MComIoV: Secure and Energy-Efficient Message Communication Protocols for Internet of Vehicles

Trupil Limbasiya, *Student Member, IEEE*, Debasis Das, *Senior Member, IEEE*, and Sajal K. Das, *Fellow, IEEE*

***Abstract*— The Internet of Vehicles (IoV) offers an emerging paradigm that deals with interconnected vehicles interacting with the infrastructure, roadside units (RSUs), sensors, and mobile devices with a goal to sense, compute, store, and transmit vital information or data over a common channel while vehicles are moving. Secure and reliable communication and efficient on-device performance are thus crucial challenges in this paradigm, particularly in presence of limited computation resources. This paper presents a novel secure and energy-efficient message communication system, called *MComIoV*, using a one-way hash function and elliptic curve cryptography (ECC). We evaluate MComIoV through security proof and analysis against various attacks to verify its robustness. The proposed system is also implemented and tested on Raspberry Pi 3B+. Experimental results demonstrate the efficiency in computation time, storage cost, communication overhead, and energy consumption.**

***Index Terms*— Authentication, message communication, confidentiality, integrity, IoV, privacy.**

I. Introduction

MODERN vehicles are not only envisioned as a means for transportation, but also as contributors to different kinds of data collection, computation, and transmission. For example, vehicular ad-hoc network (VANET) is capable of exchanging road-safety and environmental data with nearby vehicles via vehicle-to-vehicle (V2V) communication, and roadside units (RSUs) via vehicle-to-infrastructure (V2I) communication using the dedicated short-range communication (DSRC) standard. Indeed, VANET is used in diverse applications like collision warning, traffic management, cooperative messaging, emergency information, and navigation [1], [2]. However, significant challenges are posed by rapid change in the communication range, reliability in the transient (vehicular) network, node disruption, and fixed bandwidth [3], [4].

It is expected that around 47 million cars of the world will be enabled with the Internet by 2020 [5], and nearly 70% of people on earth will live in urban areas by 2050 [6]. If the current trend continues, people may experience even more crowded situation, polluted air, heavy traffic, overburdened infrastructures, parking issue, and more fuel/energy demand in cities rather than we do have today. Thus, the extensive vehicular communication system is required for the benefits of society, environment, and business growth by exchanging relevant data on the road between a vehicle and nearby smart devices like mobile device, RSU, sensor, other vehicles, etc.

Given the mobile cellular network has many advantages (e.g., large coverage area, pre-existing infrastructure, high data rate, robust scalability, quality of service, and deterministic security) over the DSRC technology, vehicle-to-everything (V2X) communications that use the combination of DSRC and long term evolution (LTE) is more effective. Such communications help to advance the coordination of vehicles, pedestrians, and transport infrastructure on the road, thereby extending the ability of VANET and supporting modern applications for road safety, traveler infotainment, manufacturer services, and traffic optimization [7]–[9]. Thus, V2X communication technologies are emerging to the *Internet of Vehicles* (IoV) paradigm to attain large-scale and ubiquitous automotive infrastructure access by evolving advanced vehicular applications [10].

The IoV paradigm aims to collaborate with the Internet of things (IoT) and VANET architectures for device-to-device communications using DSRC, LTE, and wireless fidelity (Wi-Fi) for various modern smart transportation applications. The IoV framework consists of five different types of devices: the infrastructure, RSUs, wireless sensors, vehicles, and mobile devices for information sensing, processing, storage, and exchanges. Since it is desirable to have direct communication from a vehicle (user) to each of the IoV devices, as shown in Fig. 1, the IoV architecture supports five types of communications – V2V, vehicle-to-roadside unit (V2R), vehicle-to-wireless sensor (V2S), vehicle-to-mobile device (V2M), and vehicle-to-infrastructure (V2I) – to transmit vital information through DSRC, Wi-Fi, or 4G/5G [11], [12].

Due to extensive communication types, the IoV offers advanced applications, collaboration, data awareness, and connectivity for better user experience while moving on the road [13]. The IoV paradigm is an emerging system to transform existing research fields like smart industry, smart healthcare, smart home, and other pertinent applications by connecting to smart transportation for a new line of thought. Hence, IoV applications are classified in two categories as (i) safety and traffic management (i.e., navigation, remote

Manuscript received August 22, 2019; revised June 7, 2020 and September 24, 2020; accepted February 11, 2021; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor Y. Chen. The work of Sajal K. Das was supported by NSF under Grant CNS-2008878, Grant SaTC-2030624, Grant CNS-1818942, Grant OAC-1725755S, and Grant DGE-1433659. *(Corresponding author: Trupil Limbasiya.)*

Trupil Limbasiya is with the Department of Computer Science and Information Systems, Birla Institute of Technology and Science Pilani, K. K. Birla Goa Campus, Zuarinagar 403726, India (e-mail: limbasiyatrupil@gmail.com).

Debasis Das is with the Department of Computer Science and Engineering, Indian Institute of Technology Jodhpur, Jodhpur 342037, India (e-mail: debasis@iitj.ac.in).

Sajal K. Das is with the Department of Computer Science, Missouri University of Science and Technology, Rolla, MO 65409 USA (e-mail: sdas@mst.edu).

Digital Object Identifier 10.1109/TNET.2021.3062766

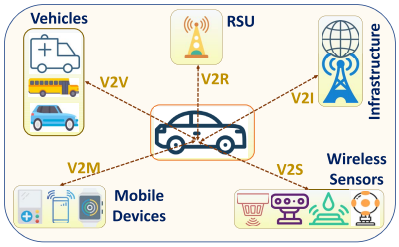

Fig. 1. Different Communications in the IoV Paradigm.

telematics, safety, and diagnostic) (ii) business (i.e., car sharing, infotainment, insurance, payment, and notification) [11], [14].

Since the IoV paradigm connects to many smart transportation applications, its potential economic value is estimated in the range of USD 0.2-0.7 trillion per year by 2025 [15]. One connected vehicle passenger can save around USD 1400 per year collectively for service providers, vehicle user, automotive manufacturers, and society [16]. However, there are vital challenges for V2X communications, such as network scalability, dynamic network topology, heterogeneity, attack prevention, communication latency, user trust and privacy [17]. The IEEE 1609.2 standard is used as security services to transmit applications and management messages in V2X communications. Thus, security protocols are designed to prevent illegal data access and forgery during vehicular data exchanges, thereby the protocols situate in the application layer [18]–[20]. The success of the IoV architecture depends on how secure and privacy-preserving different mechanisms are, including user authentication, data integrity, message confidentiality, and user anonymity [21]. Otherwise, an adversary can launch a wide variety of attacks, such as impersonation, modification, password guessing, session key disclosure, Sybil, replay, man-in-the-middle, and so on to intercept/interrupt the IoV system [22]. Moreover, the IoV devices are configured with different computing, storage, and communication capabilities. For example, a vehicle has limited computing power to process, store, and transmit data, while performing such operations on the move. Furthermore, a vehicle connects with heterogeneous IoV devices through DSRC, LTE, or Wi-Fi for data exchanges. Hence, it is essential to take the computation time, energy consumption, storage cost, and communication overhead into consideration for designing energy-efficient, cost-effective, and secure vehicular communication protocols [11], [23].

To the best of our knowledge, there exists no complete IoV communication system that efficiently provides all five types of IoV communication protocols yet preserving security and privacy. This motivated us to propose new secure and efficient message communication protocols, called MComIoV, for the IoV structure. Our novel contributions are given as follows.

- **MComIoV:** We develop different communication protocols using a one-way hash function (i.e., SHA256) and elliptic curve cryptography (ECC) for V2V, V2R, V2S, V2M, and V2I to transmit important information directly between a vehicle and other IoV devices.
- **Security Analysis:** To guarantee the security robustness, we provide (i) security proof to verify MComIoV's effectiveness for authentication, confidentiality, integrity, and user anonymity through the random oracle model; (ii) security analysis to confirm its strengths against session key disclosure, Sybil, replay, modification, impersonation, password guessing, and man-in-the-middle attacks.
- **Performance Evaluation:** Our experimental results show on the test-bed implementation (through Raspberry Pi 3B+) that the MComIoV not only satisfies security and user privacy, but it is also proven to be efficient in computation time, energy consumption, storage cost, and communication overhead comparatively.

This paper is organized as follows. Section II discusses related works on VANET and IoV communications protocols with emphasis on their security and performance features. Section III gives the design overview of MComIoV including the system model, security goals, and the adversary model. Section IV proposes the MComIoV system for exchanging information between a vehicle and different IoV devices directly. Section V discusses security evaluations while Section VI presents experimental performance results. Section VII concludes the paper with directions for future research.

II. Related Works

Due to various real-life applications, many research and development projects have been implemented in the United States, the European Union, Japan, and other countries around the world. However, the communication system is the key challenge in VANET due to mobility and public channel data transmission [3], [4]. RSUs and on-board-units (OBUs) transmit meaningful data using DSRC publicly. Therefore, there are different data security issues like modification, delay, data loss, impersonation, bogus data, etc. Consequentially, the receiver should verify data and its sender before using it for further process. Thereby, efficient and secure data transmission protocols are necessary for VANETs [24], [25]. We discuss on the existing VANET and IoV communication protocols, as follows.

A. Vehicular Ad-Hoc Networks

In [26], the authors introduced a new message authentication method using RSUs to address security and privacy issues, but it is vulnerable to replay and man-in-the-middle attacks. Besides, it is time-consuming due to the usage of the Diffie-Hellman key agreement. A distributed key management architecture was proposed in [27] to verify messages based on the group signature and to identify selfish vehicles. However, the message verification overhead problem is present at RSUs in [27], and thus, other vehicles do not get on-time services. Similarly, researchers suggested various cooperative message authentication schemes to deal with different vehicular communication issues [20]. The scheme in [28] is proposed using the public-key cryptography to address the non-repudiation issue, and it was designed in such a way so it can be implemented with other schemes together for better performance and security improvements. However, it is time-consuming due to the usage of a signature in data transmission, and the storage cost is high. In [34], a vehicular communication

protocol is presented using bi-linear pairing, ECC, exponential, and one-way hash to send on-road information from a vehicle to nearby RSUs and other vehicles. However, the computation and communication costs are high in [34] due to the usage of more bi-linear pairing and ECC operations. Further, it is vulnerable to man-in-the-middle and Sybil attacks.

B. Internet of Vehicles

Some communication schemes (e.g., [29]–[33]) have referred the IoV structure for data transmission, but none of them have proposed direct vehicular communication protocols for all five types of IoV communications separately.

In [29], they proposed an authentication system for IoV in which the Internet server collects data from different devices (wireless sensors, OBUs, and mobile devices) to share it with OBUs and wireless sensors via RSUs. Hence, OBUs cannot get vital information directly, and it leads to more time-consuming communication during emergency services. Also, no cryptographic primitive is used in [29] before sending data, allowing an adversary to perform different malicious activities.

In [30], the authors suggested a V2V privacy-preserving authentication and key establishment method using asymmetric, exponential, and one-way hash primitives for IoV, but a sender should involve a nearby RSU and the trusted authority to send a message to another vehicle. Hence, it increases the number of connections during V2V communication. Due to the usage of bi-linear pairing and RSA, the computation time is high in [30], and it offers only V2V communication. A data transmission scheme is proposed in [31] for V2R and V2V communications. In V2V, a vehicle sends data to other vehicles via a nearby RSU. Thus, the scope of this protocol is limited for only V2V and V2R communications, and it is vulnerable to replay, concatenation, impersonation, and modification attacks.

The authors in [32] suggested a V2R data batch verification scheme in which OBUs transfer data to an RSU, so the aggregated data is sent to the IoV data center to store meaningful information. However, it is weak against replay and man-in-the-middle attacks. Furthermore, the computational cost and communication overhead are high in [32] due to the usage of bi-linear pairing operation. In [33], a V2R communication scheme is proposed for IoV in which an OBU sends data to other vehicles via a nearby RSU. The performance results in [33] are not efficient in terms of computation time, communication overhead, and energy consumption due to the usage of high-cost operations like RSA and bi-linear pairing.

III. Design Overview of the MComIoV

We illustrate the system model to get an overview of the proposed system (MComIoV), security goals for the MComIoV, and valid assumptions in the adversary model.

A. System Model

In the MComIoV, five types of devices such as vehicles, RSUs, wireless sensors, mobile devices, and the infrastructure are involved for IoV communications through DSRC, Wi-Fi, or 4G/5G, as shown in Fig. 1 [11], [12]. And these devices once connect to the IoV server directly through the transport layer security (TLS) protocol [28], [30] for the registration/initial setup process, as displayed in Fig. 2.

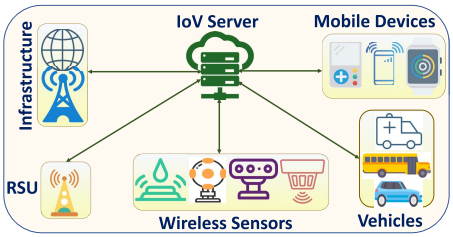

Fig. 2. Basic Setup and Registration Connections in the IoV Architecture.

1) **IoV Server:** It is the road-transport trusted authority, acting as the central registration center for trusted devices (wireless sensors, RSUs, and the infrastructure) and end-user devices (vehicles and mobile devices). It deploys trusted devices, whereas end-user devices initiate the registration process with the IoV server to get various parameters for future communications with other IoV devices. The IoV server keeps the registration record of all IoV devices in its secure database and can trace the real identity of any registered device if necessary.
2) **Infrastructure:** It is a trusted entity (e.g., cloud) in the IoV with the highest computational and storage capacity for data analytics of the received data from different vehicles. Also, it provides meaningful information to a vehicle based on the request (as V2I communication). The infrastructure has tamper-resistance hardware (TRH) as a storage space to keep its private values securely.
3) **RSU:** It is a trusted device located near the road for V2R communication through DSRC, having high computation and storage power compared to OBUs, mobile devices, and wireless sensors. An RSU contains a TRH to save its private values securely and verifies/computes the messages during the V2R communication.
4) **Wireless Sensor:** It is available at different spots in a vehicle to sense in-vehicle automotive and environmental information. Further, it shares relevant up-to time information with a vehicle after verifying the user requests during V2S communication. A TRH is fixed into a wireless sensor to save its secret parameters.
5) **Vehicle:** A vehicle user owns it, and an OBU is installed in a vehicle during the registration phase by configuring with limited computational power for computation, transmission, and verification on behalf of a vehicle user during IoV communications. Further, an OBU consists of small storage memory to save sensitive information securely, and it is called as a tamper-proof-device (TPD).
6) **Mobile Device:** It is one kind of portable computing device (like mobile phone, wearable device, tablet, etc.) to communicate with a vehicle (user) directly using 4G/5G or Wi-Fi. A smart-chip (i.e., smart card) is fixed in a mobile device during the registration phase with fixed computing capacity to process/transmit/confirm

message request and its response during V2M communication.

B. Security and Privacy Goals

IoV communications happen in a public network in which messages include private and confidential information like user activity, personal conversation, vehicle location, payment details, etc. Thus, an adversary may intercept or interrupt IoV communications for user impersonation, message intervention, data tampering, identity tracing, stop/delay messages, etc. Hence, it is necessary to achieve different security and privacy goals during communications [28], [30], [34]. We illustrate our security and privacy goals for the MComIoV, as follows.

Integrity: When communications or online transactions are carried out in a public environment, it is necessary to confirm the correctness of the obtained data at the receiver side to maintain data integrity in the communication system.

Confidentiality: IoV communications include various confidential and private information. Thus, it is important to transmit messages secretly to preserve confidentiality.

Privacy: People are not interested to disclose their personal information and practices like vehicle movement pattern, identity, already visited places, current location, present activities, etc. Hence, the protection of personal activities and information is an essential goal in a public network.

Authentication: When the user is interested to connect with another user for some information over a public channel, both users (sender and receiver) should confirm each other's authenticity before proceeding to a communication.

C. Adversary Model

The goal of an adversary is to interrupt or intercept IoV communications centered on a vehicle to get services as an unauthorized user, understand transmitted messages illegally, send forged messages, delay vital information, and re-transmit packets to reduce the performance efficiency of the receiver. We consider following security and performance assumptions as the adversary's capability in the system [35]–[37].

1) In the communication system, the registration/initial phase is performed through the transport layer security (TLS) protocol, considering a private/secure channel, whereas authentication/communication phases are executed via a public/insecure channel. If any variables are sent in a public network, then only an adversary ($\mathcal{A}$) can capture these values for deletion, modification, rerouting, re-transmission, and interception. However, $\mathcal{A}$ cannot get any parameters from a secure channel [28], [30].
2) A smart-chip is not tamper-proof storage space and thus, if $\mathcal{A}$ gets the access of a smart-chip, then s/he can reveal stored values from this smart-chip. However, $\mathcal{A}$ cannot extract any values from a TPD/TRH, and if $\mathcal{A}$ attempts to access the stored information from a TPD/TRH, then they are destroyed instantly [24], [25], [28].
3) We assume $\mathcal{X}$ and $\mathcal{Y}$ are valid users in the system. If $\mathcal{X}$ can correctly compute all necessary values to communicate with other users on behalf of $\mathcal{Y}$, then $\mathcal{X}$ is an adversary for $\mathcal{Y}$, being a legitimate user in the system.
4) A one-way hash function is irreversible. Thus, it is not feasible to reveal information from the computed hash value once the one-way hash operation is applied.
5) $\mathcal{A}$ can guess only one value at a time. It means that $\mathcal{A}$ can consider either the user password or random nonce as a guessable value in the same computation. However, two random nonce or more than one parameter cannot be guessed together in polynomial time.
6) $\mathcal{A}$ knows the complete design of the protocol.
7) We have an equation as $\alpha = \beta \oplus \gamma$. If $\mathcal{A}$ knows α and β, then s/he can get γ easily. However, $\mathcal{A}$ cannot compute α, β, or γ by having only one parameter (β or γ or α).
8) If both (sender and receiver) agree on common session key parameters, then only the session key is computed with the validity of a limited period. If it expires, then both should recompute a new session key.

IV. MComIoV: Proposed Communication System

The IoV architecture offers five types of IoV communications to exchange various kinds of information with different categories of IoV devices through DSRC, LTE, or Wi-Fi. Thus, it is worthwhile to have separate reliable communication protocols in the interest of a vehicle user to transmit safety, infotainment, and business-related messages while connecting a vehicle with all other heterogeneous IoV devices. Hence, we propose new secure and privacy-preserving efficient different communication protocols (called MComIoV) for all five types of IoV communications. The MComIoV is designed using low-cost cryptographic primitives, i.e., SHA-256, ECC, concatenation ($||$), and bit-wise XOR ($\oplus$) for cost-effective, efficient, secure, and privacy-preserving data exchanges. The MComIoV mainly consists of two phases as (i) basic setup and registration (ii) IoV communications. For the system initialization, an elliptic curve (EC) group G is considered as $E_p(a, b)$ on $y^2 = x^3 + ax + b$ to generate point values with P as the generator and an order of q, where p is a 256-bit large prime number. The EC scalar multiplication is written as $k \cdot P = P + P + \ldots + P, \in Z_q^*$. If P is known, then also it is infeasible to get k due to the EC discrete logarithm problem [38]. The IoV server (S_{IoV}) takes two random nonce (x and RN_{SK}) and the initial time-stamp (IT_{SK}) to calculate $SK = h(RN_{SK} \oplus PW_{SK} \oplus IT_{SK})$, $h(SK||IT_{SK}||x)$ and keeps SK and $h(SK||IT_{SK}||x)$ securely, where PW_{SK} is the secret key password of S_{IoV}. We use different notations in the design of MComIoV, and they are described in Table I.

A. Basic Setup and Registration Phase

This phase is a primary step and a one-time process for all IoV players. Once the IoV server completes the initial procedure, it saves some values in the protected memory of trusted devices (RSUs, wireless sensors, and infrastructure) to deploy them at different locations for V2R/V2S/V2I communications. When trusted devices receive the vehicle user request/message in the future, it is verified, referring to storage memory

TABLE I
LIST OF SYMBOLS WITH ITS DESCRIPTION

Symbol	Description
V_i	A vehicle user
RSU_j	A Road-side-unit
WS_k	A wireless sensor
MD_l	A mobile use
$Infra$	The infrastructure
S_{IoV}	The IoV server
SK	256-bit secret key of S_{IoV}
ST_{SK}	The initial time-stamp of S_{IoV}
ID_X	An identity of X entity
PW_{V_i}	Password of V_i
$a_i/b_i/x/RN_{SK}$	Random nonce
T_{V_i}	V_i registration time-stamp
K_X	256-bit secret key of X entity
$List_Y$	List of Y value
TPD_i/OBU_{V_i}	A TPD/OBU of V_i's vehicle
TRH_j/TRH_m	A tamper-resistance hardware
SC_{MD_l}	A smart chip
Pub_{RSU_j}	The public key of RSU_j
ΔT	The maximum time delay
T_1/T_3	Time-stamp at the sender side
T_2	Time-stamp at the receiver end

parameters (of trusted devices). On the other side, end-user devices (vehicles and mobile devices) are registered with S_{IoV} by their owner to get some parameters, which are used in future for IoV communications to authenticate the owner and compute/verify messages. We explain the setup/registration process for each IoV device in-detail as follows.

ⓘ **RSU Setup:** The IoV server (S_{IoV}) performs the following steps to install tamper-resistance hardware (TRH_j) in road-side-unit (RSU_j) and deploys it on the road for V2R communication. Fig. 3 shows the RSU setup phase.

- S_{IoV} selects an RSU identity (ID_{RSU_j}) and 256-bit random secret key (K_{RSU_j}) for RSU_j to calculate the private key, $Pri_{RSU_j} = h(ID_{RSU_j}||K_{RSU_j}) \oplus h(SK||IT_{SK}||x)$ and the public key, $Pub_{RSU_j} = Pri_{RSU_j} \cdot P$.
- S_{IoV} saves ID_{RSU_j} in its database, and $h(SK||IT_{SK}||x)$, ID_{RSU_j}, K_{RSU_j}, and Pub_{RSU_j} in TRH_j securely. Finally, S_{IoV} installs TRH_j in RSU_j to deploy it on the road.

ⓘⓘ **Vehicle Registration:** A vehicle user (V_i) should register his/her vehicle with the IoV server (S_{IoV}) through the following steps to participate in different IoV communications legitimately. A vehicle registration is a one-time and essential process for all new vehicle users, as shown in Fig. 3.

- V_i selects his/her identity (ID_{V_i}), password (PW_{V_i}), and a random nonce (a_i) to compute $A_i = h(ID_{V_i}||PW_{V_i}) \oplus h(PW_{V_i}||a_i)$, $B_i = A_i \oplus a_i \oplus h(PW_{V_i}||a_i)$. V_i sends $\{ID_{V_i}, A_i, B_i\}$ to S_{IoV} over the TLS protocol [28], [30].
- S_{IoV} computes $C_i = h(ID_{V_i}||A_i||B_i)$, $E_i = B_i \oplus ID_{V_i}$, $D_i = h(C_i||SK||T_{V_i}||b_i)$, and $F_i = D_i \oplus h(SK||IT_{SK}||x)$, where T_{V_i} is a registration time-stamp for V_i; b_i and x are randomly generated numbers.
- S_{IoV} stores $C_i, D_i, E_i, F_i, List_{Pub_{RSU_j}}$ into a tamper-proof device (TPD_i) of V_i to install it in a vehicle of V_i and keeps ID_{V_i}, D_i in its database securely.

ⓘⓘⓘ **Wireless Sensor Setup:** S_{IoV} performs the following steps to install a wireless sensor (WS_k) in a vehicle for V2S communication, and its process is displayed in Fig. 3.

- S_{IoV} chooses an identity (ID_{WS_k}) for WS_k and computes $AID_{V_i} = h(ID_{V_i}||D_i||ID_{WS_k})$.
- S_{IoV} saves ID_{WS_k} in its database for the reference and $List_{D_i}$, $List_{AID_{V_i}}$, $h(SK||IT_{SK}||x)$, ID_{WS_k} in a tamper-resistance hardware (TRH_k) of WS_k securely. Finally, S_{IoV} installs TRH_k in WS_k to deploy WS_k in a vehicle.

ⓘⓥ **Mobile Device Registration:** A mobile device user registers his/her mobile device with S_{IoV} as follows for legal V2M communication in future, also as described in Fig. 3.

- A mobile device user (MD_l) chooses his/her identity (ID_{MD_l}), password (PW_{MD_l}), and a random nonce (d_l) to calculate $U_l = h(ID_{MD_l}||PW_{MD_l}||d_l)$ and sends $\{ID_{MD_l}, U_l\}$ to S_{IoV} over the TLS protocol [28], [30].
- S_{IoV} computes $W_l = h(U_l) \oplus h(SK||IT_{SK}||x)$, $X_l = W_l \oplus ID_{MD_l} \oplus U_l$ and saves W_l, X_l into a smart-chip (SC_{MD_l}) to fix it in a mobile device of MD_l.
- MD_l computes $G_l = h(PW_{MD_l} \oplus ID_{MD_l}) \oplus d_l$, $H_l = X_l \oplus h(PW_{MD_l}||d_l)$, $I_l = W_l \oplus h(d_l \oplus PW_{MD_l})$. MD_l removes W_l, X_l from SC_{MD_l} and stores G_l, H_l, I_l in SC_{MD_l}.

ⓥ **Infrastructure Setup:** The infrastructure (e.g., cloud) should know essential credentials of the IoV communication system to exchange meaningful information with vehicle users through V2I communication. Thus, S_{IoV} installs tamper-resistance hardware (TRH_m) in the infrastructure ($Infra$) and deploys $Infra$, performing as follows. The infrastructure setup procedure is also displayed in Fig. 3.

- S_{IoV} takes 256-bit random secret key (K_{Infra}) for $Infra$ to compute $M_{Infra} = h(K_{Infra}||T_{Infra})$ and $AID_{V_i} = h(ID_{V_i}||D_i)$, where T_{Infra} is the infrastructure setup time-stamp. S_{IoV} stores $M_{Infra}, h(SK||IT_{SK}||x)$, $List_{AID_{V_i}}$, $List_{D_i}$ into TRH_m to install it in $Infra$ for the deployment. S_{IoV} regularly updates TRH_m for AID_{V_i}, and D_i of new vehicles over the TLS protocol.

B. Data Transmission/Communication Phase

The IoV architecture has a huge scope for business growth and various smart transportation applications, keeping the focus on a vehicle to transmit pertinent information directly with other heterogeneous IoV devices through V2V, V2R, V2S, V2M, and V2I communications. The IoV devices are different in terms of configuration, device type (trusted or end-user and who is sender/receiver), and communication technology, thereby having dissimilar computation, storage, and communication abilities. Further, IoV communications also differ based on the priority of message availability, information type, data transmission (one-to-one or broadcasting), and user/message verification (one by one or batch). Hence, we propose different protocol designs for each IoV communication while balancing security, user privacy, and operational efficiency requirements. We describe the design of each protocol in detail as follows.

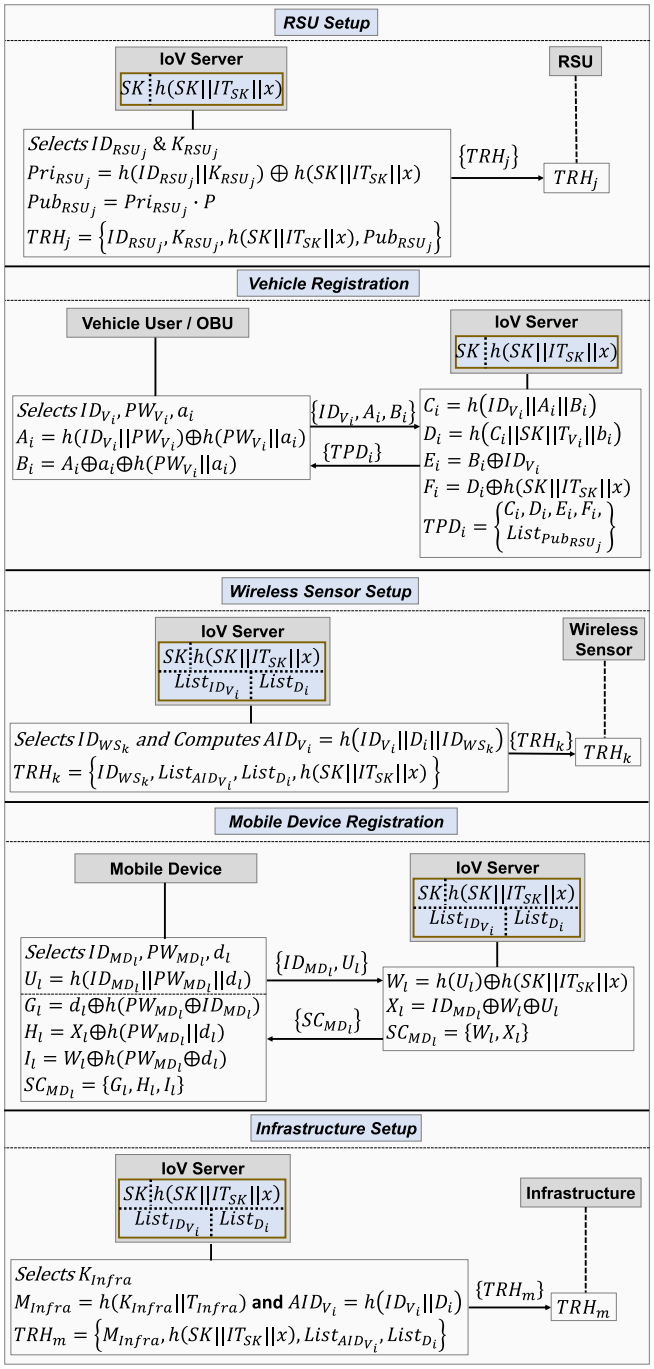

Fig. 3. MComIoV: Registration/Setup Phases.

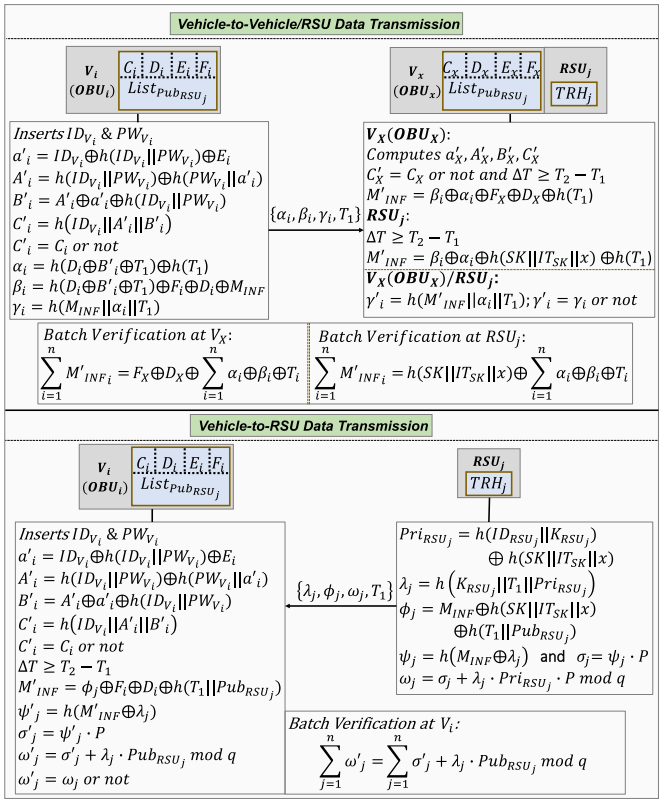

Fig. 4. MComIoV: V2V and V2R Communication Phases.

1) Vehicle-to-Vehicle/RSU Data Transmission: When a vehicle user (V_i) wants to exchange traffic and safety information with nearby other vehicles/RSUs using DSRC, V_i executes the following steps, also shown in Fig. 4. V_i regularly sends safety messages to the receivers (another vehicle (V_X) and RSU (RSU_j)) after every 300 milliseconds (*ms*) to inform neighbours about their status while on the move [1]. The receiver performs batch verification to decrease the verification overhead. If it is valid, then only the receiver considers the obtained messages. Otherwise, it discards them directly.

(i) V_i inserts ID_{V_i} and PW_{V_i} in OBU_{V_i} to calculate $a'_i = E_i \oplus h(ID_{V_i}||PW_{V_i}) \oplus ID_{V_i}$, $A'_i = h(ID_{V_i}||PW_{V_i}) \oplus h(ID_{V_i}||PW_{V_i})$, $B'_i = a'_i \oplus A'_i \oplus h(ID_{V_i}||PW_{V_i})$, and $C'_i = h(ID_{V_i}||A'_i||B'_i)$. If $C'_i = C_i$, then only V_i is a legal vehicle user. Otherwise, OBU_{V_i} terminates the session directly.

(ii) If $C'_i = C_i$, OBU_{V_i} calculates $\alpha_i = h(D_i \oplus T_1 \oplus B'_i) \oplus h(T_1)$, $\beta_i = M_{\mathcal{INF}} \oplus h(D_i \oplus T_1 \oplus B'_i) \oplus F_i \oplus D_i$, $\gamma_i = h(M_{\mathcal{INF}}||\alpha_i||T_1)$ and sends $\{\alpha_i, \beta_i, \gamma_i, T_1\}$ to V_X/RSU_j over a public channel. $M_{\mathcal{INF}}$ is on-road safety and traffic message to send from a vehicle to other vehicles/RSUs.

(iii) If the receiver is V_X, then OBU_{V_X} verifies the driver (V_X) by asking ID_{V_X}, PW_{V_X} and computes a'_X, A_X, B_X, C_X (similar to the first step). If $C'_X = C_X$, then only V_X is a legitimate vehicle user to proceed to the next step. If the receiver is RSU_j, then it directs to the next step instantly.

(iv) V_X/RSU_j confirms the validity of $\{\alpha_i, \beta_i, \gamma_i, T_1\}$, computing $\Delta T \geq T_2 - T_1$, where T_1 is the current time-stamp of V_i, T_2 is a receiving time of $\{\alpha_i, \beta_i, \gamma_i, T_1\}$, and ΔT is the threshold time. If it holds, then V_X and RSU_j calculates $M'_{\mathcal{INF}} = \alpha_i \oplus \beta_i \oplus h(T_1) \oplus F_X \oplus D_X$ and $M'_{\mathcal{INF}} = \alpha_i \oplus \beta_i \oplus h(SK||IT_{SK}||x) \oplus h(T_1)$ respectively. Further, V_X/RSU_j computes $\gamma'_i = h(M'_{\mathcal{INF}}||\alpha_i||T_1)$ to confirm $\gamma'_i = \gamma_i$ or not. If both are equal, then only V_X/RSU_j accepts $M'_{\mathcal{INF}}$ to make their decision(s). If $\gamma'_i \neq \gamma_i$, then V_X/RSU_j immediately rejects the session.

2) RSU-to-Vehicle Data Transmission: When vehicles move on the road, they get only nearby information from in-range vehicles due to DSRC. Thus, RSUs send extensive

environmental and on-road information to in-range vehicles after every 300 *ms* by transmitting warning and traffic-related messages to deal with current and forthcoming situations while on the move [1]. Hence, vehicle users can take suitable decision(s) ahead of time while driving. A vehicle receives multiple messages from RSUs, thereby increasing the verification overhead at OBU. Consequently, we design a data transmission protocol using the batch verification concept to reduce the verification cost. It is also displayed in Fig. 4.

(i) A road-side-unit (RSU_j) does $Pri_{RSU_j} = h(SK||IT_{SK}||x) \oplus h(ID_{RSU_j}||K_{RSU_j})$, $\lambda_j = h(K_{RSU_j}||T_1||Pri_{RSU_j})$, $\phi_j = M_{\mathcal{INF}} \oplus h(SK||IT_{SK}||x) \oplus h(T_1||Pub_{RSU_j})$, $\psi_j = h(M_{\mathcal{INF}} \oplus \lambda_j)$, $\sigma_j = \psi_j \cdot P$, $\omega_j = \sigma_j + \lambda_j \cdot Pri_{RSU_j} \cdot P$ mod q to broadcast $\{\lambda_j, \phi_j, \omega_j, T_1\}$ to nearby vehicles.

(ii) The receiver vehicle (V_i) follows Step-1 of *Vehicle-to-Vehicle/RSU Data Transmission* phase [Section IV.B.1].

(iii) OBU_i checks validity of $\{\lambda_j, \phi_j, \omega_j, T_1\}$ by $\Delta T \geq T_2 - T_1$, where T_2 is the receiving time-stamp at the receiver end, T_1 is the current time-stamp at the sender side, and ΔT is the threshold time. If the freshness holds, OBU_i computes $M'_{\mathcal{INF}} = h(T_1||Pub_{RSU_j}) \oplus \phi_j \oplus D_i \oplus F_i$, $\psi'_j = h(M'_{\mathcal{INF}} \oplus \lambda_j)$, $\sigma'_j = \psi'_j \cdot P$, $\omega'_j = \sigma'_j + \lambda_j \cdot Pub_{RSU_j}$ mod q. If $\omega'_j = \omega_j$, OBU_i considers $M'_{\mathcal{INF}}$ as unmodified message sent by RSU_j. Otherwise, OBU_i instantly discards that message. OBU_i computes the following equation for the batch verification to confirm legality and integrity of received multiple messages from RSUs.

$$\sum_{j=1}^{n} \omega'_j = \sum_{j=1}^{n} \sigma'_j + \lambda_j \cdot P_{Pub} \ mod \ q$$

3) Vehicle-to-Wireless Sensor Communication: When a vehicle user (V_i) needs in-vehicle automotive and environmental information to take better decision(s) on the road, s/he sends a request message ($M_{\mathcal{RE}}$) to a wireless sensor (WS_k) using Wi-Fi or 4G/5G technology. If the request is valid, then WS_k sends a response message ($M_{\mathcal{RS}}$) to V_i. The detailed procedure is as follows, also displayed in Fig. 5.

(i) V_i follows Step-1 of *Vehicle-to-Vehicle/RSU Data Transmission* phase [refer Section IV.B.1].

(i) OBU_{V_i} computes $P_i = h(ID_{WS_k}||T_1||D_i) \oplus F_i \oplus D_i \oplus M_{\mathcal{RE}}$, $AID_{V_i} = h(ID_{V_i}||D_i||ID_{WS_k})$, $Q_i = h(P_i||M_{\mathcal{RE}}||T_1||AID_{V_i})$ to send $\{P_i, Q_i, AID_{V_i}, T_1\}$ to WS_k over a public channel. Here, OBU_{V_i} gets the wireless sensor identity (ID_{WS_k}) by scanning the Wi-Fi network and T_1 is the current time-stamp.

(ii) WS_k checks the freshness of $\{P_i, Q_i, ID_{V_i}, T_1\}$ through $\Delta T \geq T_2 - T_1$, where T_2 is a receiving time of the message request at WS_k. If it holds, WS_k calculates $M'_{\mathcal{RE}} = P_i \oplus h(ID_{WS_k}||T_1||D_i) \oplus h(SK||IT_{SK}||x)$, $Q'_i = h(P_i||M'_{\mathcal{RE}}||T_1||AID_{V_i})$ to check $Q'_i \stackrel{?}{=} Q_i$. Here, WS_k gets D_i from TRH_{WS_k} based on AID_{V_i}. If $Q'_i = Q_i$, WS_k does $R_i = M_{\mathcal{RS}} \oplus h(ID_{WS_k} \oplus T_2 \oplus M'_{\mathcal{RE}}) \oplus h(SK||IT_{SK}||x)$, $S_i = h(M_{\mathcal{RS}}||T_2||Q'_i)$ to send $\{R_i, S_i, T_2\}$ to V_i. If $Q'_i \neq Q_i$, WS_k immediately ends the session.

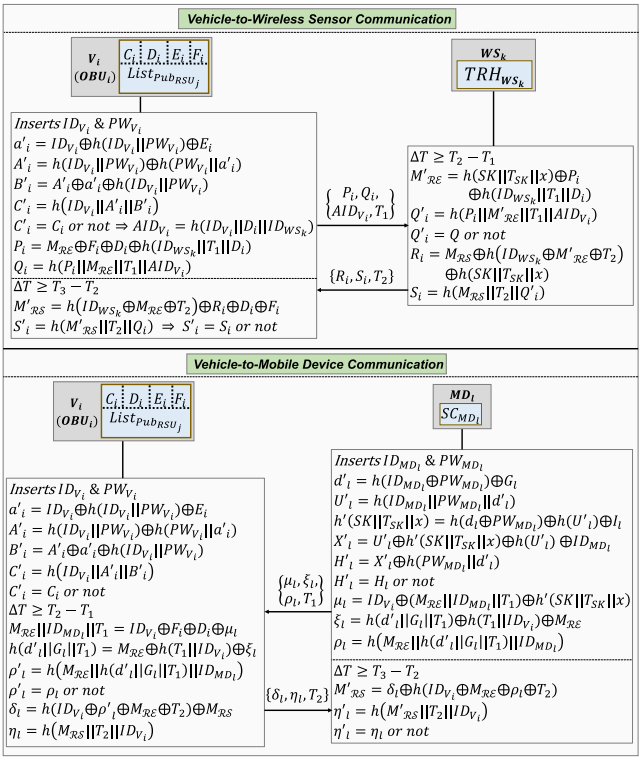

Fig. 5. MComIoV: V2S and V2M Communication Phases.

(iii) OBU_{V_i} computes $\Delta T \geq T_3 - T_2$, where $T_3 =$ receiving time of $\{R_i, S_i, T_2\}$ at V_i. If it holds, OBU_i calculates $M'_{\mathcal{RS}} = R_i \oplus F_i \oplus D_i \oplus h(ID_{WS_k} \oplus T_2 \oplus M_{\mathcal{RE}})$, $S'_i = h(M'_{\mathcal{RS}}||T_2||Q_i)$. If $S'_i = S_i$, OBU_i considers $M'_{\mathcal{RS}}$ as valid information to make its decision(s) else, OBU_i discards $M'_{\mathcal{RS}}$.

4) Vehicle-to-Mobile Device Communication: When a mobile device user (MD_l) wants to connect with V_i for personal conversations like location status, on-road information, or private chat, s/he performs the following steps for V2M communication through 4G/5G or Wi-Fi, shown in Fig. 5.

(i) MD_l inserts ID_{MD_l}, PW_{MD_l} in SC_{MD_l} to compute $d'_l = h(PW_{MD_l} \oplus ID_{MD_l}) \oplus G_l$, $U'_l = h(ID_{MD_l}||PW_{MD_l}||d'_l)$, $h'(SK||IT_{SK}||x) = h(U'_l) \oplus h(d'_l \oplus PW_{MD_l}) \oplus I_l$, $X'_l = U'_l \oplus ID_{MD_l} \oplus h(U'_l) \oplus h'(SK||IT_{SK}||x)$, $H'_l = X'_l \oplus h(PW_{MD_l}||d'_l)$. If $H'_l = H_l$, then only SC_{MD_l} calculates $\mu_l = (M_{\mathcal{RE}}||ID_{MD_l}||T_1) \oplus h'(SK||IT_{SK}||x) \oplus ID_{V_i}$, $\xi_l = M_{\mathcal{RE}} \oplus h(T_1||ID_{V_i}) \oplus h(d'_l||G_l||T_1)$, $\rho_l = h(M_{\mathcal{RE}}||h(d'_l||G_l||T_1)||ID_{MD_l})$ and transfers $\{\mu_l, \xi_l, \rho_l, T_1\}$ to V_i over a public channel.

(ii) V_i follows Step-1 of *Vehicle-to-Vehicle/RSU Data Transmission* phase [refer Section IV.B.1].

(iii) If $C'_i = C_i$, OBU_i checks the freshness of $\{\mu_l, \xi_l, \rho_l, T_1\}$ through $\Delta T \geq T_2 - T_1$ and computes $(M_{\mathcal{RE}}||ID_{MD_l}||T_1) = \mu_l \oplus F_i \oplus D_i \oplus ID_{V_i}$, $h(d'_l||G_l||T_1) = h(T_1||ID_{V_i}) \oplus \xi_l \oplus M'_{\mathcal{RE}}$, $\rho'_l = h(M'_{\mathcal{RE}}||h(d'_l||G_l||T_1)||ID_{MD_l})$. If $\rho'_l = \rho_l$, then OBU_i calculates $\delta_l = M_{\mathcal{RS}} \oplus h(M'_{\mathcal{RE}} \oplus ID_{V_i} \oplus T_2 \oplus \rho'_l)$, $\eta_l = h(M_{\mathcal{RS}}||T_2||ID_{V_i})$ to send $\{\delta_l, \eta_l, T_2\}$ to MD_l.

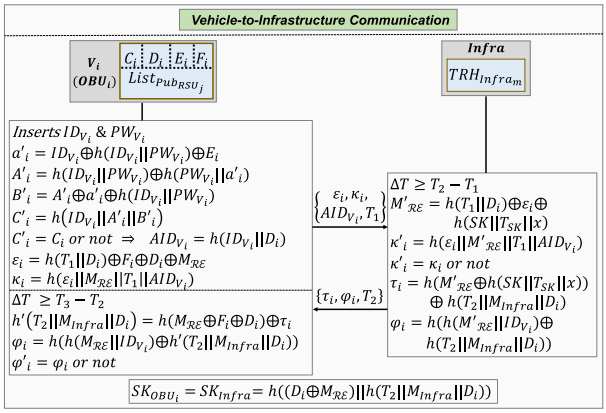

Fig. 6. MComIoV: V2I Communication Phase.

(iv) SC_{MD_l} checks validity of $\{\delta_l, \eta_l, T_2\}$ through $\Delta T \geq T_3 - T_2$. If it holds, SC_{MD_l} computes $M'_{\mathcal{RS}} = \delta_l \oplus h(ID_{V_i} \oplus M_{\mathcal{RE}} \oplus \rho_l \oplus T_2)$, $\eta'_l = h(M'_{\mathcal{RS}}||T_2||ID_{V_i})$. If $\eta'_l = \eta_l$, then only MD_l will consider $M'_{\mathcal{RS}}$ as a valid response. In other cases, SC_{MD_l} immediately rejects the session.

5) Vehicle-to-Infrastructure Communication: When V_i requires some global information (such as location-based information, remote diagnostic, or relevant automotive services) extensively, s/he can connect with the infrastructure (e.g., cloud) via V2I communication using Wi-Fi or 4G/5G, as follows and also displayed in Fig. 6.

(i) V_i follows Step-1 of *Vehicle-to-Vehicle/RSU Data Transmission* phase [refer Section IV.B.1].

(ii) OBU_i computes $AID_{V_i} = h(ID_{V_i}||D_i)$, $\varepsilon_i = F_i \oplus D_i \oplus M_{\mathcal{RE}} \oplus h(T_1||D_i)$, $\kappa_i = h(\varepsilon_i||M_{\mathcal{RE}}||T_1||AID_{V_i})$ to send $\{\varepsilon_i, \kappa_i, AID_{V_i}, T_1\}$ to the infrastructure ($Infra$). $Infra$ checks its validity by $\Delta T \geq T_2 - T_1$. If it holds, then $Infra$ proceeds for $M'_{\mathcal{RE}} = \varepsilon_i \oplus h(T_1||D_i) \oplus h(SK||IT_{SK}||x)$, $\kappa'_i = h(\varepsilon_i||M'_{\mathcal{RE}}||T_1||AID_{V_i})$. If $\kappa'_i = \kappa_i$, then $Infra$ calculates $\tau_i = h(T_2||M_{Infra}||D_i) \oplus h(M'_{\mathcal{RE}} \oplus h(SK||IT_{SK}||x))$, $\varphi_i = h(h(M'_{\mathcal{RE}}||ID_{V_i}) \oplus h(T_2||M_{Infra}||D_i))$ to transfer $\{\tau_i, \varphi_i, T_2\}$ as a response message to OBU_i (of V_i).

(iii) OBU_i checks its freshness by calculating $\Delta T \geq T_3 - T_2$. If it is valid, OBU_i computes $h'(T_2||M_{Infra}||D_i) = \tau_i \oplus h(M_{\mathcal{RE}} \oplus F_i \oplus D_i)$, $\varphi'_i = h(h(M_{\mathcal{RE}}||ID_{V_i}) \oplus h'(T_2||M_{Infra}||D_i))$. If $\varphi'_i = \varphi_i$, then both (OBU_i and $Infra$) separately calculate the temporary session key as $SK_{OBU_i} = SK_{Infra} = h((D_i \oplus M_{\mathcal{RE}})||h(T_2||M_{Infra}||D_i))$ to exchange messages. If this key gets expired, then they should calculate it again.

V. Security Analysis

We discuss the security proof of the MComIoV to confirm its security robustness by considering three definitions based on the random oracle model (ROM) as (i) outsider adversary (ii) insider adversary and (iii) user privacy. Furthermore, we explain how the MComIoV can resist various security attacks by referring to the adversary model (Section III.C).

A. Outsider Adversary

Definition 1: An adversary ($\mathbb{AA}$) is not a registered user in the communication system. However, $\mathbb{AA}$ can capture common channel messages (sent during all five types of IoV communications) in the MComIoV.

Theorem 1: The MComIoV can withstand against $\mathbb{AA}$'s adaptive illegal actions under a one-way hash function properties based on the ROM in polynomial time.

Proof: According to *Definition 1*, $\mathbb{AA}$ knows public channel parameters $\alpha_i, \beta_i, \gamma_i, T_1$ (V2V data transmission), $\lambda_j, \phi_j, \omega_j, T_1$ (V2R data transmission), P_i, Q_i, AID_{V_i}, T_1, R_i, S_i, T_2 (V2S communication), μ_l, ξ_l, ρ_l, T_1, δ_l, η_l, T_2 (V2MD communication), ε_i, κ_i, AID_{V_i}, T_1, τ_i, φ_i, T_2 (V2I communication). An adversary performs malicious activities mainly for two reasons as (i) to know some information, which can help in future to get something more and (ii) to interrupt a connection during the communication phase to gain some information from the system. First instance is an action of a passive attack, and second case is an active attack.

To apply a passive attack in the MComIoV, $\mathbb{AA}$ wants to know vital information $M_{\mathcal{INF}}$ (in V2V and V2R data transmissions) and $M_{\mathcal{RE}}, M_{\mathcal{RS}}$ (in V2S, V2M, and V2I communications). We explain in-detail as follows that how there is no possibility to reveal $M_{\mathcal{INF}}, M_{\mathcal{RE}}, M_{\mathcal{RS}}$ as per the *Definition 1*. Therefore, $\mathbb{AA}$ cannot understand transmitted messages.

- To get $M_{\mathcal{INF}}$, $\mathbb{AA}$ should know F_i, D_i, but these values are not available to $\mathbb{AA}$ because s/he is not a legal user of the system as per the *Definition 1*. In V2V and V2R data transmission protocols, the sender transfers messages to all nearby OBUs and RSUs. Thus, only authorized entities (RSUs and OBUs) can reveal M_{INF} by calculating $\alpha_i \oplus F_X \oplus D_X \oplus h(T_1) \oplus \beta_i$ (if V_X is the receiver.) and $\alpha_i \oplus h(SK||IT_{SK}||x) \oplus h(T_1) \oplus \beta_i$ (RSU_j as the recipient) during V2V data transmission. For V2R data transmission, M_{INF} can be extracted as $\phi_j \oplus F_i \oplus D_i \oplus h(T_1||Pub_{RSU_j})$ by V_i legally. However, $\mathbb{AA}$ cannot get F_X/F_i and D_X/D_i in the MComIoV (for V2V and V2R). Hence, it is not feasible to understand $M_{\mathcal{INF}}$ in the proposed V2V and V2R data transmissions.
- In V2S communication, $\mathbb{AA}$ needs F_i, D_i, ID_{WS_k} for $M_{\mathcal{RE}}$ by intercepting P_i. However, $\mathbb{AA}$ is unknown to D_i and F_i according to *Definition 1*. Also, it is not an easy task as $\mathbb{AA}$ to get F_i, D_i due to unavailability of required parameters for the computation of these parameters (refer Fig. 5). Further, it is very hard to know $M_{\mathcal{RS}}$ without knowing $M_{\mathcal{RE}}, F_i, D_i$ in V2S communication.
- $\mathbb{AA}$ needs $F_i, ID_{V_i}, D_i, G_l, d_l$ to understand $M_{\mathcal{RE}}$ in V2M communication, but $\mathbb{AA}$ does not know these values anyhow. Thus, $\mathbb{AA}$ is unable to know $M_{\mathcal{RE}}$ in V2M communication (see Fig. 5). Moreover, $\mathbb{AA}$ does not have $M_{\mathcal{RE}}$, ID_{V_i}. Hence, it becomes more difficult to know $M_{\mathcal{RS}}$ during V2M communication.
- $\mathbb{AA}$ requires $D_i, F_i, h(SK||IT_{SK}||x)$ to know $M_{\mathcal{RE}}$ in V2I communication (refer Fig. 6), but $\mathbb{AA}$ cannot compute all these values from public channel parameters due to unavailability of other required values.

In the case of an active attack, an adversary wants to do modification, delay, re-transmission, interception, or impersonation during IoV communications. To perform these malicious activities in the MComIoV, $\mathbb{AA}$ should know B_i, D_i, F_i (in V2V data transmission), $K_{RSU_j}, Pri_{RSU_j}, h(SK||IT_{SK}||x)$ (for V2R data transmission), ID_{WS_k}, F_i, D_i (in V2S communication), $h(SK||IT_{SK}||x), ID_{MD_l}, ID_{V_i}$ (for V2M communication), D_i, F_i (in V2I communication).

B_i, D_i, and F_i are computed as $A_i \oplus a_i \oplus h(PW_{V_i}||a_i)$, $h(C_i||SK||T_{V_i}||b_i)$, and $D_i \oplus h(SK||IT_{SK}||x)$ respectively (refer Vehicle Registration phase in Fig. 3). In the MComIoV, it is not possible for $\mathbb{AA}$ to compute/reveal B_i, D_i, and F_i due to unavailability of essential values for the computation.

K_{RSU_j} is the 256-bit secret key of RSU_j, and $h(SK||IT_{SK}||x)$ is calculated using SK (secret key of S_{IoV}), IT_{SK} (initial time-stamp of S_{IoV}), and x (random nonce). Pri_{RSU_j} is computed as $h(ID_{RSU_j}||K_{RSU_j}) \oplus h(SK||IT_{SK}||x)$. Hence, it is hard to get all essential values for illegal V2R communication because $\mathbb{AA}$ does not have all vital credentials.

$\mathbb{AA}$ gets ID_{WS_k} by scanning the Wi-Fi network, but D_i and F_i are not known, and they are computed as $h(C_i||SK||T_{V_i}||b_i)$ and $h(SK||IT_{SK}||x) \oplus D_i$ respectively. Thus, $\mathbb{AA}$ cannot calculate D_i and F_i, as s/he does not know none of these values. Hence, it is not feasible to send forged messages to the receiver illegally during V2S communication.

$\mathbb{AA}$ should know D_i and F_i to do malicious activities during V2I communication, but s/he does not have these values, as discussed previously. Hence, $\mathbb{AA}$ cannot execute illegal activities in V2I communication, considering *Definition 1*.

$\mathbb{AA}$ does not know $h(SK||IT_{SK}||x)$ as per the *Definition 1*. ID_{MD_l} is a mobile user identity, and ID_{V_i} is a vehicle user identity. The IoV communication system includes a large number of vehicles and mobile device users for V2M communication. Therefore, it is difficult to guess ID_{V_i} and ID_{MD_l} correctly together in polynomial time. ■

B. Insider Adversary

Definition 2: Now, we consider an adversary ($\mathbb{AB}$) is a registered vehicle user (V_a) of the IoV communication system. Thus, $\mathbb{AB}$ knows his/her private credentials and public communication parameters. In this definition, V_a plays two roles (as a legal user and as an attacker for other IoV entities).

Theorem 2: The MComIoV is secure to $\mathbb{AB}$'s adaptive unauthorized activities under a one-way hash function consideration in the random oracle model in polynomial time.

Proof: As per the *Definition 2*, V_a knows his/her ID_{V_a}, PW_{V_a} and can compute a_a (chosen random nonce during V_a registration), A_a, B_a (refer Vehicle Registration phase). Besides, V_a knows public channel parameters α_i, β_i, γ_i (in V2V); λ_j, ϕ_j, ω_j (in V2R); P_i, Q_i, AID_{V_i}, R_i, S_i (in V2S); μ_l, ξ_l, ρ_l, δ_l, η_l (in V2M); and ε_i, κ_i, AID_{V_i}, τ_i, φ_i (in V2I).

In V2V and V2R data transmission protocols, the sender broadcasts $M_{\mathcal{INF}}$ (contains on-road information) to all nearby RSUs/OBUs using DSRC standard. If the receiver is registered with S_{IoV}, then s/he is authorized to understand $M_{\mathcal{INF}}$. Hence, it is not an illegal activity to get vital information as a registered vehicle user. If the receiver is not a registered user of the MComIoV, then s/he cannot retrieve the original messages due to the unavailability of required values, as discussed in the proof of *Theorem 1*. Besides, V_a needs B_i, D_i, K_{RSU_j}, Pri_{RSU_j} to do modification/impersonation during V2V and V2R communications. However, V_a cannot compute these necessary values even though s/he is a registered vehicle user, as these parameters are not the same for different vehicle users. Hence, if V_a attempts to do forgery on behalf of any legal vehicle user, then s/he is identified by the receiver directly.

In V2S communication, P_i, Q_i, and AID_{V_i} are computed as $h(ID_{WS_k}||T_1||D_i) \oplus F_i \oplus D_i \oplus M_{\mathcal{RE}}$, $h(P_i||M_{\mathcal{RE}}||T_1||AID_{V_i})$, and $h(ID_{V_i}||D_i||ID_{WS_k})$ respectively. Thus, $\mathbb{AB}$ should know ID_{WS_k}, D_i, and ID_{V_i} to understand $M_{\mathcal{RE}}$. However, V_a does not know these values because s/he is not confident that which ID_{WS_k} and ID_{V_i} (out of a large number wireless sensors and vehicle users) are used in the computation. Further, D_i is calculated as $h(C_i||SK||T_{V_i}||b_i)$, and it is difficult to recompute without knowing C_i, SK, T_{V_i}, and b_i. Consequently, it becomes hard for $\mathbb{AB}$ to compute/modify essential parameters to do malicious activities in V2S communication. Similarly, V_a cannot perform forgery in V2M and V2I communications without knowing ID_{V_i}, ID_{MD_l}, D_i, M_{Infra} correctly (refer Fig. 5 and Fig. 6) respectively. Hence, $\mathbb{AB}$ is unsuccessful to perform illegal actions in the MComIoV. ■

C. User Privacy

Definition 3: An adversary ($\mathbb{AC}$) is a vehicle/mobile device user (registered or non-registered with the IoV server). Hence, $\mathbb{AC}$ knows his/her private credentials and different public communication parameters. The prime motive of $\mathbb{AC}$ is to reveal the original identity of both (sender and receiver) during communications to trace users and their activities.

Theorem 3: The original identity and activities of vehicle and mobile device users are not revealed to preserve user privacy during IoV communications in the MComIoV.

Proof: In the MComIoV, the sender transfers different parameters over a public channel as α_i, β_i, γ_i (in V2V); λ_j, ϕ_j, ω_j (during V2R); P_i, Q_i, AID_{V_i}, R_i, S_i (in V2S); μ_l, ξ_l, ρ_l, δ_l, η_l (during V2M); ε_i, κ_i, AID_{V_i}, τ_i, φ_i (in V2I).

Firstly, ID_{V_i} and ID_{MD_l} are not sent in plain-text over a common channel in the MComIoV. Thus, $\mathbb{AC}$ cannot get the original identity of users directly. Secondly, ID_{V_i} and ID_{MD_l} are used in μ_l, ξ_l, ρ_l, δ_l, η_l, and φ_i computations, but it is not feasible to get the user identity from these values because they are calculated using different values, which are unknown to $\mathbb{AC}$. Moreover, $\mathbb{AC}$ cannot understand personal activities from public channel messages, as described in the proof of *Theorem 2*. Thirdly, the MComIoV is designed using a one-way hash function. If a variable is computed using a one-way hash, then it is not possible to know input values from its generated output due to its irreversible property. For all these reasons, $\mathbb{AC}$ cannot reveal the original iden-

tity of vehicle/mobile device users to trace them and their activities. ■

D. Protection Against Attacks

Now, we explain how the MComIoV resists to various active attacks (i.e., session key disclosure, replay, impersonation, Sybil, and modification) and passive attacks (like password guessing and man-in-the-middle) based on the adversary model (refer Section III.C) because these attacks may damage the vehicular communication system [21].

To apply any one of active attacks, an adversary ($\mathcal{A}$) should know all used parameters (in the message request computation) to regenerate and send the forged message request to the receiver on behalf of any legal user. Further, the receiver should accept the sent message (by $\mathcal{A}$), and $\mathcal{A}$ should get a response message from the receiver. As per the design of MComIoV, $\mathcal{A}$ (as a registered or non-registered user) cannot compute all message request parameters, as discussed in *Theorem 1 proof* and *Theorem 2 proof*. Besides, the receiver confirms the authenticity, integrity, and freshness of all received messages. Thus, if $\mathcal{A}$ attempts to do forgery in the MComIoV, applying any one of active attacks, then it is captured directly at the receiver. Hence, the MComIoV resists to impersonation, session key disclosure, modification, and Sybil attacks.

Messages are sent over a common channel during IoV communications, taking some time to reach at the receiver, which is known as the latency in data transmission. In the MComIoV, we consider latency as 0.419 *ms* (by considering SHA-256 bits computation) [40]. Based on this latency, we set the value of ΔT to discard delayed messages to secure the MComIoV protocols against a replay attack.

An adversary applies passive attacks (like password guessing and man-in-the-middle) to perceive vital data or the user password. Thus, s/he should know all the essential input values, which are used in the user password and message computations. In the MComIoV, the vehicle user password (PW_{V_i}) is used as one input parameter to compute A_i and B_i, but $\mathcal{A}$ cannot get these values to compare with the guessed vehicle user password, and s/he does not have ID_{V_i} and a_i for the computation. Similarly, the mobile device user password (PW_{MD_l}) is one input value to calculate U_l, G_l, H_l and I_l. In this case, we consider that $\mathcal{A}$ steals the mobile device and can extract G_l, H_l and I_l from SC_{MD_l} to verify the exactness of the guessed mobile device user password. However, $\mathcal{A}$ does not know d_l, X_l, and W_l to recompute G_l, H_l and I_l for the guessed password confirmation. Thus, it is infeasible to apply a password guessing attack in the MComIoV. Next, $\mathcal{A}$ cannot get $M_{\mathcal{INF}}$, $M_{\mathcal{RE}}$, and $M_{\mathcal{RS}}$, as discussed in *Theorem 1 proof*. Hence, the MComIoV resists to a man-in-the-middle attack.

We understand that the MComIoV satisfies authentication, integrity, confidentiality, and user privacy based on *Theorem 1 proof*, *Theorem 2 proof*, *Theorem 3 proof*, and attacks analysis. Therefore, the MComIoV is secure against various passive, active, and relevant future attacks. We present the comparison of different security attributes in Table II to understand the security robustness of the MComIoV and relevant protocols.

TABLE II
SECURITY ATTRIBUTES COMPARISON FOR COMMUNICATION PROTOCOLS

Schemes	A1	A2	A3	A4	A5	A6	A7	A8
Li et al. [28]	NA	NA	✓	✓	✓	✓	⊗	No
Liu et al. [30]	✓	✓	⊗	✓	⊗	✓	✓	Yes
Wu et al. [31]	NA	NA	✓	⊗	✓	⊗	⊗	Yes
Liu et al. [32]	NA	NA	✓	⊗	✓	✓	⊗	No
Liu et al. [33]	NA	NA	✓	✓	✓	✓	⊗	Yes
Cui et al. [34]	NA	NA	⊗	✓	✓	✓	⊗	Yes
MComIoV	✓	✓	✓	✓	✓	✓	✓	Yes

A1: Session key disclosure**; A2:** Password guessing**; A3:** Sybil **; A4:** Replay**; A5:** Impersonation**; A6:** Modification**; A7:** Man-in-the-middle**; A8:** User anonymity**; ✓: Secure; ⊗: Vulnerable; NA: Not applicable;**

TABLE III
EXECUTION TIME FOR DIFFERENT CRYPTOGRAPHIC OPERATIONS

Operation	Execution Time
RSA encryption (T_{ERSA})	1.1895 *ms*
RSA decryption (T_{DRSA})	37.6819 *ms*
One-way hash SHA 256-bit ($T_{h(\cdot)}$)	0.0382 *ms*
Modulo exponential (T_{Exp})	0.3785 *ms*
Bi-linear paring (T_{BP})	41.6712 *ms*
EC small-scale multiplication (T_{ECSM})	2.8207 *ms*
EC map-to-point (T_{ECMP})	6.1840 *ms*
Hashed-MAC (T_{HMAC})	0.1075 *ms*

VI. PERFORMANCE EVALUATION

We do test-bed implementation on the Raspberry Pi 3B+ platform to measure performance results of relevant vehicular communication schemes because it has a similar kind of configuration to an OBU. The performance results are dependent on the design of a communication protocol. Hence, the implementation output is proportional to the device configuration. Thus, if the MComIoV performs comparatively better on Raspberry Pi 3B+, then it can also achieve reliable results on other hardware devices. Raspberry Pi 3B+ is configured as Quad-core 64-bit ARM Cortex-A53 1.4 GHz CPU with BCM2837B0 chip, 1 GB SRAM, 2.5 Amp power, and 5 V voltage supply [39]. We discuss four performance measures, such as computation time, communication overhead, storage cost, and energy consumption to know the performance efficiency of the MComIoV, [28], [30]–[33], and [34]. Specifically, computation time and communication overhead are comparatively more worthwhile measures in the communication protocol for rapid data transmission, as they are required every time while transmitting messages.

A. Computation Time

The computing device takes some amount of time to execute diverse cryptographic operations, and it is called as the computation time [41]. We execute different cryptographic operations on the test-bed setup using Python 3.1 with *pycrypto*, *bplib*, and *py-ecc* libraries. The average execution time of each operation is shown in Table III after 1000 runs, and it is measured in milliseconds (*ms*). Specifically, the execution time of $\oplus$ and $||$ is very negligible and thus, we do not consider these operations in the computation time. We calculate the total number of required different cryptographic operations for [28], [30]–[34], and MComIoV, as described in Table IV. Referring

TABLE IV
PERFORMANCE MEASURES COMPARISON FOR RELEVANT VEHICULAR COMMUNICATION SCHEMES

Schemes	Type	Communication Cost	Storage Cost	Required Cryptographic operations	Time (*ms*)	Energy (mJ)
Li et al. [28]	V2R	1700 bytes	1604 bytes	$3T_{ERSA} + 3T_{DRSA}$	116.691	1458.633
	V2V	820 bytes		$2T_{ERSA} + 2T_{DRSA}$	77.743	971.785
	V2V-RSU	2496 bytes		$4T_{ERSA} + 4T_{DRSA}$	155.486	1943.570
Liu et al. [30]	V2V-RSU-TA	1524 bytes	332 bytes	$2T_{BP} + 14T_{h(\cdot)} + 1T_{Exp} + 3T_{ERSA} + 2T_{DRSA}$	163.188	2039.850
Wu et al. [31]	V2V-RSU	892 bytes	912 bytes	$2T_{h(\cdot)} + 4T_{BP} + 9T_{ECMP}$	222.417	2780.215
Liu et al. [32]	V2R	284 bytes	164 bytes	$6T_{h(\cdot)} + 1T_{ECSM} + 1T_{BP} + 5T_{ECMP}$	75.641	945.514
Liu et al. [33]	V2R	780 bytes	716 bytes	$1T_{ERSA} + 1T_{DRSA} + 1T_{HMAC} + 6T_{h(\cdot)} + 1T_{BP} + 2T_{ECSM} + 10T_{ECMP}$	148.361	1854.509
Cui et al. [34]	V2V/V2R	548 bytes	332 bytes	$4T_{BP} + 29T_{ECMP}$	346.021	4325.260
MComIoV	V2V/V2R	104 bytes	816 bytes	$16T_{h(\cdot)}$	0.611	7.640
	V2R	136 bytes		$12T_{h(\cdot)} + 5T_{ECMP}$	31.378	392.230
	V2S	176 bytes		$15T_{h(\cdot)}$	0.573	7.163
	V2MD	176 bytes		$19T_{h(\cdot)}$	0.726	9.073
	V2I	176 bytes		$18T_{h(\cdot)}$	0.688	8.595

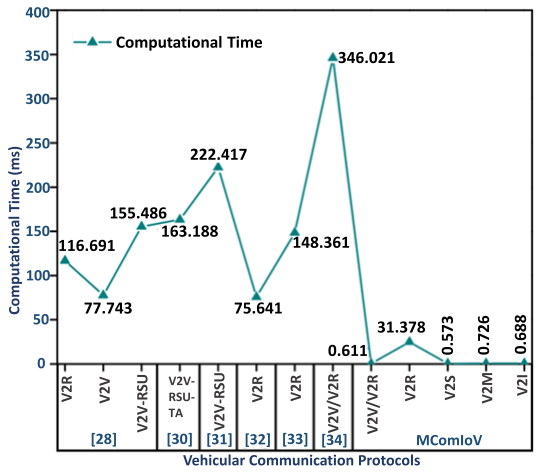

Fig. 7. Computation Time Comparison for Communication Schemes.

to Table III, we count the total computation time for each communication scheme, as compared in Fig. 7 and Table IV. The MComIoV offers all the five types of IoV communications directly, taking the less computation time.

B. Storage Cost and Communication Overhead

Both (sender and receiver) require some memory (in bytes) to transmit different types of parameters before establishing a connection for data exchanges, and it is called the communication overhead. Various parameters are stored in different devices (such as server, OBU, RSU, TPD, sensor, smart chip, and infrastructure) during the registration/setup phases, and the required memory is called as the storage cost. In general, the size of identity random value/user password, time-stamp, exponential (EXP), RSA (3072-bit key), and SHA-256 is 12 bytes, 8 bytes, 32 bytes, 384 bytes and 32 bytes respectively. Bi-linear pairing (BP) and EC multiplication (ECMP) individually need 64 bytes due to the size of $p = 256$ bits [41].

Considering the above number of bytes, we count the total number of required bytes based on the type of parameters for the communication overhead and the storage cost. These costs are calculated for [28], [30]–[34], and MComIoV, as described in Table IV.

- The communication overhead is 1700 bytes (for V2R in [28]), 820 bytes (for V2V in [28]), 2496 bytes (for V2V-RSU in [28]), 1524 bytes (in [30]), 892 bytes (in [31]), 284 bytes (in [32]), 780 bytes (in [33]), and 548 bytes (in [34]). However, the MComIoV needs 104 bytes (for V2V), 136 bytes (for V2R), 176 bytes (for V2S, V2M, and V2I separately).
- The storage cost is 1604 bytes (in [28]), 332 bytes in [30], 912 bytes in [31], 164 bytes in [32], 716 bytes in [33], 332 bytes in [34], and 816 bytes in the MComIoV.

We observe that the MComIoV needs more number of bytes for the storage cost compared to [30], [32], [33], and [34], but it is one-time cost during the basic/registration phase. Thereby, it does not affect much in the communication protocol. However, the impact of the communication overhead is more, as it requires every time when both (sender and receiver) want to connect for data exchange. The communication cost is less in the MComIoV for all the five types of IoV communications compared to [28], [30]–[33], and [34].

C. Energy Consumption

The protocol consumes energy during the communication phase, and it is totally dependent on the computation time. The energy consumption is computed as $E_C = P_{CPU} * T_{COMP}$, and measured in millijoule (mJ), where P_{CPU} = the maximum CPU power, and T_{COMP} = computation time [42]. P_{CPU} is 12.5 W (V_{INPUT} = 5 V and S_{POWER} = 2.5 Amp) for Raspberry Pi 3B+ model [39]. The registration/setup phase is performed once for all IoV devices. However, IoV communications are routinely practiced to transmit pertinent information. Thus, the energy consumption of all IoV communication phases are more worthwhile for energy-efficient communication system. Considering this CPU power and above E_C formula, we calculate the energy consumption of all communication phases for [28], [30]–[34], and MComIoV, as compared in Table IV.

VII. CONCLUSION

We have proposed new communication protocols using ECC and SHA256 for reliable direct V2V, V2R, V2S, V2M,

and V2I communications in a public network. The security evaluation shows that the MComIoV fulfills different security and user privacy requirements and resists critical attacks for vehicular communications, such as impersonation, Sybil, modification, man-in-the-middle, replay, session key disclosure, and password guessing. Our experimental results show on the test-bed implementation that the MComIoV not only satisfies security and privacy, but it is also proven to be efficient comparatively in communication overhead, storage cost, computation time, and energy consumption.

Based on security and privacy robustness as well as experimental results, the MComIoV will provide a platform to exchange vital information on the road between a vehicle and other IoV components directly, assuring authenticity, anonymity, confidentiality, and integrity in the IoV system. Consequently, it creates a new source of data to generate revenue, involving different stakeholders for modern smart city applications. Our future work is to design new secure and efficient IoV communication protocols, improving security strengths to withstand new side-channel attacks.

ACKNOWLEDGMENT

The authors would like to thank the Associate Editor and anonymous reviewers for constructive comments that helped to improve the quality of the manuscript significantly.

REFERENCES

[1] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the united states," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.

[2] G. Karagiannis *et al.*, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 584–616, 4th Quart., 2011.

[3] H. Hartenstein and L. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 6, pp. 164–171, Jun. 2008.

[4] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *J. Netw. Comput. Appl.*, vol. 37, pp. 380–392, Jan. 2014.

[5] (2018). *WHO: Global Status Report on Road Safety*. Available online:. [Online]. Available: https://www.who.int/publications-detail/global-status-report-on-road-safety-2018

[6] U. Desa, "World urbanization prospects: The 2011 revision," *United Nations, Department of Economic and Social Affairs*. New York, NY, USA: Population Division, 2012.

[7] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of DSRC and cellular network technologies for V2X communications: A survey," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9457–9470, Dec. 2016.

[8] S. Chen, J. Hu, Y. Shi, and L. Zhao, "LTE-V: A TD-LTE-based V2X solution for future vehicular network," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 997–1005, Dec. 2016.

[9] Z. MacHardy, A. Khan, K. Obana, and S. Iwashina, "V2X access technologies: Regulation, research, and remaining challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1858–1877, 3rd Quart., 2018.

[10] H. Zhou, W. Xu, J. Chen, and W. Wang, "Evolutionary V2X technologies toward the Internet of vehicles: Challenges and opportunities," *Proc. IEEE*, vol. 108, no. 2, pp. 308–323, Feb. 2020.

[11] O. Kaiwartya *et al.*, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[12] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero Ibáñez, "A seven-layered model architecture for Internet of vehicles," *J. Inf. Telecommun.*, vol. 1, no. 1, pp. 4–22, Jan. 2017.

[13] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibanez, "Internet of vehicles: Architecture, protocols, and security," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3701–3709, Oct. 2018.

[14] M. M. Gerla and E. K. G. U. Lee Pau Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in *Proc. IEEE World Forum Internet Things*, Mar. 2014, pp. 241–246.

[15] McKinsey. (2015). *Unlocking the Potential of the Internet of Things*. [Online]. Available: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

[16] A. Mai and D. Schlesinger, "A business case for connecting vehicles executive summary," Cisco Internet Bus. Solutions Group, San Jose, CA, USA, Tech. Rep., Apr. 2011, pp. 1–15.

[17] A. Ghosal and M. Conti, "Security issues and challenges in V2X: A survey," *Comput. Netw.*, vol. 169, Dec. 2020, Art. no. 107093.

[18] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, Nov. 2014.

[19] *IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages*, Standard 1609.2-2016 Revision IEEE Std 1609.2-2013, Mar. 2016, pp. 1–240.

[20] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Veh. Commun.*, vol. 9, pp. 19–30, Jul. 2017.

[21] Y. Sun *et al.*, "Attacks and countermeasures in the Internet of vehicles," *Ann. Telecommun.*, vol. 72, nos. 5–6, 283-295, 2017.

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

[23] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 289–299, Aug. 2014.

[24] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, 2007.

[25] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Secur. Privacy Mag.*, vol. 2, no. 3, pp. 49–55, May 2004.

[26] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in *Proc. IEEE Int. Conf. Commun.*, 2008, pp. 1451–1457.

[27] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 616–629, Mar. 2011.

[28] 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.

[29] 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.

[30] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure V2 V communications in an IoV paradigm," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2740–2749, Oct. 2017.

[31] H.-T. Wu and G.-J. Horng, "Establishing an intelligent transportation system with a network security mechanism in an Internet of vehicle environment," *IEEE Access*, vol. 5, pp. 19239–19247, 2017.

[32] 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.

[33] J. Liu, Q. Li, R. Sun, X. Du, and M. Guizani, "An efficient anonymous authentication scheme for Internet of vehicles," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.

[34] H. Cui, R. H. Deng, and G. Wang, "An attribute-based framework for secure communications in vehicular ad hoc networks," *IEEE/ACM Trans. Netw.*, vol. 27, no. 2, pp. 721–733, Apr. 2019.

[35] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. IACR Annu. Int. Cryptol. Conf. (CRYPTO)*, 1999, pp. 388–397.

[36] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.

[37] R. Madhusudhan and R. C. Mittal, "Dynamic ID-based remote user password authentication schemes using smart cards: A review," *J. Netw. Comput. Appl.*, vol. 35, no. 4, pp. 1235–1248, Jul. 2012.

[38] V. S. Miller, "Use of elliptic curves in cryptography," in *Proc. Adv. Cryptol.*, 1986, pp. 417–426.

[39] (Jul. 2019). *Raspberry Pi 3 Model B+*. [Online]. Available: https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/

[40] D. Zelle, C. Krauß, H. Strauß, and K. Schmidt, "On using TLS to secure in-vehicle networks," in *Proc. 12th Int. Conf. Availability, Rel. Secur.*, Aug. 2017, pp. 1–10.

[41] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.

[42] D. He, C. Chen, S. Chan, and J. Bu, "Secure and efficient handover authentication based on bilinear pairing functions," *IEEE Trans. Wireless Commun.*, vol. 11, no. 1, pp. 48–53, Jan. 2012.

Trupil Limbasiya (Student Member, IEEE) is currently the Ph.D. Research Scholar with the Department of Computer Science and Information Systems, Birla Institute of Technology and Science (BITS) Pilani, K. K. Birla Goa Campus, India. He has published multiple research articles in peer-reviewed international journals and well-known international conferences. His research interests include cryptography, information security, network security, and smart city applications.

Debasis Das (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from the Indian Institute of Technology (IIT) Patna, India. He joined as an Assistant Professor at the Department of Computer Science and Engineering, IIT Jodhpur, India. In 2019 before that, he worked as an Assistant Professor with the BITS Pilani, K. K. Birla Goa Campus, India, and NIIT University, India. His research interests include VANETs, smart cities, lightweight cryptography, Internet of Vehicles, blockchain, and network security.

Sajal K. Das (Fellow, IEEE) is currently a Professor of Computer Science and the Daniel St. Clair Endowed Chair with the Missouri University of Science and Technology. His research interests include wireless sensor networks, mobile and pervasive computing, cyber-physical systems and IoT, smart environments, cloud computing, cyber security, and social networks. He also serves as the founding Editor-in-Chief for Elsevier's *Pervasive and Mobile Computing* journal, and as an Associate Editor for the IEEE TRANSACTIONS OF MOBILE COMPUTING, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, and *ACM Transactions on Sensor Networks*.