K_S, and Q_{V_a}). Besides, α_i, β_i, and σ_i are computed using Pri_{RSU}, SK_{RSU}, t_1, and ID_{RSU}. Hence, it is hard to intercept $\mathcal{MRV}$. Consequentially, it is difficult to get $\mathcal{MXX}$ correctly without having K_S, M_{XX}, and Q_{V_a} at the same time. Besides, it is sometimes extremely difficult to compute Δt_1 correctly. Thus, the IoVCom can withstand against a plain-text attack.

3) ***Replay:*** To delay or stop any request/response, $\mathcal{A}$ applies a replay attack. At the same time, $\mathcal{A}$ can become a successful person in this attack if the receiver accepts a late request (sent by an adversary). According to the IoVCom, $V_i/V_a/RSU_c/S_d/I_e/M_b$ firstly checks the validity of a received request from the sender. If it is not beyond $\Delta t_1/\Delta t_2/\Delta t_3$, then only $V_i/S_d/I_e/V_a/RSU_c/M_b$ proceeds for further steps. Here, $\Delta t_1, \Delta t_2$, and Δt_3 are the maximum delay at the receiving side, and they are fixed in the transmission channel (Latency is described in Section 4.2.1.) [39]. Next, $\Delta t_1, \Delta t_2$, and Δt_3 are also used in M_2, M_4, M_5, M_6 computation (using one-way hash) directly before transmitting request/response messages. Here, one-way hash is an irreversible operation of 256-bit. Hence, none can derive any data from the hashed value. Next, $\mathcal{A}$ cannot change t_1, t_2 or t_3 in $M_2/M_4/M_5/M_6$ because $V_a/RSU_c/V_i/S_d/I_e/M_b$ verifies the exactness of all received parameters (M_3, M_5, M_6) over a public channel. In this way, an adversary cannot perform a replay attack in the suggested schemes.

4) ***Password Guessing:*** If $\mathcal{A}$ can get the correct password (PW_i) using a guessed password $(\overline{PW_{V_a}})$ by having public variables, then this attack is feasible in the system. To know PW_i, $\mathcal{A}$ should calculate Q_{V_a}, and it is computed as $p_i \oplus P_{V_a}$. Here, $P_{V_a} = h(ID_{V_a}||PW_{V_a})$ and p_i is 128-bit random nonce chosen by V_a during the registration phase. We consider that $\mathcal{A}$ calculates $\overline{P_{V_a}}$ as $h(ID_{V_a}||\overline{PW_{V_a}})$, but s/he does not know p_i exactly. Here, p_i is known to only V_a, and there is also a possibility that V_a might not remember p_i after the registration phase. According to the IoVCom, V_a does not need to remember p_i. By considering the threat model, $\mathcal{A}$ cannot guess two different variables polynomially. Hence, $\mathcal{A}$ cannot proceed further in the computation. Moreover, $\mathcal{A}$ does not know other vital credentials $(\mathcal{MXX}, K_S, Q_{V_a}, X_{V_a})$ and thus, s/he is unable to obtain necessary parameters through M_2, M_4, M_5, M_6. Thus, $\mathcal{A}$ fails to check the correctness of $\overline{PW_{V_a}}$. Consequently, it is also difficult to get correct values of these credentials within stipulated time. Thus, the IoVCom is secure against a password guessing attack.

5) ***Impersonation:*** If $\mathcal{A}$ wants to access privileged services on behalf of other users, then he or she should generate a valid login/message request. If $\mathcal{A}$ succeeds in this process, then a user impersonation attack is possible. By considering the proposed protocols, $\mathcal{A}$ should compute M_1/M_2 and M_3 correctly to send a valid request to the reviver. Further, $\mathcal{A}$ should calculate all required values (M_4, M_5, t_2) to get a response message from the receiver and clear $M'_6 \overset{?}{=} M_6$ test by the receiver.

To calculate these values, $\mathcal{A}$ should know K_S, ID_{V_i}/ID_{V_a} (an identity of the receiver/sender), C_{XX}, Q_{V_a}, X_{V_a}. However, $\mathcal{A}$ has no knowledge about these parameters as discussed earlier in the security analysis section. Thus, he/she cannot proceed for a fake message creation. If $\mathcal{A}$ thinks to re-use $\{ID'_{V_a}, M_1, M_3, t_1\}$, then s/he fails to impersonate a legitimate user because this request includes time-stamp (t_1), and it is valid for a limited period in the IoVCom. Similarly, $\mathcal{A}$ cannot generate $\{M_4, M_5, t_2\}$ or $\{M_6, t_3\}$ because $\mathcal{A}$ does not know/compute $\mathcal{MXX}, M_{XX}, \mathcal{C}_{XX}$ by having public channel values. Hence, the IoVCom is resistant to a user impersonation attack.

6) ***Man-in-the-middle:*** An adversary can understand M_{XX} or $\mathcal{MXX}$ after knowing public channel values, then a man-in-the-middle attack is possible in the system. According to the proposed system, IoV components transmit M_1/M_2, M_3, t_1, ID'_{V_a}, M_4, M_5, t_2, M_6, t_3 via a public channel. Hence, $\mathcal{A}$ knows all these values. However, M_1 is calculated as $K_S \oplus M_{XX} \oplus Q_{V_a}$ in the IoVCom and thus, $\mathcal{A}$ should get K_S, Q_{V_a}, and M_1 to get M_{XX}. Further, V_a does not send M_1 to the IoV component, and K_S is only known to the IoV server. Besides, $\mathcal{A}$ cannot calculate Q_{V_a} because s/he does not have PW_{V_a} and p_i. Further, $M_1/M_2, M_3, M_4, M_5$, and M_6 are computed using a one-way hash function. Therefore, $\mathcal{A}$ cannot get M_{XX} correctly. Further, $\mathcal{A}$ should have $M_{XX}, K_S, Q_{V_a}, X_{V_a}$ to know $\mathcal{MXX}$, but s/he is unable to get these values through public channel parameters due to unavailability of K_S, M_{XX}, Q_{V_a}. It is hard to know $\mathcal{MXX}$ or M_{XX} and hence, a man-in-the-middle attack is not feasible in the IoVCom.

7) ***Sybil:*** $\mathcal{A}$ applies this attack to reduce the system performance and thus, legal users do not get required resources on-time, which may lead to the system failure in some circumstances. An adversary (a legal/illegal user) sends a good number of request using different identities to the receiver (e.g. IoV components). Hence, the verification process (at the receiver side) requires more computational resources to perform necessary execution, and it leads to a high requirement of operational cost and wastage of resources. The IoVCom quickly completes all essential operations (refer Table 3) and an adversary does not have any opportunity to succeed in performing illegal activities as discussed in other attacks (refer Section 4.1.1 and 4.1.5). Therefore, if $\mathcal{A}$ sends multiple login requests using different identities, then also the receiver confirms its correctness immediately and rejects the forged requests directly. Thus, an adversary fails to put the high impact of a Sybil attack in the IoVCom.

8) ***Illusion:*** This attack is similar to a modification attack, but it is carried out by executing two operations as (1) sends bogus/modified messages to the receivers and (2) does changes in a vehicle (e.g. OBU) to send false information from a vehicle itself. Therefore, it is difficult to identify the correctness of messages. An illusion attack cannot be identified easily because $\mathcal{A}$ attempts to do some alterations at a low level (e.g. OBU) and thus, the receiver believes on the received messages from the sender after confirming the legitimacy of a user. However, a vehicle user is directly connected with different data sources (i.e., RSU, wireless sensor, infrastructure) to exchange information in the IoV structure and thus, it is justifiable for the receiver to believe on messages once s/he verifies the legitimacy of a sender as per the proposed system. Here, TPD/OBU/RSU/Sensor/Smart-chip/Infrastructure are installed by the TA, and an adversary cannot manipulate any hardware device(s) of IoV components. To verify message correctness and user legitimacy, the IoVCom performs well for security requirements (i.e., authenticity, confidentiality, and integrity) as discussed in other security attacks analysis previously (refer Section 4.1.1 to 4.1.6). It means that $\mathcal{A}$ fails to perform any malicious activities based on modification, delay in messages, impersonation, understanding transferred messages, etc. Therefore, the IoVCom is protected against an illusion attack.

9) ***Collision Induction:*** In general, vehicles disseminate their present location to nearby vehicles to stop/reduce collision between moving vehicles on the road. However, if a user suddenly decreases the speed of a vehicle, then nearby vehicle users do not get enough time to manage the distance between these vehicles and thus, there is a collision between vehicles. When the system takes more time in the implementation process, there is a very high probability of accidents on the road for safety-related services. Thus, the communication overhead and execution time of the system should be minimal to prevent this kind of situation on the road. In the IoVCom (for V2V communication), the execution time and communication cost are 0.0600 *ms* (refer Table 3) and 188 bytes (refer Table 4) respectively due to usage of low-cost operations (SHA-256 and EC 256-bit) and primitives (identity, SHA-256, time-stamp, and EC). Hence, the receivers have more time to manage the collision situation on the road, which reduces a very high number of vehicle accidents. For this reason, the IoVCom has a very low impact of a collision induction attack or collisions are easily prevented in the IoVCom.

Now, we do the comparison for various attacks among different data transmission protocols, and it is described in Table 2. In this table, two attacks (Sybil and collision induction) are characterized in four different categories (i.e., low, average, high, very high) based on their impact on the communication protocol, and other attacks are represented as ∅ (if possible) or ✓ (if not feasible).

4.2 Performance Analysis

This section discusses performance results (for computational cost, communication overhead, storage cost, and energy consumption) of various data verification schemes.

1) ***Computational Time:*** It is calculated by considering the total number of essential cryptographic operations during the communication phase [22]. Vehicular communication schemes are designed using different operations, i.e., one-way hash function ($T_{h(\cdot)}$), asymmetric encryption/decryption (T_{enc}/T_{dec}), EC multiplication (T_{EC}), exponential (T_{exp}), and bi-linear pairing (T_{bp}). On the system configuration (Intel(R) Core (TM), 5200U 2.20 GHz, Core i5 processor, RAM 8 GB), $T_{h(\cdot)}$ expects 0.0060 milliseconds (*ms*) and T_{exp} needs 2.0202 *ms*. Further, T_{enc} requires 1.2861 *ms*, T_{dec} takes 38.9570 *ms*, T_{EC} needs 1.0384 *ms*, and T_{bp} requires 43.7419 *ms*.

Table 2: Security Attributes Comparison for Relevant Vehicular Communication Schemes

Schemes	Type	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
Li et al. [17]	V2R	✓	∅	✓	NA	✓	∅	✓	Average	Average	★
	V2V-Direct	✓	∅	✓	NA	✓	∅	✓	Average	Average	☒
	V2V-RSU	✓	∅	✓	NA	✓	∅	✓	Average	Average	★
Sun et al. [29]	V2R	✓	∅	✓	NA	✓	∅	✓	Average	Average	★
	V2V-Direct	✓	∅	✓	NA	✓	∅	✓	Average	Average	☒
	V2V-RSU	✓	∅	✓	NA	✓	∅	✓	High	High	★
Muthumeenakshi et al. [30]	V2V-RSU	✓	✓	∅	✓	∅	✓	✓	Very High	Very High	★
Liu et al. [31]	V2R	✓	∅	∅	NA	✓	∅	✓	Very High	Very High	☒
Wang et al. [32]	V2R	∅	✓	✓	NA	∅	✓	∅	Very High	Very High	★
Zhang et al. [33]	V2V/V2R	✓	∅	✓	NA	✓	∅	✓	High	High	☒
IoVCom	V2V	✓	✓	✓	✓	✓	✓	✓	Low	Low	★
	M2V	✓	✓	✓	✓	✓	✓	✓	Low	Low	★
	V2R	✓	✓	✓	✓	✓	✓	✓	Low	Low	★
	V2S	✓	✓	✓	✓	✓	✓	✓	Low	Low	★
	V2I	✓	✓	✓	✓	✓	✓	✓	Low	Low	★

A1-Modification; **A2-**Plain-text; **A3-**Replay; **A4-**Password guessing; **A5-**Impersonation; **A6-**Man-in-the-middle; **A7-**Illusion; **A8-**Impact of Sybil; **A9-**Impact of collision induction; **A10-**Mutual authentication; ✓−Secure; ∅−Insecure; ★−Available; ☒−Does not provide;

A message requires some amount of time to reach at the receiver side from a sender and this time is called as the latency. According to [39], the latency is 0.419 *ms* for hashed parameters. By considering this latency, we fix the value of $\Delta t_1/\Delta t_2/\Delta t_3$ in the proposed protocols. Similarly, we consider the same latency in [17], [29], [30], [31], [32], and [33].

In [17], data is exchanged in three ways as (1) V2R (2) vehicle-to-vehicle straight away**:** V2V-Direct (3) vehicle-to-vehicle via RSU**:** V2V-RSU and accordingly, the execution time is 4.3800 *ms*, 2.9200 *ms*, and 6.1600 *ms* for V2R, V2R-Direct, and V2V-RSU respectively. Similarly, Sun et al. [29] came up with three different communication schemes (V2R, V2V-Direct, and V2V-RSU) to exchange information, and they expect 6.1720 *ms* for V2R, 6.1600 *ms* for V2V-Direct, and 8.7600 *ms* for V2V-RSU. In [30], the system needs 28.3908 *ms* to convey relevant data for V2V-RSU communication. The computational time is 50.0083 *ms* for V2R in [31], 123.0448 *ms* for V2R in [32], and 7.2988*ms* for V2V/V2R in [33].

However, the IoVCom presents five different types of communications (V2I, V2R, V2V, V2S, and M2V) to exchange relevant information, and it expects $8T_{h(\cdot)} + 3T_{EC}$= 3.1632 *ms*, $6T_{h(\cdot)} + 2T_{EC}$ = 2.0768 *ms*, $10T_{h(\cdot)}$ = 0.0600 *ms*, $8T_{h(\cdot)}$ = 0.0480 *ms*, and $10T_{h(\cdot)}$ = 0.0600 *ms* for V2I, V2R, V2V, V2S, and M2V respectively. The computational time is comparatively high as 3.1632 *ms* (for V2I) and 2.0768 *ms* (for V2R) in the IoVCom because we have used EC small-scale multiplication. However, all legitimate receivers can extract important information from the same message without compromising security requirements in V2R communication. Further, the infrastructure verifies more than one messages at the same time by taking 3.1632 *ms*. Hence, the IoVCom is collectively efficient for all five types of communications. Here, wireless sensor, RSU, and infrastructure are installed by the concerned authority and thus, these components are reliable. However, mobile device and vehicle are totally independent devices and hence, we confirm the correctness (by checking $W'_{V_i} \overset{?}{=} W_{V_i}$ or $W'_{V_a} \overset{?}{=} W_{V_a}$) at the other end. Table 3 shows the experimental time comparison for different schemes.

2) ***Communication and Storage Cost:*** The communication cost is calculated based on the total number of used various variables during the transmission over a public channel. The storage cost is a memory requirement to save essential parameters. We consider that SHA-2 hash digest ($h(\cdot)$) is of 256 bits (32 bytes); the public key is 3072-bit RSA key; a size of identity/random number (*ID*) is of 16 bytes; a time-stamp (*T*) needs 4 bytes; asymmetric encryption/decryption (*PE/D*) requires 384 bytes; and an elliptic curve (*EC*) takes 64 bytes (since the size of p is 256 bits.) [22]. Sometimes, a sender transfers a variable, which is computed using two identity/normal parameters and thus, the cost of this variable (*ID-ID*) is 32 bytes. Further, an exponential (*EXP*) variable requires 32 bytes. A sender transfers a variable (computed using time-stamp, public key, and identity parallel) and therefore, it needs 404 bytes, and we have denoted it as *T-PubK-ID*. Similarly, 420 bytes are expected for *T-PubK-ID-ID* (computed using time-stamp, public key, and two identities parallel). Moreover, 40 bytes are expected when a variable is sent after computing exponential and normal parameters (*EXP-ID*) collectively.

By considering the required cost for each parameter, we calculate the communication overhead and the storage cost for [17], [29], [30], [31], [32], [33], and the IoVCom. Table 4 shows statistics for communication and storage costs. The total cost (communication and storage) is 2000 bytes (for V2R), 840 bytes (for V2V-Direct), and 2792 bytes (for V2V-RSU) in [17]; 2464 bytes (for V2R), 1648 bytes (for V2V-Direct), and 4400 bytes (for V2V-RSU) in [29]; 608 bytes (for V2V-RSU) in [30]; 704 bytes (for V2R) [31]; 1004 bytes (for V2R) in [32]; and 452 bytes (for V2V/V2R) [33]. However, the communication overhead is 188 bytes for V2V, V2M, and V2S communications in the IoVCom. And, the communication cost is 132 bytes for V2R communication and 236 bytes for V2I communication in the IoVCom. Besides, the storage cost is 448 bytes for V2V, 128 bytes for V2M, 48 bytes for V2R, 64 bytes V2S, and 128 bytes for V2I in the IoVCom. Figure 13 shows the total cost comparison for relevant vehicular communication protocols to understand the IoVCom's efficiency for the memory requirement.

Table 3: Computational Analysis Statistics for Different Communication Protocols

Schemes	Type	Cryptographic Operations	Time (*ms*)	Energy (mJ)
Li et al. [17]	V2R	$3T_{enc} + 3T_{dec}$	4.3800	284.700
	V2V-Direct	$2T_{enc} + 2T_{dec}$	2.9200	189.800
	V2V-RSU	$4T_{enc} + 4T_{dec}$	6.1600	400.400
Sun et al. [29]	V2R	$4T_{enc} + 4T_{dec} + 2T_h(\cdot)$	6.1720	401.180
	V2V-Direct	$4T_{enc} + 4T_{dec}$	6.1600	400.400
	V2V-RSU	$6T_{enc} + 6T_{dec}$	8.7600	569.400
Muthumeenakshi et al. [30]	V2V-RSU	$18T_h(\cdot) + 14T_{exp}$	28.3908	1845.402
Liu et al. [31]	V2R	$6T_{EC}$+$6T_{h(\cdot)}$+$1T_{bp}$	50.0083	3250.5395
Wang et al. [32]	V2R	$15T_{exp}$+$11T_{h(\cdot)}$+$5T_{EC}$+$2T_{bp}$	123.0448	7997.912
Zhang et al. [33]	V2V/V2R	$7T_{EC}$+$5T_{h(\cdot)}$	7.2988	474.422
Proposed	V2V	$10T_{h(\cdot)}$	0.0600	3.900
	V2M	$10T_{h(\cdot)}$	0.0600	3.900
	V2R	$6T_{h(\cdot)} + 2T_{EC}$	2.0768	134.992
	V2S	$8T_{h(\cdot)}$	0.0480	3.120
	V2I	$8T_{h(\cdot)} + 3T_{EC}$	3.1632	205.608

Table 4: Communication and Storage Cost Comparison for Various Communication Protocols

Schemes	Type	Communication Overhead (bytes)	Storage Cost (bytes)
Li et al. [17]	V2R	3(*T*) +7 (*ID*) + 3(*PE/D*) + 1(*ID-ID*) + 1(*T-PubK-ID-ID*) = 1728	1(*PubK*) + 1(*ID*) = 272
	V2V-Direct	1(*T*) + 1(*ID*) + 1(*PE/D*) + 1(*T-PubK-ID-ID*) = 824	1(*ID*) = 16
	V2V-RSU	3(*T*) + 6(*ID*) + 3(*PE/D*) + 3(*T-PubK-ID-ID*) = 2520	1(*ID*) + 1(*PubK*) = 272
Sun et al. [29]	V2R	7(*ID*) + 1(*ID-ID*) + 4(*PE/D*) + 3(*T*) + 2($h(\cdot)$) + 1(*T-PubK-ID*) = 2160	1(*ID*) + 1(*PubK*) + 1($h(\cdot)$) = 304
	V2V-Direct	3(*ID*) +2 (*PE/D*) + 2(*T*) + 2(*T-PubK-ID*) = 1632	1(*ID*) = 16
	V2V-RSU	12(*ID*) + 4(*T-PubK-ID*) + 6(*PE/D*) + 4(*T*) = 4128	1(*ID*) + 1(*PubK*) = 272
Muthumeenakshi et al. [30]	V2V-RSU	6($h(\cdot)$) + 6(*ID*) +2 (*EXP*) + 4(*EXP-ID*) = 544	4(*ID*) = 64
Liu et al. [31]	V2R	1(*ID*) +2 (*ID-ID*) + 5(*EC*) = 400	3(*ID*) + 4 (*EC*) = 304
Wang et al. [32]	V2R	6(*ID*) + 7($h(\cdot)$) + 9(*EXP*) + 3(*EC*) = 604	3(*ID*) + 11(*EXP*) = 400
Zhang et al. [33]	V2V/V2R	1(*ID*) + 1(*T*) + 1($h(\cdot)$) + 2(*EC*) = 180	1(*ID*) + 4(*EC*) = 272
IoVCom	V2V	1(*ID*) + 3(*T*) + 5($h(\cdot)$) = 188	6($h(\cdot)$) + 4(*ID*) + 3(*EC*) = 448
	V2M	1(*ID*) + 3(*T*) + 5($h(\cdot)$) = 188	2(*ID*) + 3($h(\cdot)$) = 128
	V2R	1(*T*) + 2($h(\cdot)$) + 1(*EC*) = 132	1(*ID*) + 1($h(\cdot)$) = 48
	V2S	1(*ID*) + 3(*T*) + 5($h(\cdot)$) = 188	2(*ID*) + 1($h(\cdot)$) = 64
	V2I	3(*T*) + 6($h(\cdot)$) = 236	2(*ID*) + 1($h(\cdot)$) + 1(*EC*) = 128

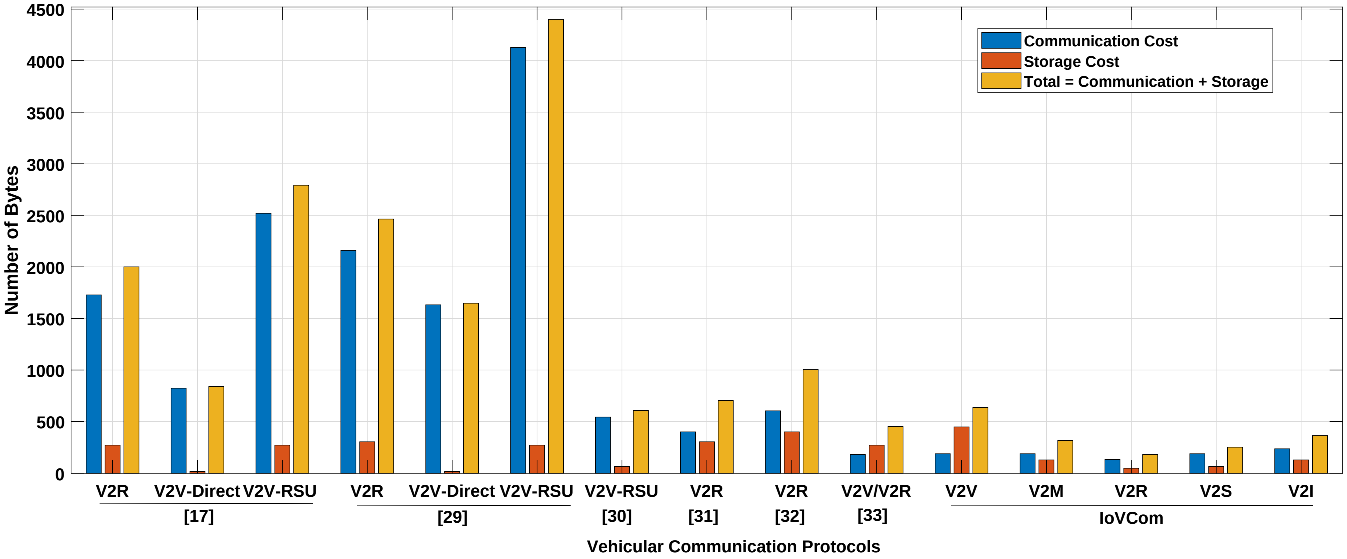


Figure 13: Total (communication and storage) cost comparison for different vehicular communication schemes.

3) ***Energy consumption:*** To execute the system procedures, it needs an amount of energy, and it is called as energy consumption. It is computed as $EC = T_E * C$ and is measured in millijoule (mJ). Here, T_E = Total required experimental time; EC = energy consumption power; C = the CPU maximum power, 65 W (20 V input and 3.25 Amp power) for the used system configuration [40]. Accordingly, we have calculated energy requirement for [17], [29], [30], [31], [32], [33], and the IoVCom. The energy consumption is described in Table 3 for all these vehicular communication protocols. The IoVCom takes 3.900 mJ (for V2V and V2M communications), 3.120 mJ (for V2S communication), 134.992 mJ (for V2R communication), and 205.608 mJ (for V2I communication). During the V2R communication, the IoVCom sends one message to all nearby vehicle by

using 134.992 mJ, and all receivers can extract vital information from the same message without compromising security requirements. Further, the infrastructure verifies more than one messages with 205.608 mJ during V2I communication (in the IoVCom). Hence, the proposed IoV communication system is comparatively efficient for energy consumption.

5 Conclusions and Future Works

We have proposed a secure and energy-efficient communication system for the IoV architecture by including all five communications (V2V, V2R, V2M, V2S, and V2I). Thus, the IoVCom is helpful in various applications for vehicle users on the road. Moreover, security evaluations show that the IoVCom resists to well-known security attacks such as Sybil, user impersonation, illusion, modification, collision induction, man-in-the-middle, password guessing, plain-text, and replay. Further, we have compared the IoVCom with different communication protocols (of VANETs, IoT, and IoV) to measure performance (for storage cost, communication overhead, execution time, and energy consumption), and the performance results achieve better outcomes comparatively. Hence, the IoVCom is highly expedient for IoV-based applications in this smart environment. Therefore, the proposed communication protocols can be practiced reliably in different smart city applications to transmit meaningful data between IoV components, and this will generate a new source of revenue for private and public sector stakeholders.

In the future, we shall come up with new communication protocols for the IoV framework to resist future cyber-attacks by verifying security strengths through security tools and improve performance results.

References

[1] M. Batty, K. W. Axhausen, F. Giannotti, A. Pozdnoukhov, A. Bazzani, M. Wachowicz, G. Ouzounis, and Y. Portugali, ”Smart cities of the future,” *The European Physical Journal Special Topics*, vol. 214, no. 1, pp. 481-518, 2012.

[2] V. Albino, U. Berardi, and R. M. Dangelico, ”Smart cities: Definitions, dimensions, performance, and initiatives,” *Journal of urban technology*, vol. 22, no. 1, pp. 3-21, 2015.

[3] J. B. Kenney, ”Dedicated short-range communications (DSRC) standards in the United States,” *Proceedings of the IEEE*, vol. 99, no. 7,pp. 1162-1182, 2011

[4] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, ”A comprehensive survey on vehicular ad hoc network,” *Journal of network and computer applications*, vol. 37, pp. 380-392, 2014.

[5] S. B. Lee, G. Pan, J. S. Park, M. Gerla, and S. Lu, ”Secure incentives for commercial ad dissemination in vehicular networks,” *in proc. of* 8^{th} *ACM Mobihoc*, 2007, pp. 150-159.

[6] S. Bitam, A. Mellouk, and S. Zeadally, ”VANET-cloud: a generic cloud computing model for vehicular Ad Hoc networks,” *IEEE Wireless Communications*, vol. 22, no. 1, pp. 96-102, 2015.

[7] 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.

[8] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, ”Internet of things: A survey on enabling technologies, protocols, and applications,” *IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2347-2376, 2015.

[9] K. Abboud, H. A. Omar, and W. Zhuang, ”Interworking of DSRC and cellular network technologies for V2X communications: A survey,” *IEEE transactions on vehicular technology*, vol. 65, no. 12, pp. 9457-9470, 2016.

[10] K. Wevers, and M. Lu, ”V2X Communication for ITS - from IEEE 802.11p Towards 5G,” *IEEE 5G Tech Focus*, vol. 1, no. 2, 2017.

[11] J. Contreras, S. Zeadally, and J. A. Guerrero-Ibanez, ”Internet of Vehicles: Architecture, Protocols, and Security,” *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3701-3709, 2017.

[12] J. A. Guerrero-Ibanez, S. Zeadally, and J. Contreras-Castillo, ”Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies,” *IEEE Wireless Communications*, vol. 22, no. 6, pp. 122-128, 2015.

[13] M. Gerla, E. K. Lee, G. Pau, and U. Lee, ”Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds,” *in proc. of* 1^{st} *IEEE WFIoT*, 2014, pp. 241-246.

[14] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, ”Routing in internet of vehicles: A review,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 5, pp. 2339-2352, 2015.

[15] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, ”Connected vehicles: Solutions and challenges,” *IEEE internet of things journal*, vol. 1, no. 4, pp. 289-299, 2014.

[16] C. Zhang, X. Lin, R. Lu, P. H. Ho, and X. Shen, ”An efficient message authentication scheme for vehicular communications,” *IEEE Transactions on Vehicular Technology*, vol. 57, no. 6, pp. 3357-3368, 2008.

[17] J. Li, H. Lu, and M. Guizani, ”ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 938-948, 2015.

[18] J. P. Hubaux, S. Capkun, and J. Luo, ”The security and privacy of smart vehicles,” *IEEE Security & Privacy*, vol. 2, pp. 49-55, 2004.

[19] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, and X. Cui, ”Attacks and countermeasures in the internet of vehicles,” *Annals of Telecommunications*, vol. 72, no. 5-6, pp. 283-295, 2017.

[20] W. Xi, C. Qian, J. Han, K. Zhao, S. Zhong, X. Y. Li, and J. Zhao, ”Instant and robust authentication and key agreement among mobile devices,” *in proc. of* 23^{rd} *ACM CCS*, 2016, pp. 616-627.

[21] J. Wan, D. Zhang, S. Zhao, L. Yang, and J. Lloret, ”Context-aware vehicular cyber-physical systems with cloud support: architecture, challenges, and solutions,” *IEEE Communications Magazine*, vol. 52, no. 8, pp. 106-113, 2014.

[22] D. He, S. Zeadally, B. Xu, and X. Huang, ”An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681-2691, 2015.

[23] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, ”2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 2, pp. 896-911, 2016.

[24] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, ”Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response,” *IEEE Transactions on Computers*, vol. 65, no. 8, pp. 2562-2574, 2016.

[25] C. Lyu, D. Gu, Y. Zeng, and P. Mohapatra, ”PBA: Prediction-based authentication for vehicle-to-vehicle communications,” *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 71-83, 2016.

[26] P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, ”Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015-1028, 2016.

[27] J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, ”An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 5, pp. 1621-1632, 2018.

[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 Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2740-2749, 2017.

[29] C. Sun, J. Liu, X. Xu, and J. Ma, ”A Privacy-Preserving Mutual Authentication Resisting DoS Attacks in VANETs,” *IEEE Access*, vol. 5, pp. 24012-24022, 2017.

[30] R. Muthumeenakshi, T. R. Reshmi, and K. Murugan, ”Extended 3PAKE authentication scheme for value-added services in VANETs,” *Computers & Electrical Engineering*, vol. 59, pp. 27-38, 2017.

[31] J. Liu, Q. Li, H. Cao, R. Sun, X. Du, and M. Guizani, ”MDBV: Monitoring Data Batch Verification for Survivability of Internet of Vehicles,” *IEEE Access*, vol. 6, pp. 50974-50983, 2018.

[32] Y. Wang, Y. Ding, Q. Wu, Y. Wei, B. Qin, and H. Wang, ”Privacy-preserving cloud-based road condition monitoring with source authentication in VANETs,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1779-1790, 2018.

[33] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, ”PA-CRT: Chinese Remainder Theorem Based Conditional Privacy-preserving Authentication Scheme in Vehicular Ad-hoc Networks,” *IEEE Transactions on Dependable and Secure Computing*, 2019.

[34] P. Gandotra, R. K. Jha, and S. Jain, ”A survey on device-to-device (D2D) communication: Architecture and security issues,” *Journal of Network and Computer Applications*, vol. 78, pp. 9-29, 2017.

[35] M. N. Mejri, J. Ben-Othman, and M. Hamdi, ”Survey on VANET security challenges and possible cryptographic solutions,” *Vehicular Communications*, vol. 1, no. 2, pp. 53-66, 2014.

[36] F. Sakiz, and S. Sen, ”A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV,” *Ad Hoc Networks*, vol. 61, pp. 33-50, 2017.

[37] V. S. Miller, ”Use of elliptic curves in cryptography,” *in proc. of Advances in Cryptology - CRYPTO*, 1986, pp. 417-426.

[38] X. Lin, and X. Li, ”Achieving efficient cooperative message authentication in vehicular ad hoc networks,” *IEEE Transactions on Vehicular Technology*, vol. 62, no. 7, pp. 3339-3348, 2013.

[39] D. Zelle, C. Kraub, H. Straub, and K. Schmidt, ”On Using TLS to Secure In-Vehicle Networks,” *in* 12^{th} *ACM ARES*, 2017, pp. 1-10.

[40] D. He, C. Chen, S. Chan, and J. Bu, ”Secure and efficient handover authentication based on bilinear pairing functions,” *IEEE Transactions on Wireless Communications*, vol. 11, no. 1, pp. 48-53, 2012.

Trupil Limbasiya is a Ph.D. research scholar in the Department of Computer Science & Information Systems, Birla Institute of Technology & Science (BITS) Pilani, K. K. Birla Goa Campus, India. His research interests include Cryptography, Network Security, and Smart City applications. He has published multiple research articles in peer-reviewed International journals and well-known International conferences. He has also written two book chapters.

Debasis Das received his Ph.D. in Computer Science and Engineering from Indian Institute of Technology (IIT) Patna, India. He joined as Assistant Professor in the Department of Computer Science and Engineering(CSE) at Indian Institute of Technology (IIT) Jodhpur, Rajasthan, India in 2019 and before joining IIT Jodhpur, he was working as an Assistant Professor at Birla Institute of Technology and Science, Pilani (BITS Pilani), K. K. Birla Goa Campus, Goa, India and NIIT University, Rajasthan, India. His research interests include VANETs, Smart Cities, Lightweight Cryptography, Internet of Vehicles (IoV), Blockchain, and Network Security.