Hindawi
Security and Communication Networks
Volume 2021, Article ID 5554318, 9 pages
https://doi.org/10.1155/2021/5554318

Research Article

Designing an Efficient and Secure Message Exchange Protocol for Internet of Vehicles

Shehzad Ashraf Chaudhry

Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey

Correspondence should be addressed to Shehzad Ashraf Chaudhry; sashraf@gelisim.edu.tr

Received 28 February 2021; Accepted 8 May 2021; Published 19 May 2021

Academic Editor: Prosanta Gope

In the advancements in computation and communication technologies and increasing number of vehicles, the concept of Internet of Vehicles (IoV) has emerged as an integral part of daily life, and it can be used to acquire vehicle related information including road congestion, road description, vehicle location, and speed. Such information is very vital and can benefit in a variety of ways, including route selection. However, without proper security measures, the information transmission among entities of IoV can be exposed and used for wicked intentions. Recently, many authentication schemes were proposed, but most of those authentication schemes are prone to insecurities or suffer from heavy communication and computation costs. Therefore, a secure message authentication protocol is proposed in this study for information exchange among entities of IoV (SMEP-IoV). Based on secure symmetric lightweight hash functions and encryption operations, the proposed SMEP-IoV meets IoV security and performance requirements. For formal security analysis of the proposed SMEP-IoV, BAN logic is used. The performance comparisons show that the SMEP-IoV is lightweight and completes the authentication process in just 0.198 ms.

1. Introduction

The Internet of Vehicles (IoV) is a self-organized network of vehicles on the road and the road side units (RSUs). The IoV provides intervehicles (V2V) and vehicles to RSUs (V2R) communication infrastructure [1], which can benefit in many ways including the information relating to road congestion/traffic issues, parking information, alternative routes, and warnings of potential accidents. Using the information, the drivers can quickly make decisions relating to vehicles and/or road/s. It can further help the unmanned vehicles regarding the accuracy and safety through the use of more sophisticated information and artificial intelligence techniques. The information exchanged or the communication among entities of IoV is always through public wireless channel, which makes it prone to several attacks. An attacker can easily listen and extract the meaningful information from the exchanged messages. Such information can be very crucial for the accuracy and safety of the vehicles in an IoV. The attacker can replay an old message or can inject a message with total fake information, and it can cause some severe consequences on the vehicles and the riders including the accidents. Moreover, the listened information can be used by an attacker to trace/track a vehicle/rider, and such information can be used for criminal/terrorism purposes. The information can also be faked for marketing purposes to gain attraction of the riders, while they are attracted to a specific route through false information of traffic as well as to compete for the parking lots [2].

Therefore, the security and privacy of the entire IoV including the communicating entities have more importance than all other factors. The goal can be achieved through authentication of the entities including vehicles before initiation of the communication among the entities of IoV. In this study, we proposed a lightweight symmetric key-based authentication scheme to secure message exchange among the entities of the IoV. We organize rest of the study as follows: Table 1 provides the notation guide. In Subsection

Table 1: Notations guide.

Symbols	Representations
VS, V_i	Vehicle server, vehicle
RSU_j	Road side unit
ID_{vi}, ID_{rj}	ID's of V_i and RSU_j
K_{VS}	Master secret key of VS
K_{rj}	Shared key among RSU_j and V_i
t_x, r_s	Timestamp and random number of entity x
PID_{vi}	Pseudoidentity of V_i
$H(a), \|$	Hash of a and concatenation

1.1, the system model is described. The motivations and contributions of the study are explained in Subsection 1.2, while the Subsection 1.3 discusses the adopted adversarial model. The Section 2 summarizes the existing related literature; whereas, our proposed secure message exchange protocol for IoV (SMEP-IoV) scheme is explained in Section 3. Using BAN logic, the Section 4 formally proves the security of the SMEP-IoV. In Section 5, a discussion on functional security and attack resilience of the proposed SMEP-IoV is given. Security and performance comparisons of the proposed SMEP-IoV with related schemes are given in Section 6. The study is concluded finally in Section 7.

1.1. System Model. Figure 1 shows a typical IoV scenario. It consists of vehicles, each having installed a processing unit called on-board unit, which is responsible for communication and processing of exchanged data among the vehicle and other entities of an IoV. Along with vehicles, there are road side units (RSUs), which are the infrastructure deployed on the road. Typically, communication is performed among vehicles and nearby RSU. Moreover, inter-vehicle communication is also an important component of the IoV. The whole network is administered by a trusted authority called vehicle server (VS). All the vehicles and related entities (RSUs) join the IoV by registering with VS. After getting registered with VS, the two entities can communicate with each other, for which both have to authenticate each other, and the authentication ensures that both communicating entities are legitimate.

1.2. Motivation and Contributions. Recently, many authentication schemes are proposed to secure message exchange among the entities of an IoV. However, many authentication schemes for IoV lack the required security features and resistance to known attacks. In this connection, Yu et al. proved some of the weaknesses of the scheme of Vasudev et al. Yu et al. further claimed to propose a secure authentication scheme with all required security features. The arguments in preceding section of this study refute their claim and the proof relating to several insecurities of Yu et al.'s scheme calls for an authentication scheme with all required security features.

The contributions of this study are many folds:

(i) Initially, we unveiled that the insecurities of the IoV authentication scheme proposed by Yu et al. We then proposed a robust authentication scheme using symmetric key-based encryption and hash functions.

(ii) The security of the proposed scheme is proved using formal RoR.

(iii) The comparative study with respect to efficiency and security among proposed and several existing studies is also provided in this study.

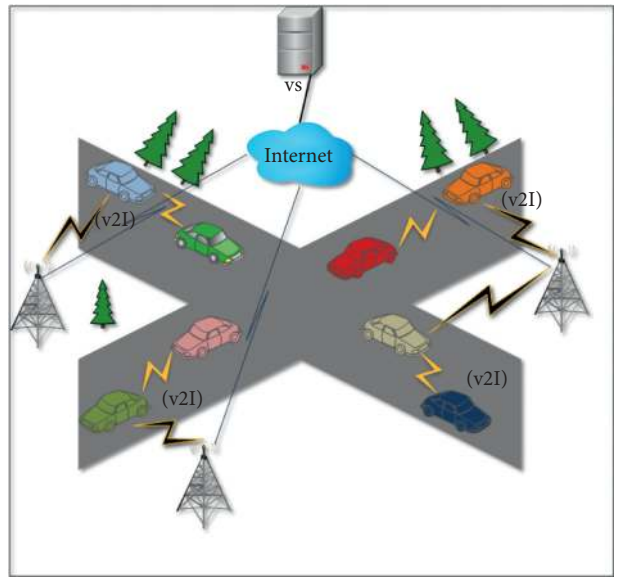

Figure 1: Typical IoV scenario.

1.3. Attack Model. We have taken into consideration the eCK adversary model [3], with strong adversary as compared with DY [4] and CK [5] models. The eCK is an extension of the CK model with a more strong adversary having capabilities to launch a key compromise impersonation attack in addition to controlling the communication channel, launching the power analysis to extract secrets stored in the smart card and access to all public parameters [6,7].

2. Related Literature

In their survey, Contreras-Castillo et al. [8] pointed out some security requirements and suggested to address authentication, integrity, confidentiality, and related security requirement before the IoV gain popularity. Some future directions were also discussed in [8]. In addition to the mentioned security requirements in [8], Mokhtar and Azab [9] stressed vehicle privacy, untraceability, access control, and resistance against tempering/forgery and jamming attacks.

In recent times, some authentication schemes were proposed [10–13]. Two different schemes were proposed by Lin et al. [14] and Yin et al. [15] using hashchains. Both schemes provided efficient and rapid authentication but lacked vehicle/user anonymity. The absence of anonymity could lead towards the leakage of sensitive vehicle/user

information, IoV. In 2015, the scheme of Li et al. [16] was proved to have weaknesses against disclosure of session key attack by Dua et al. [17]. Afterwards in 2016, Wang et al. also proposed a smartcard-based two-factor authentication scheme for IoV [18], which was proved as having weaknesses against many attacks including vehicle/user forgery and smart card stolen attacks, and the scheme was also lacking anonymity by Amin et al. [19]. A pairing-based scheme was also proposed by Liu et al. [20]. However, due to usage of expensive pairing operations, a considerable delay can happen, which is unsuitable for fast moving vehicles. Another lightweight scheme was proposed by Ying et al. [21]. However, Chen et al. [2] found critical weaknesses in the scheme of Ying et al. Due to usage of modular exponentiation, the scheme of Chen et al. entails inefficiencies against storage, communication cost, and computation time. Quite recently, in 2020, Vasudev et al. [22] presented another efficient authentication scheme. In 2020, Yu et al. [23] pointed out that the scheme of Vasudev et al. lacks mutual authentication and has weaknesses against some attacks including session key disclosure and vehicle/user forgery attacks. Yu et al. also proposed an improved scheme. However, the scheme of Yu et al. is prone to many attacks including disclosure of master secret key K_{VS} of the vehicle server. Due to leakage of K_{VS}, the scheme of Yu et al. cannot be deployed in any environment because if an attacker is able to get K_{VS}, it can generate secret parameters for any of the existing device to impersonate on behalf of that device; moreover, the attacker can register and deploy fake vehicles in the system. Any registered device can compute K_{VS} using the Q_i stored in the smartcard and its own password and identity related parameters, i.e., RPW_i and RID_i. For this, a vehicle/user V_i computes enters password (PW_{Ai}), identity (ID_{Ai}), and computes $\mathrm{RID}_i = h(\mathrm{ID}_{Ai} \| \mathrm{PW}_{Ai})$, $\mathrm{RN}_i = E_i \oplus h(\mathrm{PW}_{Ai} \| \mathrm{RID}_i)$ and $\mathrm{RPW}_i = h(\mathrm{PW}_{Ai} \| \mathrm{RN}_i)$. The V_i now computes $K_{\mathrm{VS}} = Q_i \oplus h(\mathrm{RID}_i \| \mathrm{RPW}_i)$. Here, K_{VS} is the master secret key of the vehicle server. Now, using K_{VS}, any dishonest vehicle of the system can launch any attack on any devices. For example,

(i) The dishonest vehicle with extracted K_{VS} can disclose any session key shared among two vehicles. Let V_x initiates a login request by sending $\{M_{i1}, M_{i2}, M_{\mathrm{AE}}, T_1\}$. By just listening to the request, the dishonest vehicle using M_{i1}, M_{i2}, and T_1 can compute $R_1 = M_{i1} \oplus h(K_{\mathrm{VS}} \| T_1)$ and $M_{\mathrm{request1}} = M_{i2} \oplus h(R_1 \| K_{\mathrm{VS}})$, on the fly. Similarly, when the responding vehicle V_y sends reply message $\{M_3, M_{\mathrm{EA}}, T_2\}$, the dishonest vehicle using M_3 and T_2 can compute $(M_{\mathrm{request2}} \| R_2)$ and the session key $\mathrm{SK} = h(R_1 \| R_2 \| K_{\mathrm{VS}})$ by just executing instep two hash functions on the public parameters.

(ii) Likewise, the dishonest device can launch man in middle, impersonation, and all related attacks using K_{VS}. For example, when V_x sends request message $\{M_{i1}, M_{i2}, M_{\mathrm{AE}}, T_1\}$ to V_y, the dishonest vehicle can extract R_1 and then can generate another valid response message $\{M_3, M_{\mathrm{AE}}, T_2\}$ by using K_{SV} and current timestamp. Ultimately, the possession of K_{SV} enables a dishonest vehicle to generate a valid request and a response message, and it can act like a man in middle.

3. Proposed SMEP-IoV

The proposed secure message exchange protocol for IoV (SMEP-IoV) consists of four phases. Table 1 provides the notation guide to understand the technical details of the proposed SMEP-IoV, briefed in following subsections:

3.1. SMEP-IoV: Initialization. The vehicle server (VS) selects its secret key K_{vs}, a one way hash function $H: \{0,1\}^* \longrightarrow \{0,1\}^l$ and a symmetric encryption/decryption function $X = E_k(Y)$.

3.2. SMEP-IoV: RSU Registration. During this phase, VS registers all road side units by assigning a unique identity ID_{rj} and a shared secret key $K_{rj} = h(\mathrm{ID}_{rj} \| K_{\mathrm{VS}})$. The VS stores ID_{rj} in its database.

3.3. SMEP-IoV: Vehicle Registration. During this phase, VS registers all vehicles by assigning a unique identity ID_{vi}. Moreover, VS computes $A_{vi} = h(K_{\mathrm{VS}} \| \mathrm{ID}_{vi})$, $\mathrm{PID}_{vi} = E_{K_{\mathrm{VS}}}(\mathrm{ID}_{vi} \| r_i 0)$, and $B_{vi} = h(\mathrm{PID}_{vi} \| K_{\mathrm{VS}})$. The VS stores ID_{vi}, PID_{vi}, A_{vi}, and B_{vi} in the memory of the vehicle V_i. Furthermore, the VS stores ID_{vi} in its own memory. Please note, except ID_{vi}, the VS does not store any other parameter relating to a vehicle say V_i. Specifically, PID_{vi}, A_{vi}, and B_{vi} are not stored in the memory of VS.

3.4. SMEP-IoV: Message Authentication. For message authentication, the vehicle V_i initiates the following steps with RSU_j and vehicle server VS, the in-sequence steps as shown in Figure 2:

3.4.1. PMA 1.

$$V_i \longrightarrow \mathrm{RSU}_j\colon M_{vi} = \{\mathrm{PID}_{vi}, M_{i1}, M_{i2}, t_i\}, \tag{1}$$

where V_i initiates the message authentication process by generating fresh timestamp t_i and a random number r_i. V_i further computes $M_{i1} = h(A_{vi} \| \mathrm{ID}_{vi} \| t_i \| r_i)$ and $M_{i2} = r_i \oplus B_{vi}$. V_i finalizes these steps by sending $M_{vi} = \{\mathrm{PID}_{vi}, M_{i1}, M_{i2}, t_i\}$ to RSU_j.

3.4.2. PMA 2.

$$\mathrm{RSU}_j \longrightarrow \mathrm{VS}\colon M_{rj1} = \{\mathrm{ID}_{rj}, M_{vi}, M_{j1}, t_j\} \tag{2}$$

On receiving $M_{vi} = \{\mathrm{PID}_{vi}, M_{i1}, M_{i2}, t_i\}$, the RSU_j checks the freshness of t_i by comparing it with current timestamp; if the delay is not within a predefined tolerable range ΔT, the RSU_j terminates the process; otherwise, RSU_j generates new timestamp t_j and a random number r_j. Moreover, RSU_j computes $M_{j1} = E_{K_{rj}}(r_j, t_j)$ and sends $M_{rj1} = \{\mathrm{ID}_{rj}, M_{vi}, M_{j1}, t_j\}$ to VS.

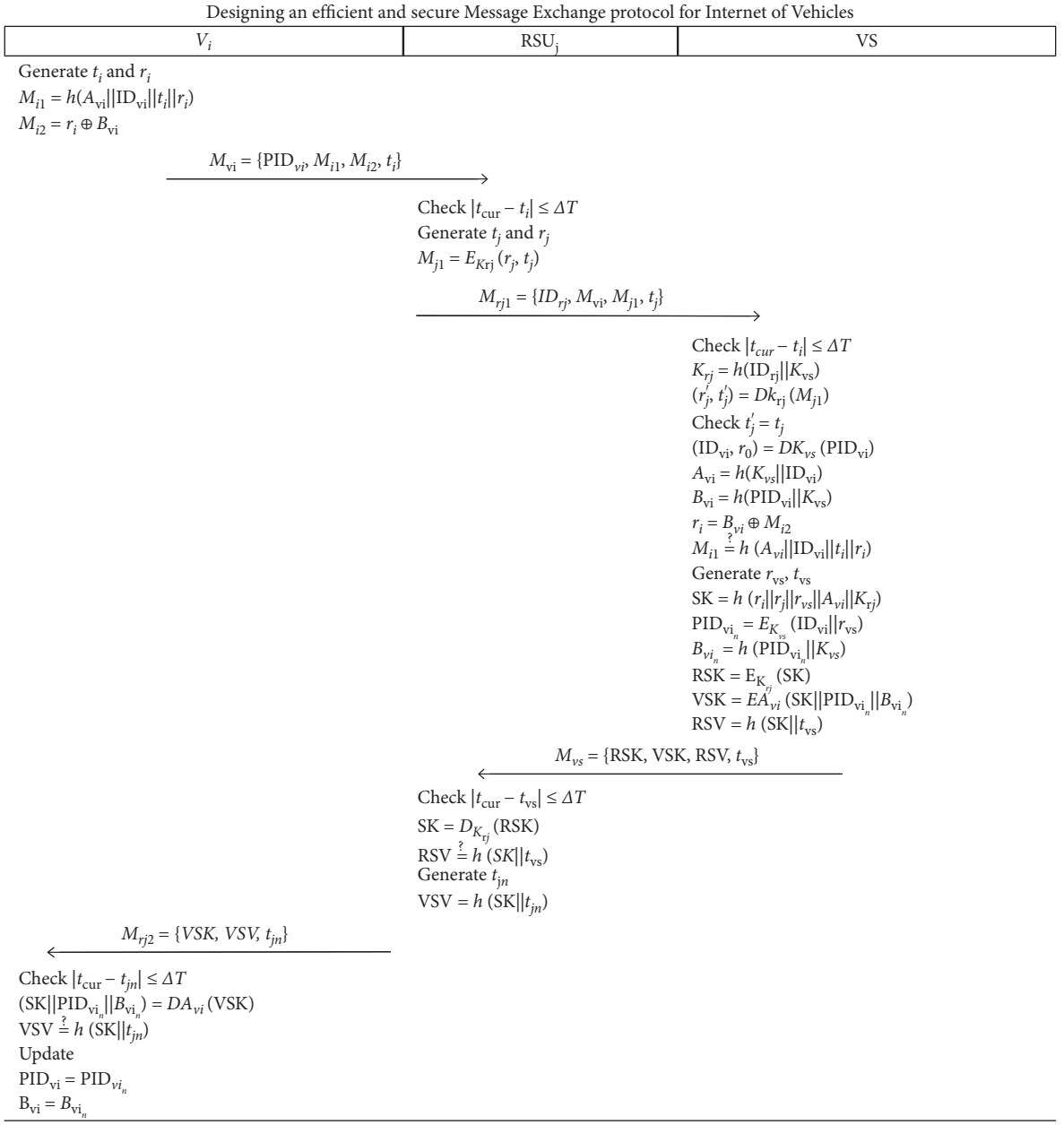

Figure 2: Proposed SMEP-IoV.

3.4.3. PMA 3.

$$VS \longrightarrow \text{RSU}_j\colon M_{vs} = \{\text{RSK}, \text{VSK}, \text{RSV}, t_{vs}\} \quad (3)$$

After receiving $M_{rj1} = \{\text{ID}_{rj}, M_{vi}, M_{j1}, t_j\}$, the VS checks the freshness of t_j by comparing it with current timestamp; if the delay is not within a predefined tolerable range ΔT, the VS terminates the process; otherwise, VS computes $K_{rj} = h(\text{ID}_{rj}\|K_{\text{VS}})$ and decrypts M_{j1} using K_{rj} to obtain the pair (r_j', t_j'). The VS also verifies the sameness of received t_j with decrypted t_j', and in case both are same, the VS using its secret key K_{vs} decrypts PID_{vi} and obtains (ID_{vi}, r_0). Now, the VS computes $A_{vi} = h(K_{\text{vs}}\|\text{ID}_{vi})$ and $B_{vi} = h(\text{PID}_{vi}\|K_{\text{vs}})$ and gets $r_i = B_{vi} \oplus M_{i2}$. After that, the VS checks $M_{i1} \stackrel{?}{=} h(A_{vi}\|\text{ID}_{vi}\|t_i\|r_i)$, and if verification is successful, the VS generates timestamp t_{vs} and a random number r_{vs}. The VS computes session key $\text{SK} = h(r_i\|r_j\|r_{vs}\|A_{vi}\|K_{rj})$, $\text{PID}_{vi_n} = E_{K_{\text{vs}}}(\text{ID}_{vi}\|r_{\text{vs}})$, $B_{vi_n} = h(\text{PID}_{vi_n}\|K_{\text{vs}})$, and $\text{RSK} = E_{K_{rj}}(\text{SK})$. In addition, the VS computes $\text{VSK} = E_{A_{vi}}(\text{SK}\|\text{PID}_{vi_n}\|B_{vi_n})$ and $\text{RSV} = h(\text{SK}\|t_{\text{vs}})$. Now, the VS sends $M_{\text{vs}} = \{\text{RSK}, \text{VSK}, \text{RSV}, t_{\text{vs}}\}$ to RSU_j.

3.4.4. PMA 4.

$$\text{RSU}_j \longrightarrow V_i\colon M_{rj2} = \{\text{VSK}, \text{VSV}, t_{j_n}\}. \quad (4)$$

After receiving $M_{\text{vs}} = \{\text{RSK}, \text{VSK}, \text{RSV}, t_{\text{vs}}\}$, the RSU_j checks the freshness of t_{vs} by comparing it with current timestamp; if the delay is not within a predefined tolerable range ΔT, the RSU_j terminates the process; otherwise, RSU_j

computes session key $SK = D_{K_{rj}}(RSK)$. Now, RSU_j checks the session key verifier $RSV \stackrel{?}{=} h(SK \| t_{vs})$, and if RSV is verified successfully, the RSU_j accepts the session key. Now, RSU_j generates new timestamp t_{j_n} and session key verifier $VSV = h(SK \| t_{j_n})$ for V_i. After that, the RSU_j sends $M_{rj2} = \{VSK, VSV, t_{j_n}\}$ to V_i.

3.4.5. PMA 5. After receiving $M_{rj2} = \{VSK, VSV, t_{j_n}\}$, the V_i checks the freshness of t_{j_n} by comparing it with current timestamp; if the delay is not within a predefined tolerable range ΔT, the V_i terminates the process; otherwise, V_i decrypts VSK using A_{vi} and obtains $(SK \| PID_{vi_n} \| B_{vi_n})$. Now, V_i checks the session key verifier $VSV \stackrel{?}{=} h(SK \| t_{j_n})$, and if VSV is verified successfully, the V_i accepts the session key and updates $PID_{vi} = PID_{vi_n}$ and $B_{vi} = B_{vi_n}$.

4. Formal Security Analysis through BAN

The Burrows–Abadi–Needham (BAN) logic analysis is performed to test the protocol from various security aspects with a focus on mutual key agreement, key sharing, and protection from exposure to session key. We used the following symbolic tokens to perform this analysis.

(i) $L| \equiv \overline{w}$: L believes $\overline{w}$
(ii) $L \triangleleft \overline{w}$: L sees $\overline{w}$
(iii) $L| \sim \overline{w}$: L once said $\overline{w}$, some time ago
(iv) $L| \Rightarrow \overline{w}$: L has got the entire jurisdiction over $\overline{w}$
(v) (#bar$w$): the message $\overline{w}$ is fresh
(vi) $(L)\overline{w}$: L is used in formulae with $\overline{w}$
(vii) $(\overline{w}, \overline{w}')_k$: $\overline{w}$ or $\overline{w}'$ is symmetrically encrypted with key K
(viii) $\{\overline{w}, \overline{w}'\}_k$: $\overline{w}$ or $\overline{w}'$ is hashed with key K
(ix) $\{L, \overline{w}\}_k$: K is used in formula with $\overline{w}$ and L
(x) $LK \leftrightarrow L'$: L communicates with the key K

The following BAN logic rules are used to verify the security features:

Rule 1. Message meaning.

$$\frac{L| \equiv LK \leftrightarrow L', L \triangleleft < \overline{w} >_{\overline{w}}}{L| \equiv L| \sim \overline{w}}. \tag{5}$$

Rule 2. Nonce verification.

$$\frac{L| \equiv \#(\overline{w}), L| \equiv L'| \sim \overline{w}}{L| \equiv L'| \equiv \overline{w}}. \tag{6}$$

Rule 3. Jurisdiction.

$$\frac{L| \equiv L' \Rightarrow \overline{w}, L| \equiv L'| \equiv \overline{w}}{L| \equiv \overline{w}}. \tag{7}$$

Rule 4. Freshness conjunction.

$$\frac{L| \equiv \#(\overline{w})}{L| \equiv \#(\overline{w}, \overline{w}')}. \tag{8}$$

Rule 5. Belief rule.

$$\frac{L| \equiv (\overline{w}), L| \equiv (\overline{w}')}{L| \equiv (\overline{w}, \overline{w}')}. \tag{9}$$

Rule 6. Session key.

$$\frac{L| \equiv \#(\overline{w}), L| \equiv L' \equiv \overline{w}}{L| \equiv LK \leftrightarrow L'}. \tag{10}$$

Corresponding with the above rules and assumptions, we accomplish the following goals in the BAN logic analysis. The symbols used here, i.e., (g, RSU_j, V_i, V_s), represent the goal, road side unit, vehicle, and vehicle server.

(i) G1: $RSU_j| \equiv (RSU_j \overset{SK}{\leftrightarrow} V_s)$
(ii) G2: $RSU_i| \equiv V_s| \equiv (RSU_i \overset{SK}{\leftrightarrow} V_s)$
(iii) G3: $V_i| \equiv (RSU_j \overset{SK}{\leftrightarrow} V_i)$
(iv) G4: $V_i| \equiv RSU_j| \equiv (RSU_j \overset{SK}{\leftrightarrow} V_i)$
(v) G5: $V_s| \equiv (V_i \overset{SK}{\leftrightarrow} V_s)$
(vi) G6: $V_s| \equiv (V_i \overset{SK}{\leftrightarrow} V_i)$

Initially, the communication contents must be adapted into idealized form as shown in the following:

(i) M1: $V_i \longrightarrow RSU_j$: $PID_{vi}, M_{i1}, M_{i2}, t_i$: $\{PID_{vi}, ID_{vi}, t_i, (r_i)_{Bvi}, t_i\}$
(ii) M2: $RSU_j \longrightarrow V_s$: $ID_{rj}, PID_{vi}, \langle ID_{vi}, t_i, r_{iAvi} \rangle, \langle ri_{Bvi} \rangle, t_i, M_{j1}, t_j$: $\{ID_{rj}, PID_{vi}, \langle ID_{vi}, t_i, r_{iAvi} \rangle, (r_i)_{Bvi}, t_i, \{r_j, t_j\}_{Krj}, t_j\}$
(iii) M3: $V_s \longrightarrow RSU_j$: RSK, VSK, RSV, t_{vs}: $\{(SK)_{Krj}, \{SK, PID_{vin}, B_{vin}\}_{Avi}, (tvs)_{SK}, t_{vs}\}$
(iv) M4: $RSU_s \longrightarrow V_i$: VSK, VSV, T_{jn}: $\{\{SK, PID_{vin}\}_{Avi}, (t_{jn})_{SK}, t_{jn}\}$

Furthermore, we take the following assumptions to support the security proof.

(i) $B1$: $V_i| \equiv \#(t_i)$
(ii) $B2$: $RSU_j| \equiv \#t_j, t_{jn}$
(iii) $B3$: $V_s| \equiv \#t_{vs}$
(iv) $B4$: $V_i| \equiv (V_i A_{vi} \leftrightarrow V_s)$
(v) $B5$: $V_i| \equiv (V_i \overset{SK \| t_{jn}}{\leftrightarrow} RSU_j)$
(vi) $B6$: $RSU_J| \equiv (RSU_j \overset{SK \| t_{jn}}{\leftrightarrow} V_i)$
(vii) $B7$: $RSU_j| \equiv RSU_j \overset{K_{rj}}{\leftrightarrow} RSU_j$
(viii) $B8$: $V_s| \equiv (V_s A_{vi} \leftrightarrow V_i)$
(ix) $B9$: $V_s| \equiv V_s \overset{K_{rj}}{\leftrightarrow} RSU_j$
(x) $B10$: $V_i| \equiv RSU_j| \equiv V_i \overset{SK}{\leftrightarrow} RSU_j$
(xi) $B11$: $RSU_j| \equiv V_i| \equiv V_i \overset{SK}{\leftrightarrow} RSU_j$

(xii) $B12$: $V_s| \equiv V_i| \equiv V_i \overset{SK}{\leftrightarrow} V_s$

(xiii) $B13$: $\text{RSU}_j| \equiv V_s| \equiv V_s \overset{SK}{\leftrightarrow} RSU_j$

(xiv) $B14$: $V_s| \equiv \text{RSU}_j| \equiv V_i \overset{SK}{\leftrightarrow} \text{RSU}_i$

(xv) $B15$: $V_i| \equiv V_s| \equiv V_i \overset{SK}{\leftrightarrow} \text{RSU}_j$

Next, employing the above assumptions, we further analyze the idealized forms.

Taking the idealized version of M1 and M2:

(i) M1: $V_i \longrightarrow \text{RSU}_j$: $\text{PID}_{vi}, M_{i1}, M_{i2}, t_i$: $\{\text{PID}_{vi}, \text{ID}_{vi}, t_i, (r_i)_{Bvi}, t_i\}$

(ii) M2: $\text{RSU}_j \longrightarrow V_s$: $\text{ID}_{rj}, \text{PID}_{vi}, \langle \text{ID}_{vi}, t_i, r_{iAvi} \rangle$, $\langle ri_{Bvi} \rangle, t_i$,

(iii) M_{j1}, t_j: $\{\text{ID}_{rj}, \text{PID}_{vi}, \langle \text{ID}_{vi}, t_i, r_{iAvi} \rangle, (r_i)_{Bvi}, t_i, \{r_j, t_j\}_{Krj}, t_j\}$

By applying seeing rule, we get

(i) $X1$: $\text{RSU}_j \triangleleft \{\text{PID}_{vi}, M_{i1}, M_{i2}, t_i$: $\{\text{PID}_{vi}, \text{ID}_{vi}, t_i, (r_i)_{Bvi}, t_i\}\}$

(ii) $X2$: $V_s \triangleleft \{\text{ID}_{rj}, \text{PID}_{vi}, \langle \text{ID}_{vi}, t_i, r_{i_{Avi}} \rangle, \langle ri_{Bvi} \rangle, t_i, M_{j1}, t_j$: $\{\text{ID}_{rj}, \text{PID}_{vi}, \langle \text{ID}_{vi}, t_i, r_{i_{Avi}} \rangle, (r_i)_{Bvi}, t_i, \{r_j, t_j\}_{Krj}, t_j\}\}$

According to $D1, D2, P8, B9$, and $R1$, we get

(i) $X3$: $V_s| \equiv V_i \sim \{\text{PID}_{vi}, \text{ID}_{vi}, t_i, (r_i)_{Bvi}, t_i\}$

(ii) $X4$: $V_s| \equiv \text{RSU}_j \sim \{\text{ID}_{rj}, \text{PID}_{vi}, \langle \text{ID}_{vi}, t_i, r_{i_{Avi}} \rangle, (r_i)_{Bvi}, t_i, \{r_j, t_j\}_{Krj}, t_j\}$

Referring to $X3, B1, R2$, and $R4$, we get

(i) $X5$: $V_s| \equiv V_i \equiv \{\text{PID}_{vi}, \text{ID}_{vi}, t_i, (r_i)_{Bvi}, t_i\}$

(ii) $X6$: $V_s| \equiv \text{RSU}_j \equiv \{\text{ID}_{rj}, \text{PID}_{vi}, \langle \text{ID}_{vi}, t_i, r_{i_{Avi}} \rangle, (r_i)_{Bvi}, t_i, \{r_j, t_j\}_{Krj}, t_j\}$

Referring to $X5, B12$, and $R3$,

(i) $X7$: $V_s| \equiv \{\text{PID}_{vi}, \text{ID}_{vi}, t_i, (r_i)_{Bvi}, t_i\}$

In accordance with $X6, B14$, and $R3$, we have

(i) $X8$: $V_s| \equiv \{\text{ID}_{rj}, \text{PID}_{vi}, \langle \text{ID}_{vi}, t_i, r_{i_{Avi}} \rangle, (r_i)_{Bvi}, t_i, \{r_j, t_j\}_{Krj}, t_j\}$

Referring to $X5, X7$, and $R6$, we have

(i) $X9$: $V_s| \equiv V_i \overset{SK}{\leftrightarrow} V_s$ (goal 5)

Using $X5, X7, B8$, and $R2$, we get

(i) $X10$: $V_s| \equiv V_i| \equiv V_i \overset{SK}{\leftrightarrow} V_s$ (goal 6)

Taking the idealized version of $M3$,

(i) $M3$: $V_s \longrightarrow \text{RSU}_j$: $\text{RSK}, \text{VSK}, \text{RSV}, t_{vs}$: $\{(\text{SK})_{Krj}, \{\text{SK}, \text{PID}_{vin}, B_{vin}\}_{Avi}, (\text{tvs})_{\text{SK}}, t_{vs}\}$

On the application of seeing rule for $M3$, we get

(i) $X11$: $V_s| \equiv V_i \sim \text{RSK}, \text{VSK}, \text{RSV}, t_{vs}$: $\{(\text{SK})_{Krj}, \{\text{SK}, \text{PID}_{vin}, B_{vin}\}_{Avi}, (\text{tvs})_{\text{SK}}, t_{vs}\}$

Using $X11, B7$, and $R1$, we have

(i) $X12$: $\text{RSU}_j| \equiv V_s \sim \{(\text{SK})_{Krj}, \{\text{SK}, \text{PID}_{vin}, B_{vin}\}_{Avi}, (tvs)_{\text{SK}}, t_{\text{vs}}\}$

(ii) $\text{RSU}_j| \equiv (\text{RSU}_j \overset{SK}{\leftrightarrow} V_s)$ (goal 1)

According to $X12, B3, B13, R2$, and $R4$, we have

(i) $X13$: $\text{RSU}_j| \equiv V_s | \equiv \{(\text{SK})_{Krj}, \{\text{SK}, \text{PID}_{vin}, \backslash\backslash B_{vin}\}_{Avi}, (tvs)_{\text{SK}}, t_{\text{vs}}\}$

(ii) $\text{RSU}_i| \equiv V_s| \equiv (\text{RSU}_i \overset{SK}{\leftrightarrow} V_s)$ (goal 2)

Next, considering $M4$ idealized form,

(i) M4: $\text{RSU}_s \longrightarrow V_i$: $\text{VSK}, \text{VSV}, T_{jn}$: $\{\{\text{SK}, \text{PID}_{vin}\}_{Avi}, (t_{jn})_{\text{SK}}, t_{jn}\}$

On the application of seeing rule for $M4$, we have

(i) $X14$: $V_i \triangleleft V_i$: $\text{VSK}, \text{VSV}, T_{jn}$: $\{\{\text{SK}, \text{PID}_{vin}\}_{Avi}, (t_{jn})_{\text{SK}}, t_{jn}\}$

While $X14, B4, B5$, and $R1$ imply

(i) $X15$: $V_i| \equiv RSU_j \sim \{\{\text{SK}, \text{PID}_{vin}\}_{Avi}, (t_{jn})_{\text{SK}}, t_{jn}\}$

Referring to $X15, B2, B3, R2$, and $R4$, we have

(i) $X16$: $V_i| \equiv \text{RSU}_j| \equiv \{\{\text{SK}, \text{PID}_{vin}\}_{Avi}, (t_{jn})_{\text{SK}}, t_{jn}\}$

From $X16, B4, B10, B15$, and rule 3, we get

(i) $X17$: $V_i| \equiv \{\{\text{SK}, \text{PID}_{vin}\}_{Avi}, (t_{jn})_{\text{SK}}, t_{jn}\}$

Referring to $X17$, we apply $R6$ as

(i) $X18$: $V_i| \equiv (\text{RSU}_j \overset{SK}{\leftrightarrow} V_i)$ (goal 3)

According to $X18, B2$, we apply the $R6$ as

(i) $X19$: $V_i| \equiv \text{RSU}_j| \equiv (\text{RSU}_j \overset{SK}{\leftrightarrow} V_i)$ (goal 3)

The discussed cases for proving the protocol in BAN logic make obvious that the contributed scheme entirely supports mutual authentication and protects the established session key among the three participating members.

5. Informal Security Analysis

An informal security discussion on the security features of the proposed scheme is provided in following subsection:

5.1. Mutual Authentication. The SMEP-IoV ensures mutual authenticity for all participating entities of the system. In particular, the RSU_j authenticates both entities, VS and V_i, by means of equality check comparing RSV against the computed $h(\text{SK} \| t_{\text{vs}})$ parameter. Since, RSU_j is aware of the fact, the generated session key SK can only be constructed by a legitimate VS entity having access to master secret key K_{vs}. Using K_{vs}, VS can access r_i, r_j, A_{vi}, and K_{rj} factors to compute a valid SK. Likewise, V_i authenticates RSU_j on the basis of VSV equality check, after comparing it with the computed $h(\text{SK} \| t_{jn})$. Similarly, Vs authenticates V_i by computing $h(A_{vi} \| \text{ID}_{vi} \| t_i \| r_i)$ against M_{i1}. Realizing the fact that A_{vi} is only held with a valid V_i entity, it can validate the

vehicle V_i. If these equality checks fail, the mutual authentication cannot be assured in the protocol.

5.2. Stolen Verifier Attack. In the proposed scheme, the vehicle server VS stores only public identities ($\{ID_{vi}: i = 1, 2 \ldots n\}$) of all the registered vehicles in its memory. VS does not store any other vehicle-related secret parameter in its own memory, and the verifier is with the vehicle. Therefore, the possibility of stolen verifier attack on proposed SMEP-IoV is negligible.

5.3. Vehicle Anonymity. The SMEP-IoV employs a pseudoidentity PID_{vi} for each vehicle, which is renewed and replaced after the termination of each session. In this manner, the vehicle or user remains anonymous during the execution of the protocol. Moreover, there is no desynchronization possible in case an adversary holds or blocks the message on its way.

5.4. VS Impersonation Attack. No adversary A can impersonate as Vs in the SMEP-IoV scheme. This is because, if an adversary attempts the same towards V_i, the latter may discern the possibility of attack by comparing VSV against the computed factor $h(SK\|t_{jn})$. Similarly, if A attempts to impersonate as VS against RSU_j, the RSU_j may successfully thwart this attack on the basis of comparison of RSV and calculated $h(SK\|t_{vs})$. Hence, the SMEP-IoV is immune to VS impersonation attack.

5.5. RSU Impersonation Attack. The SMEP-IoV is immune to RSU impersonation attack. Both entities V_i and VS may easily prevent any attempt of impersonation as RSU on the part of adversary. This is due to the fact that VS shares a secret with RSU_j. The use of fresh timestamps along with the shared secrets helps the VS entity in authenticating a legitimate RSU. Similarly, V_i authenticates RSU_j on account of the derived session key SK from the VSK message as submitted by a valid VS, which is further used in the later comparison of VSV. In this manner, both of the entities validate a legal RSU_j on account of provided logical comparison of equality checks.

5.6. Man-in-the-Middle Attack (MiDM). To launch a successful MiDM attack on SMEP-IoV, the adversary needs access to either the V_i registration parameters such as A_{vi} and B_{vi} or access to secret key K_{rj} or the master secret key K_{vs}. On the other hand, as we see earlier, it is less likely for an adversary to initiate an impersonation attack on the protocol.

5.7. Session Key Security. As we see earlier, no adversary could engage in the mutual authentication process until it gains access to secure credentials of the system either held by the registration authority or registered entities. Since, the SMEP-IoV provides mutual authentication to all participants, the established session key is only known to the legitimate members involved in the protocol execution.

5.8. Denial of Service. Our scheme is resistant to denial of service attacks, since it engages fresh timestamps for the generation of M_{vi} and M_{rj1}. Due to these timestamps, the receiving entity may check the freshness of the incoming message and discard the message immediately if the latency is beyond a certain preset threshold.

5.9. Replay Attack. In case an adversary attempts to initiate a replay attack towards any entity V_i, RSU_j, or VS, the SMEP-IoV may foil this attempt immediately after checking the freshness of timestamps t_i, t_j/t_{jn}, and t_{vs}, respectively. Hence our scheme is immune to this threat.

6. Performance and Security Comparisons

The performance and security comparisons of the proposed scheme with related existing scheme [22–24] are explained in the following subsections.

6.1. Performance Comparisons. For measuring the computation time and cost, Pi3 B+ is used with Cortex A53 (ARMv8) 64 bit SoC and with processing speed 1.4 GHz along with 1 GB LPDDR2 SDRAM RAM. The simulation results of basic operations executed over Pi3 are given in Table 2. For completion of authentication and a key agreement (AKA) among a vehicle V_i and RSU RSU_j through the intermediate agent VS-Vehicle Server, V_i executes $2C_{hs}$ and $3C_{ed}$ operations. Likewise, RSU_j performs $2C_{hs} + 2C_{ed}$ operations while VS accomplishes $7C_{hs}$ and $7C_{ed}$ operations. Hence, total computational operations performed to complete a cycle of AKA are $11C_{hs} + 12C_{ed}$. Using the experiment with computational times represented in Table 2, the performance comparisons are briefed in Table 3. The proposed scheme completes single AKA cycle in ≈0.198 ms. In contrast to the proposed scheme, the scheme of Yu et al. [23] completes single AKA cycle in ≈0.132 ms, the scheme of Vasudev et al. [22] and Mohit et al. [24] complete the one cycle of AKA in ≈0.082 ms and ≈0.108 ms, respectively.

For communication cost comparisons, subsequent consideration is taken as per the sizes of different parameters. Timestamps and identity are taken as 32 and 64 bits, respectively; whereas, the sizes of the outputs of the symmetric key and asymmetric key operations are taken as 128 and 1024 bits. The value of hash output is fixed at 160 bits. Moreover, the size of random numbers is also assumed as 160 bit of length. The communication cost of SMEP-IoV and related schemes of Yu et al. [23], Vasudev et al. [22], and Mohit et al. [24] is computed as the bits exchanged among the IoV entities. The V_i sends $M_{vi} = \{PID_{vi}, M_{i1}, M_{i2}, t_i\}$ to RSU_j, where the size of M_{vi} is $\{128 + 160 + 160 + 32\} = 480$. Subsequently, the RSU_j sends $M_{rj1} = \{ID_{rj}, M_{vi}, M_{j1}, t_j\}$, where the size of M_{rj} is $\{64 + 480 + 128 + 32\} = 704$. The VS replies RSU_j with $M_{vs} = \{RSK, VSK, RSV, t_{vs}\}$, where the

Table 2: Operational Cost of the primitives.

Operation	Notation	Time (ms)
Enc-decryption	C_{ed}	≈0.011
Hash function	C_{hs}	≈0.006

Table 3: Performance comparisons.

↓ protocols	C_a.	RT	C_b
Proposed	$11C_{hs} + 12C_{ed}$	≈0.198	2848
Yu et al. [23]	$22C_{hs}$	≈0.132	864
Vasudev et al. [22]	$10C_{hs} + 2C_{ed}$	≈0.082	800
Mohit et al. [24]	$18C_{hs}$	≈0.108	1760

Note: C_a, computation cost; RT, running time in ms; C_b, communication cost in bits.

Table 4: Security features.

Schemes	Our	[23]	[22]	[24]
Mutual authentication	✓	✗	✗	✓
Stolen verifier	✓	✓	✓	✓
Vehicle anonymity	✓	✗	✓	✓
VS impersonation	✓	✗	✗	✓
RSU impersonation	✓	✗	✗	✓
Vehicle impersonation	✓	✗	✗	✓
Man in middle attack	✓	✗	✗	✗
Session key security	✓	✗	✗	✓
Denial of service	✓	✓	✓	✓
Replay attack	✓	✓	✓	✓

Note: ✓, provides or resists; ✗,does not provide or does not resist.

size of M_{vs} is $\{256 + 512 + 160 + 32\} = 960$. The final message $M_{rj2} = \{VSK, VSV, t_{j_n}\}$ was sent from RSU_j to V_i, where the size of M_{rj2} is $\{512 + 160 + 32\} = 704$. Therefore, total communication cost is 2848 bits. The communication cost of Yu et al.'s scheme is 864, while the communication costs of Vasudev et al. and Mohit et al. are 800 and 1760, respectively.

6.2. Security Features. The security comparisons of the SMEP-IoV and related existing schemes [22–24] are provided in this subsection. Table 4 solicits the summary of the security comparisons. Due to disclosure of master secret key K_{VS}, the Yu et al.' scheme [23] is vulnerable to many attacks including impersonation of vehicle, RSU, and vehicle server, along with session key disclosure and vehicle/user anonymity violations attack. The scheme of Vasudev et al. [22] lacks mutual authentication and has insecurities against vehicle, RSU, and vehicle server impersonation attacks. Moreover, Vasudev et al.'s scheme is insecure against man-in-the-middle attack. The scheme of Mohit et al. [24] is also weak against man in middle attack. In contrast, proposed SMEP-IoV provides all security features and is robust against the known attacks.

7. Conclusion

Initially, this study reviewed some of the recent authentication schemes for securing IoVs. Then, we developed a symmetric key-based authentication scheme, through which a vehicle can share a secret key with corresponding RSU through the mediation of the vehicle server. The proposed secure message exchange protocol for IoV (SMEP-IoV) uses only lightweight symmetric encryption and hash functions. The comparisons of the SMEP-IoV show that proposed scheme compromises slight performance overhead and provides adequate security, which other competing schemes do not provide. Hence, due to performance and security provisions, SMEP-IoV best suits the security requirements of the fast moving vehicles in the IoV scenario.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

Acknowledgments

The author would like to thank the the academic editor Dr. Prosanta Gope for valuable suggestions to improve the quality, correctness, presentation, and readability of the manuscript.

References

[1] M. Kamal, G. Srivastava, and M. Tariq, "Blockchain-based lightweight and secured v2v communication in the internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–8, 2020.

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

[3] B. LaMacchia, K. Lauter, and A. Mityagin, "Stronger security of authenticated key exchange," in *Proceedings of the International conference on provable security*, pp. 1–16, Springer, Wollongong, NSW, Australia, November 2007.

[4] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[5] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," *Lecture Notes in Computer Science Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, Bruges, Belgium, pp. 453–474, May 2001.

[6] S. A. Chaudhry, M. S. Farash, N. Kumar, and M. H. Alsharif, "Pflua-diot: a pairing free lightweight and unlinkable user access control scheme for distributed iot environments," *IEEE Systems Journal*, pp. 1–8, 2020.

[7] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar, "Amassing the security: an ecc-based authentication scheme for internet of drones," *IEEE Systems Journal*, pp. 1–8, 2021.

[8] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: architecture, protocols, and security," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3701–3709, 2018.

[9] B. Mokhtar and M. Azab, "Survey on security issues in vehicular ad hoc networks," *Alexandria Engineering Journal*, vol. 54, no. 4, pp. 1115–1126, 2015.

[10] S. A. Chaudhry, K. Yahya, F. Al-Turjman, and M. H. Yang, "A secure and reliable device access control scheme for iot based sensor cloud systems," *IEEE Access*, vol. 8, pp. 139244–139254, 2020.

[11] S. A. Chaudhry, "Correcting "PALK: password-based anonymous lightweight key agreement framework for smart grid," *International Journal of Electrical Power and Energy Systems*, vol. 125, Article ID 106529, 2021.

[12] S. A. Chaudhry, I. L. Kim, S. Rho, M. S. Farash, and T. Shon, "An improved anonymous authentication scheme for distributed mobile cloud computing services," *Cluster Computing*, vol. 22, no. 1, pp. 1595–1609, 2019.

[13] A. Irshad, M. Usman, S. A. Chaudhry, H. Naqvi, and M. Shafiq, "A provably secure and efficient authenticated key agreement scheme for energy internet-based vehicle-to-grid technology framework," *IEEE Transactions on Industry Applications*, vol. 56, no. 4, pp. 4425–4435, 2020.

[14] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "Tsvc: timed efficient and secure vehicular communications with privacy preserving," *IEEE Transactions on Wireless Communications*, vol. 7, no. 12, pp. 4987–4998, 2008.

[15] B. Ying, D. Makrakis, and H. T. Mouftah, "Privacy preserving broadcast message authentication protocol for vanets," *Journal of Network and Computer Applications*, vol. 36, no. 5, pp. 1352–1364, 2013.

[16] 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.

[17] A. Dua, N. Kumar, A. K. Das, and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4359–4373, 2018.

[18] 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.

[19] R. Amin, P. Lohani, M. Ekka, S. Chourasia, and S. Vollala, "An enhanced anonymity resilience security protocol for vehicular ad-hoc network with scyther simulation," *Computers and Electrical Engineering*, vol. 82, pp. 1–18, 2020.

[20] 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.

[21] B. Ying and A. Nayak, "Anonymous and lightweight authentication for secure vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 10626–10636, 2017.

[22] H. Vasudev, D. Das, and A. V. Vasilakos, "Secure message propagation protocols for iovs communication components," *Computers and Electrical Engineering*, vol. 82, pp. 1–15, 2020.

[23] S. Yu, J. Lee, K. Park, A. K. Das, and Y. Park, "Iov-smap: secure and efficient message authentication protocol for iov in smart city environment," *IEEE Access*, vol. 8, pp. 167875–167886, 2020.

[24] P. Mohit, R. Amin, and G. P. Biswas, "Design of authentication protocol for wireless sensor network-based smart vehicular system," *Vehicular Communications*, vol. 9, pp. 64–71, 2017.