Journal of Network Intelligence ©2021 ISSN 2414-8105 (Online)
Taiwan Ubiquitous Information Volume **6**, Number **4**, November **2021**

Combating Identity De-Synchronization: An improved Lightweight Symmetric key based Authentication scheme for IoV

Shehzad Ashraf Chaudhry

Department of Computer Engineering
Istanbul Gelisim University
Istanbul, Turkey
sashraf@gelisim.edu.tr

Received September 2021; revised October 2021

Abstract. *Due to its resource-friendly nature, symmetric-key based authentication methods are prioritized over public key infrastructure for employment in resource-constrained devices. Recently, a large number of symmetric-key based authentication protocols are proposed; however, the real progress is still marginal owing to repeated mistakes. Specifically, the emphasis on anonymity and privacy alongside the computational and communicative efficiencies has introduced some design flaws. The Identity De-Synchronization (ID-S) is one of such important issues that surfaced owing to such design flaws. This article aims to emphasize the causes and pitfalls of ID-S and for this purpose, a recent symmetric-key based authentication for the internet of vehicles (IoV) is analyzed. Precisely, it is to show in this article that the scheme of Xu et al. is vulnerable against ID-S under the widely used DY adversarial model. The article also proposes the available remedies to avoid ID-S and proposes an improved scheme.*
Keywords: Identity De-Synchronization, Symmetric-key, Authentication protocols

1. **Introduction.** The substitution of existing communication infrastructure by the advanced 6G/IoT is on its' way to extend endless connectivity. Owing to the endless connectivity of 6G and on-demand access to infrastructure, the users can benefit in a variety of ways such as healthcare, state services, shopping, and smart transportation, etc. However, all such advantages are subject to security and privacy threats and users can not realize the real advantages of the 6G revolution until security and privacy are ensured. The authentication protocols are the most widely used mechanisms to guarantee the security and privacy of the user. The Lamport [1] was the first to present an authentication scheme for remote users. However, due to the usage of verification tables, the scheme was not practical. Soon after 2001, Chan and Cheng [2] and Chang and Wu [3] proposed two separate authentication protocols by introducing smart cards and after then many authentication schemes were proposed [4–6]. In this connection, Das et al. [7] also proposed an authentication protocol using smart cards and by introducing dynamic identities for the provision of user anonymity and privacy. The scheme of Das et al. was later proved as weak against many threats. Yoon and Yoo [8] in 2006 proposed an improvement over the scheme of Liao et al. [9], after proving the weaknesses of Liao et al.'s scheme. In 2009, Wang et al. also proposed some improvements over Das et al.'s scheme [7]. However, Wang et al.'s scheme was also proved weak against many threats by Wen and Li [10]. In 2014, Kumari et al. also analyzed and then described that a scheme of Chang et al. [11]

to have weaknesses against user and server forgery attacks. In 2015, Chaudhry et al. [12] explored some weaknesses of the scheme of Kumari et al. Kaul and Awasthi [13] also proposed a symmetric-key based authentication scheme. However, Rana et al. [14] proved that in the scheme of Kaul and Awasthi, an attacker can easily expose session key and secret parameters. In 2019, Banerjee et al. [15] also presented a symmetric key-based authentication scheme for IoT. However, in [16], Alzahrani et al. discussed the incorrectness of the scheme of Banerjee et al. and termed their scheme impractical. Using lightweight symmetric key protocols, some other schemes were also proposed, such as cloud-based [17–19] and Internet of things [20–25].

Recently, many authentication schemes using symmetric keys were proposed for the Internet of Vehicles (IoV). However, with the undue emphasis on anonymity, many such schemes were either stuck into some correctness issues or suffer from identity de-synchronization (ID-S). The hashchain based schemes of Lin et al. [24] and Yin et al. [25] were argued to lack anonymity and leakage of vehicle's secret parameters [26]. Dua et al. [27] also proved that the scheme of Li et al. [28] proposed in 2015 has weaknesses against disclosure of session key. In 2020, Amin et al. [29] also argued that the scheme of Wang et al. [30] is vulnerable to the forgery of the user and vehicle. Chen et al. [26] also exposed the weaknesses of Ying et al.'s scheme [31]. However, due to modular exponentiation, the scheme of Chen et al. cannot be deployed in resource and time-constrained systems. The scheme of Vasudev et al. [32] was proved as prone to several forgery attacks in [33]. The scheme proposed by Yu et al. [33] was later proved as insecure against disclosure of master secret key in [34]. Mahmood et al. in their survey [35] explored some challenges and countermeasures for securing vehicular ad-hoc networks.

1.1. **Motivation.** The symmetric-key based authentication schemes are best suitable for resource and time-constrained environments like IoV etc. While public key-based operations are not suitable for constrained devices, it is still a tedious task to provide user/vehicle privacy by using only symmetric-key operations. Recently, some authentication schemes are proposed using only symmetric key operations $[18-25, 30, 32, 33]$. However, some of these schemes while claiming to provide privacy and anonymity stuck into identity de-synchronization (ID-S) issue, making it impossible to succeed in subsequent authentication requests. To highlight ID-S, in this paper, we analyze a very recently published symmetric key-based authentication scheme by Xu et al. [36]. We show that the scheme of Xu et al. is prone to ID-S, we then put forward some countermeasures and as per our analysis and understanding, no other countermeasures are available for the symmetric key-based authentication scheme to provide user/vehicle privacy.

1.2. **Adversary Model.** In this paper, we adopted the common and basic adversarial model DY (Dolev-Yao) [37]. All the communication carried out on a public channel can be controlled by the adversary and as per the DY model, the attacker can read, replay, modify a legitimate message sent on the channel, and can generate a forged message from scratch. Moreover, the attacker can also block/jam one or more messages communicated through the public channel [38–42].

1.3. **Notation Guide.** The notations used in subsequent parts of this paper as explained in Table 1.

2. **Revisiting Xu et al.'s scheme.** In the following subsections, a brief revisit of the recently proposed Xu et al.'s [36] symmetric-key based authentication scheme:

Table 1. Notations guide

Notation	Description
SA	System Admin
RSU	Roadside Unit
TA	Trusted Authority
V	Vehicle
K_{TA}	Private key of TA
P_{K_s}	Shared secret key
ID_V	Real Identity of V
TID_V	Pseudo Identity of V
ID_R	Real Identity of RSU
TID_R	Pseudo Identity of RSU
A_V, X_V, B_R	Secret Authentication Params
$S_1, S_2, ..., S_{17}$	Params computed during SAC
K_s	Session key
$t_1, t_2, ..., t_6$	timestamps
$\oplus$	Bit-wise Xor
(a, b)	concatenation of b with a
$A \rightarrow B : C$	transmission of C from A to B
$\stackrel{?}{=}$	Equality Check
r, n_1, n_2, n_3, n_4	Random numbers
ΔT	Max. Transmission delay
h	Oneway Hash operation
$E_K(Z)$	SBE of Z using key K

2.1. **Initialization phase of Xu et al.'s scheme.** For initialization, the System administrator selects and stores a private key K_{TA} into the memory of trusted authority TA.

2.2. **Registration phase of Xu et al.'s scheme.** For registering RSU and vehicle V, the TA generates identity, temporary identity and random secret tuple $\{ID_V, TID_V, P_{K_s}\}$ for each vehicle. Likewise, TA generates identity and temporary identity pair $\{ID_R, TID_R\}$ for each RSU. The TA then generates r randomly and computes $A_V = r \oplus K_{TA}$, $B_R = h(ID_R, K_{TA})$, $X_V = ID_V \oplus h(r, K_{TA})$. Now, the tuple $\{ID_V, TID_V, P_{K_s}, A_V\}$ is stored in the respective vehicle's memory and stores $\{ID_R, TID_R, K_{TA}, B_R\}$ in the respective RSU's memory. Finally, $\{X_V, TID_V, P_{K_s}\}$ and $\{ID_R, TID_R, B_R\}$ in TA's memory.

2.3. **Authentication phase of Xu et al.'s scheme.** The authentication phase of the Xu et al.'s recently published scheme is depicted in Figure 1 and is explained as follows:

Step XA1: $\boldsymbol{V \rightarrow RSU : R_1}$ The V initiates authentication process by generating $\{n_1, t_1\}$ and computes $B_V = h(ID_V, P_{K_s})$, $S_1 = n_1 \oplus B_V$ and $S_2 = h(ID_V, TID_V, A_V, S_1, t_1, n_1)$. Now V sends $R_1 = \{t_1, A_V, S_2, TID_V, S_1\}$ to RSU.

Step XA2: $\boldsymbol{RSU \rightarrow TA : R_2}$ Once RSU receives R_1, it first checks the freshness of t_1, and if t_1 is fresh, the RSU generates $\{n_2, t_2\}$ and computes $S_3 = n_1 \oplus B_R$ and $S_4 = h(TID_V, TID_R, ID_R, S_3, t_2, n_2)$. Now RSU sends $R_2 = \{TID_R, S_3, t_2, TID_V, S_4\}$ to TA.

Step XA3: $\boldsymbol{TA \rightarrow RSU : R_3}$ Once TA receives R_2, it first checks the freshness of t_2, and if t_2 is fresh, the TA retrieves (TID_V, X_V, P_{K_s}) using TID_V and (TID_R, ID_R, B_R)

using TID_R. Now, TA computes $n_2^* = S_3 \oplus B_R$ and checks $S_4 \stackrel{?}{=} h(TID_V, TID_R, ID_R, S_3, t_2, n_2^*)$ and if it's true the TA generates $\{n_3, t_3\}$ & computes $M_1 = h(n_2^*, n_3, K_{TA})$, $S_5 = n_3 \oplus B_R$, $S_6 = M_1 \oplus P_{K_s}$ and $S_7 = h(ID_R, S_5, S_6, X_V, n_3, t_3)$. Now TA sends $R_3 = \{S_5, t_3, X_V, S_7, S_6\}$ to RSU.

Step XA4: ***RSU* → *TA* : *R*$_4$** Once RSU receives R_3, it first checks the freshness of t_3, and if t_3 is fresh, the RSU computes $n_3^* = S_5 \oplus B_R$ and checks $S_7 \stackrel{?}{=} h(ID_R, S_5, S_6, X_V, n_3, t_3)$ and if it's true the RSU computes $M_1 = h(n_2^*, n_3, K_{TA})$, $P_{K_s} = M_1 \oplus S_6$, $r^* = A_V \oplus K_{TA}$, $ID_v^* = X_V \oplus h(r^*, K_{TA})$, and $B_V = h(ID_v^*, P_{K_s})$, $n_1^* = S_1 \oplus P_{K_s}$. Now, the RSU checks $S_2 \stackrel{?}{=} h(ID_V^*, TID_V, A_V, S_1, t_1, n_1)$, if it's true the RSU generates $\{r^+, n_4, t_4\}$ and computes $K_s = h(n_1^*, n_4, P_{K_s})$, $P_{K_s}^+ = h(n_1^*, n_4, K_s)$, $X_V^+ = ID_V^* \oplus h(r^+, K_{TA})$, $S_8 = n_2 \oplus M_1 \oplus P_{K_s}^+$, $S_9 = n_3 \oplus M_1 \oplus X_V^+$, $S_{10} = h(S_8, S_9, K_{TA}, n_2, n_3^*, t_4)$ and sends $R_4 = \{S_8, t_4, S_9, S_{10}\}$.

Step XA5: ***TA* → *RSU* : *R*$_5$** Once TA receives R_4, it first checks the freshness of t_4, and if t_4 is fresh, the TA checks $S_{10} \stackrel{?}{=} h(S_8, S_9, K_{TA}, n_2^*, n_3, t_4)$ and if it's true, the TA computes $P_{K_s}^+ = S_8 \oplus n_2 \oplus M_1$ and $X_V^+ = S_9 \oplus n_3 \oplus M_1$. The TA now randomly generates $\{TID_V^+, TID_R^+\}$ and timestamp t_5. The TA then computes $M_2 = h(n_2^*, n_3, P_{K_s})$, $M_3 = h(ID_R, n_2^*, n_3)$, $S_{11} = TID_V^+ \oplus M_2$, $S_{12} = TID_R^+ \oplus M_3$ and $S_{13} = h(S_{11}, S_{12}, K_{TA}, M_2, M_3, t_5)$. The TA then updates (TID_V, X_V, P_{K_s}) with $(TID_v^+, X_V^+, P_{K_s}^+)$ and (TID_R, ID_R, B_R) and (TID_R^+, ID_R^+, B_R^+). Now, TA sends $R_5 = \{S_{11}, t_5, S_{12}, S_{13}\}$ to RSU.

Step XA6: ***RSU* → *V* : *R*$_6$** Once RSU receives R_5, it first checks the freshness of t_5, and if t_5 is fresh, the RSU computes $M_2^* = h(n_2, n_3^*, P_{K_s})$, $M_3^* = h(ID_R, n_2, n_3^*)$ and checks $S_{13} \stackrel{?}{=} h(S_{11}, S_{12}, K_{TA}, M_2^*, M_3^*, t_5)$ and if it's true, the RSU generates t_6 and computes $TID_V^+ = M_2^* \oplus S_{11}$, $TID_R^+ = M_3^* \oplus S_{12}$, $A_v^+ = K_{TA} \oplus r^+$, $M_4 = h(n_1^*, n_4, ID_V^*)$, $S_{14} = M_4 \oplus A_V^+$, $S_{15} = M_4 \oplus TID_V^+$, $S_{16} = n_4 \oplus B_V$ and $S_{17} = h(S_{14}, S_{15}, S_{16}, ID_V^*, n_4, t_6)$. Now, RSU updates TID_R with TID_R^+ and sends $R_6 = \{S_{14}, t_6, S_{15}, S_{16}, S_{17}\}$ to V.

Step XA7: Once V receives R_6, it first checks the freshness of t_6, and if t_6 is fresh, the V computes $n_4^* = S_{16} \oplus B_V$ and checks $S_{17} \stackrel{?}{=} h(S_{14}, S_{15}, S_{16}, ID_V^*, n_4, t_6)$ and if it's true, the V computes $M_4 = h(n_1, n_4^*, ID_V^*)$, $A_V^+ = S_{14} \oplus M_4$, $TID_V^+ = S_{15} \oplus M_4$, $K_s = h(n_1, n_4^*, P_{K_s})$ and $P_{K_s}^+ = h(n_1, n_4^*, K_s)$. Finally, V updates (TID_V, X_V, P_{K_s}) with $(TID_v^+, X_V^+, P_{K_s}^+)$.

3. **Identity De-Synchronization Attack on Xu et al.'s.** The scheme of Xu et al. can become a pray of identity de-synchronization (ID-S) under the CK adversarial model, which is very common and realistic. As per the CK model, an adversary controls the communication link, which is public in nature and the adversary can stop/jam any message originated from any of the participants. For completion of a single round of authentication among the entities (V, RSU, TA) of the Xu et al.'s scheme, six (6) messages $\{R_1, R_2, R_3, R_4, R_5, R_6\}$ are exchanged over public channel. When a vehicle V initiates an authentication request by sending $R_1 = \{t_1, A_V, S_2, TID_V, S_1\}$ to RSU. The RSU after processing R_1, sends/forwards the message $R_2 = \{TID_R, S_3, t_2, TID_V, S_4\}$ to TA. In response to the request forwarded by RSU, the TA performs initial processing on R_2 and sends challenge message $R_3 = \{S_5, t_3, X_V, S_7, S_6\}$ back to RSU. Now RSU updates P_{K_s} and X_V with newly computed $P_{K_s}^+$ and X_V^+. The RSU the sends response message $R_4 = \{S_8, t_4, S_9, S_{10}\}$ to TA. After processing the response, TA randomly selects TID_V^+ and X_V^+ for the V. The TA further selects TID_R^+ for RSU. Now, TA updates $\{TID_V, X_V\}$ with $\{TID_V^+, X_V^+\}$ and TID_R with TID_R^+. Finaly, TA sends $R_5 = \{S_{11}, t_5, S_{12}, S_{13}\}$

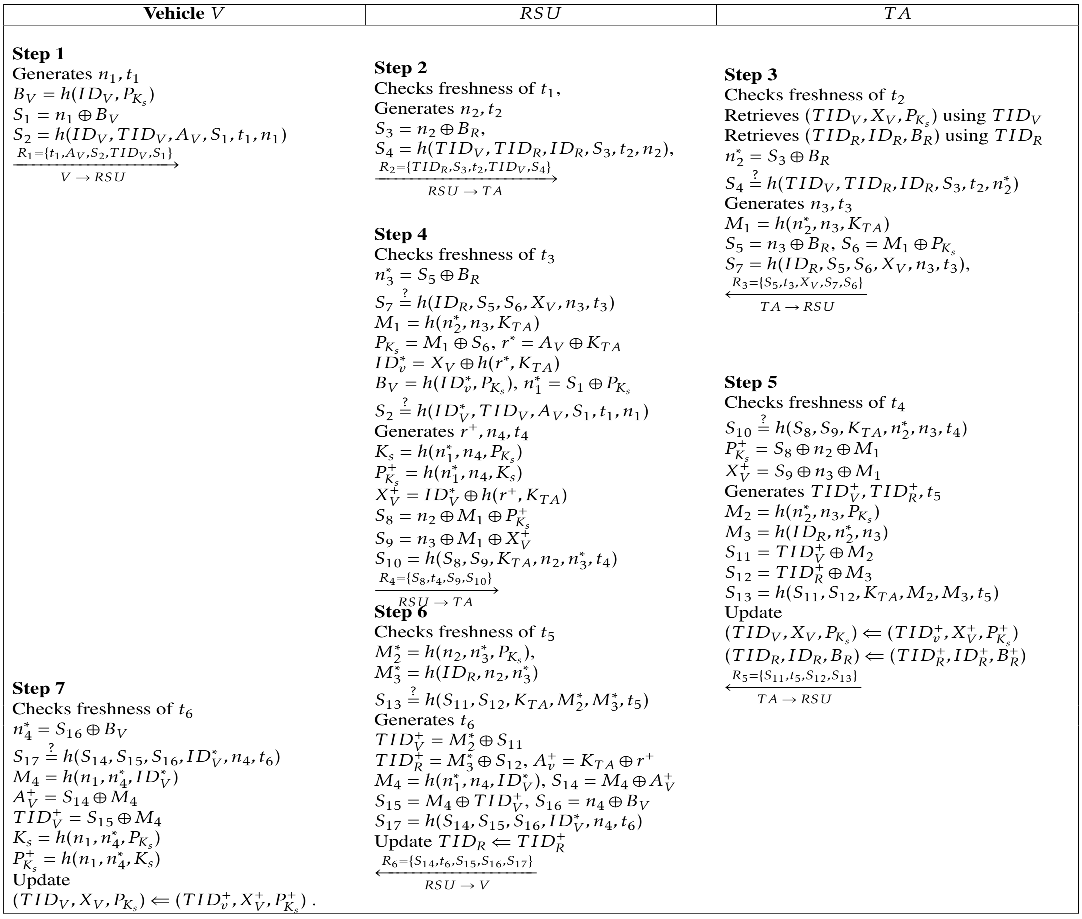

FIGURE 1. Xu et al.'s scheme

to RSU. The RSU then updates its' own temporary identity with TID_R^+ and sends $R_6 = \{S_{14}, t_6, S_{15}, S_{16}, S_{17}\}$ to V. The V on reception of R_6 after processing the message, updates $\{TID_V, X_V\}$ with $\{TID_V^+, X_V^+\}$.

Now, if the adversary stops/jams R_6, the V may have the old identity TID_V and the RSU and TA have new identity TID_V^+. The mismatch of identities at different entities can be termed as identity de-synchronization (ID-S). For subsequent authentication requests, the V in request message may send TID_V, and when RSU receives the request message, it may not recognize the vehicle V, because, TID_V is not available in its own database, which was already updated with new temporary identity TID_V^+. Therefore, due to ID-S, the legitimate authentication request of V will fail. It may also happen with all subsequent authentication requests by V. Similarly, if the adversary stops/jams reply message R_5 from TA to RSU, it may create ID-S among TA and RSU, V. Now, the TA may not recognize the temporary identities of both the RSU and V. In this case, the V is recognized by RSU but V and RSU both are not recognized by TA. This may happen to all subsequent authentication requests. The simulation of both cases (Stoppage of R_6 and R_5) of ID-S on Xu et al.'s scheme are also depicted in Figures 2 and 3, respectively.

4. **Countermeasures.** The de-synchronization may occur during the updation of temporary pseudo-identity. In case, the temporary identity remains the same and is updated on another side, the user may not be able to succeed in subsequent authentication requests as it is argued for the scheme of Xu et al. in Section 3.

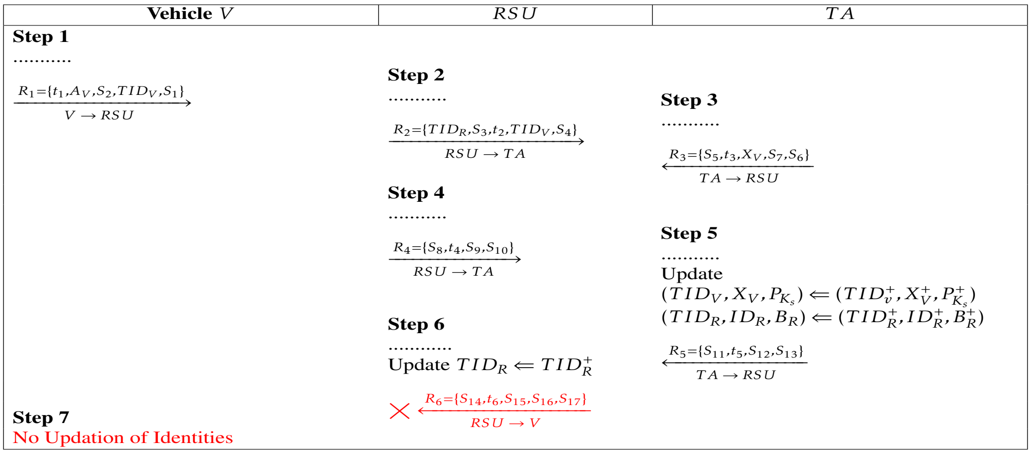

FIGURE 2. Identity De-synchronization Scenario-I

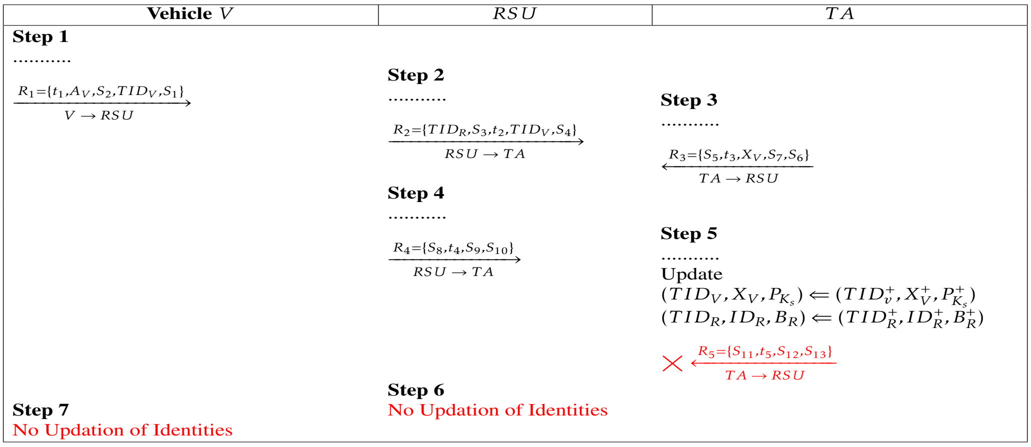

FIGURE 3. Identity De-synchronization Scenario-II

The simplest method to avoid identity de-synchronization (ID-S) is to use public key infrastructure for generating a dynamic identity for each session. However, from the analysis of symmetric key based schemes, we learned the following two remedies:

- The trusted authority or responding entity should keep two variables (say TID_{i-1} and TID_i), the TID_i to store current temporary identity and TID_{i-1} to store temporary identity generated during previous session. In the next login, TID_i will be updated with the newly computed identity, and TID_{i-1} will be updated with the identity computed during the current session. The storage of two temporary identities can avoid ID-S because if some inconsistency occurs among the requesting and responding entity, the requesting entity can use the old identity TID_{i-1} for authentication.
- Secondly, the TA or responding entity may encrypt the original identity with some padding and store it in the memory of the requesting entity. In this case, the TA does not need to store the temporary identity in its verifier. Instead, on each authentication request, the TA decrypts the temporary identity and extracts the original identity. To keep the identity dynamic, the TA using new padding encrypts the original identity and sends the new temporary identity to the requesting entity/user. In

such a case, even if one message is blocked and the user does not receive the new identity, it can use the old temporary identity for the next request. We adopted this method to design our proposed scheme, which is presented in the next subsection.

5. Proposed scheme.

5. Proposed scheme. In this section, we present our proposed scheme which is depicted in Figure 4 and explained in the following subsection:

5.1. Registration phase of proposed scheme. For registering RSU and vehicle V, the TA generates ID_V, randomly selects r and computes temporary identity $TID_V = E_{K_{TA}}(ID_V, r)$ and shared secrets $P_{K_s} = h(K_{TA}, r, ID_V)$, $X_V = h(ID_V, K_{TA}, r)$ for each vehicle. Likewise, TA generates identity ID_R, and computes temporary identity $TID_R = E_{K_{TA}}(ID_R, r)$ for each RSU. Further, the TA computes $B_R = h(ID_R, K_{TA})$. Now, the tuple $\{ID_V, TID_V, P_{K_s}\}$ is stored in the respective vehicle's memory and stores $\{ID_R, TID_R, K_{TA}, B_R\}$ in the respective RSU's memory.
Please note:- in our updated proposal the TA does not store any secret parameters relating to any of the RSU or V. The TA only stores public identities.

Vehicle V	RSU	TA
Step 1 Generates n_1, t_1 $B_V = h(ID_V, P_{K_s})$ $S_1 = n_1 \oplus B_V$ $S_2 = h(ID_V, TID_V, B_V, S_1, t_1, n_1)$ $\xrightarrow[V \to RSU]{R_1=\{t_1,S_2,TID_V,S_1\}}$	**Step 2** Checks freshness of t_1, Generates n_2, t_2 $S_3 = n_2 \oplus B_R$, $S_4 = h(TID_V, TID_R, ID_R, S_3, t_2, n_2)$, $\xrightarrow[RSU \to TA]{R_2=\{TID_R,S_3,t_2,TID_V,S_4\}}$	**Step 3** Checks freshness of t_2 $(ID_V, r) = D_{K_{TA}}(TID_V)$ $X_V = h(ID_V, K_{TA}, r)$ $P_{K_s} = h(K_{TA}, r, ID_V)$ $(ID_R, r) = D_{K_{TA}}(TID_R)$ $B_R = h(ID_R, K_{TA})$ $n_2^* = S_3 \oplus B_R$ $S_4 \stackrel{?}{=} h(TID_V, TID_R, ID_R, S_3, t_2, n_2^*)$ Generates n_3, t_3 $M_1 = h(n_2^*, n_3, K_{TA})$ $S_5 = n_3 \oplus B_R$, $S_6 = M_1 \oplus P_{K_s}$ $S_7 = h(ID_R, S_5, S_6, X_V, n_3, t_3)$, $\xleftarrow[TA \to RSU]{R_3=\{S_5,t_3,S_7,S_6\}}$
	Step 4 Checks freshness of t_3 $n_3^* = S_5 \oplus B_R$ $S_7 \stackrel{?}{=} h(ID_R, S_5, S_6, n_3, t_3)$ $M_1 = h(n_2^*, n_3, K_{TA})$ $P_{K_s} = M_1 \oplus S_6$ $(ID_V, r) = D_{K_{TA}}(TID_V)$ $X_V = h(ID_V, K_{TA}, r)$, $P_{K_s} = h(K_{TA}, r, ID_V)$ $B_V = h(ID_V^*, P_{K_s})$, $n_1^* = S_1 \oplus P_{K_s}$ $S_2 \stackrel{?}{=} h(ID_V^*, TID_V, B_V, S_1, t_1, n_1)$ Generates r^+, n_4, t_4 $P_{K_s}^+ = h(K_{TA}, r^+, ID_V)$ $X_V^+ = h(ID_V, K_{TA}, r^+)$ $S_8 = n_2 \oplus M_1 \oplus r^+$ $S_{10} = h(S_8, r^+ = K_{TA}, n_2, n_3^*, t_4)$ $\xrightarrow[RSU \to TA]{R_4=\{S_8,t_4,S_9,S_{10}\}}$	**Step 5** Checks freshness of t_4 $r^+ = S_8 \oplus n_2 \oplus M_1$ $S_{10} \stackrel{?}{=} h(S_8, r^+, K_{TA}, n_2^*, n_3, t_4)$ $TID_V^+ = E_{K_{TA}}(ID_V, r^+)$ $TID_R^+ = E_{K_{TA}}(ID_R, r^+)$ Generate t_5 $M_2 = h(n_2^*, n_3, P_{K_s})$ $M_3 = h(ID_R, n_2^*, n_3)$ $S_{11} = TID_V^+ \oplus M_2$ $S_{12} = TID_R^+ \oplus M_3$ $S_{13} = h(S_{11}, S_{12}, K_{TA}, M_2, M_3, t_5)$ $\xleftarrow[TA \to RSU]{R_5=\{S_{11},t_5,S_{12},S_{13}\}}$
Step 7 Checks freshness of t_6 $n_4^* = S_{16} \oplus B_V$ $S_{17} \stackrel{?}{=} h(S_{14}, S_{15}, S_{16}, ID_V^*, n_4, t_6)$ $M_4 = h(n_1, n_4^*, ID_V^*)$ $TID_V^+ = S_{15} \oplus M_4$ $K_s = h(n_1, n_4^*, P_{K_s})$ $P_{K_s}^+ = h(n_1, n_4^*, K_s)$ Update $(TID_V, X_V, P_{K_s}) \Leftarrow (TID_v^+, X_V^+, P_{K_s}^+)$.	**Step 6** Checks freshness of t_5 $M_2^* = h(n_2, n_3^*, P_{K_s})$, $M_3^* = h(ID_R, n_2, n_3^*)$ $S_{13} \stackrel{?}{=} h(S_{11}, S_{12}, K_{TA}, M_2^*, M_3^*, t_5)$ Generates t_6 $TID_V^+ = M_2^* \oplus S_{11}$ $TID_R^+ = M_3^* \oplus S_{12}$ $M_4 = h(n_1^*, n_4, ID_V^*)$ $S_{15} = M_4 \oplus TID_V^+$, $S_{16} = n_4 \oplus B_V$ $S_{17} = h(S_{14}, S_{15}, S_{16}, ID_V^*, n_4, t_6)$ Update $TID_R \Leftarrow TID_R^+$ $\xleftarrow[RSU \to V]{R_6=\{S_{14},t_6,S_{15},S_{16},S_{17}\}}$	

FIGURE 4. Proposed scheme

5.2. Authentication phase the proposed scheme. The authentication phase of the proposed scheme is depicted in Figure 4 and is explained as follows:

Step PA1: $\boldsymbol{V \rightarrow RSU : R_1}$ The V initiates authentication process by generating $\{n_1, t_1\}$ and computes $B_V = h(ID_V, P_{K_s})$, $S_1 = n_1 \oplus B_V$ and $S_2 = h(ID_V, TID_V, B_V, S_1, t_1, n_1)$. Now V sends $R_1 = \{t_1, S_2, TID_V, S_1\}$ to RSU.
Please note:- A_V was redundant and in proposed scheme it's not a part of request message.

Step PA2: $\boldsymbol{RSU \rightarrow TA : R_2}$ Once RSU receives R_1, it first checks the freshness of t_1, and if t_1 is fresh, the RSU generates $\{n_2, t_2\}$ and computes $S_3 = n_1 \oplus B_R$ and $S_4 = h(TID_V, TID_R, ID_R, S_3, t_2, n_2)$. Now RSU sends $R_2 = \{TID_R, S_3, t_2, TID_V, S_4\}$ to TA.

Step PA3: $\boldsymbol{TA \rightarrow RSU : R_3}$ Once TA receives R_2, it first checks the freshness of t_2, and if t_2 is fresh, the TA computes $(ID_V, r) = D_{K_{TA}}(TID_V)$, $X_V = h(ID_V, K_{TA}, r)$, $P_{K_s} = h(K_{TA}, r, ID_V)$, $(ID_R, r) = D_{K_{TA}}(TID_R)$, $B_R = h(ID_R, K_{TA})$ and $n_2^* = S_3 \oplus B_R$ and checks $S_4 \stackrel{?}{=} h(TID_V, TID_R, ID_R, S_3, t_2, n_2^*)$ and if it's true the TA generates $\{n_3, t_3\}$ and computes $M_1 = h(n_2^*, n_3, K_{TA})$, $S_5 = n_3 \oplus B_R$, $S_6 = M_1 \oplus P_{K_s}$ and $S_7 = h(ID_R, S_5, S_6, X_V, n_3, t_3)$. Now TA sends $R_3 = \{S_5, t_3, S_7, S_6\}$ to RSU.

Step PA4: $\boldsymbol{RSU \rightarrow TA : R_4}$ Once RSU receives R_3, it first checks the freshness of t_3, and if t_3 is fresh, the RSU computes $n_3^* = S_5 \oplus B_R$ and checks $S_7 \stackrel{?}{=} h(ID_R, S_5, S_6, n_3, t_3)$ and if it's true the RSU computes $M_1 = h(n_2^*, n_3, K_{TA})$, $P_{K_s} = M_1 \oplus S_6$, $(ID_V, r) = D_{K_{TA}}(TID_V)$, $X_V = h(ID_V, K_{TA}, r)$, $P_{K_s} = h(K_{TA}, r, ID_V)$, $B_V = h(ID_v^*, P_{K_s})$ and $n_1^* = S_1 \oplus P_{K_s}$. Now, the RSU checks $S_2 \stackrel{?}{=} h(ID_V^*, TID_V, B_V, S_1, t_1, n_1)$, if it's true the RSU generates $\{r^+, n_4, t_4\}$ and computes $P_{K_s}^+ = h(K_{TA}, r^+, ID_V)$, $X_V^+ = h(ID_V, K_{TA}, r^+)$, $S_8 = n_2 \oplus M_1 \oplus r^+$, $S_{10} = h(S_8, r^+, K_{TA}, n_2, n_3^*, t_4)$ and sends $R_4 = \{S_8, t_4, S_9, S_{10}\}$.

Step PA5: $\boldsymbol{TA \rightarrow RSU : R_5}$ Once TA receives R_4, it first checks the freshness of t_4, and if t_4 is fresh, the TA computes $r^+ = S_8 \oplus n_2 \oplus M_1$ and checks $S_{10} \stackrel{?}{=} h(S_8, r^+, K_{TA}, n_2^*, n_3, t_4)$ and if it's true, the TA computes $TID_V^+ = E_{K_{TA}}(ID_V, r^+)$ and $TID_R^+ = E_{K_{TA}}(ID_R, r^+)$. The TA now randomly timestamp t_5. The TA then computes $M_2 = h(n_2^*, n_3, P_{K_s})$, $M_3 = h(ID_R, n_2^*, n_3)$, $S_{11} = TID_V^+ \oplus M_2$, $S_{12} = TID_R^+ \oplus M_3$ and $S_{13} = h(S_{11}, S_{12}, K_{TA}, M_2, M_3, t_5)$. Now the TA sends $R_5 = \{S_{11}, t_5, S_{12}, S_{13}\}$ to RSU.

Step PA6: $\boldsymbol{RSU \rightarrow V : R_6}$ Once RSU receives R_5, it first checks the freshness of t_5, and if t_5 is fresh, the RSU computes $M_2^* = h(n_2, n_3^*, P_{K_s})$, $M_3^* = h(ID_R, n_2, n_3^*)$ and checks $S_{13} \stackrel{?}{=} h(S_{11}, S_{12}, K_{TA}, M_2^*, M_3^*, t_5)$ and if it's true, the RSU generates t_6 and computes $TID_V^+ = M_2^* \oplus S_{11}$, $TID_R^+ = M_3^* \oplus S_{12}$, $M_4 = h(n_1^*, n_4, ID_V^*)$, $S_{15} = M_4 \oplus TID_V^+$, $S_{16} = n_4 \oplus B_V$ and $S_{17} = h(S_{14}, S_{15}, S_{16}, ID_V^*, n_4, t_6)$. Now, RSU updates TID_R with TID_R^+ and sends $R_6 = \{S_{14}, t_6, S_{15}, S_{16}, S_{17}\}$ to V.

Step PA7: Once V receives R_6, it first checks the freshness of t_6, and if t_6 is fresh, the V computes $n_4^* = S_{16} \oplus B_V$ and checks $S_{17} \stackrel{?}{=} h(S_{14}, S_{15}, S_{16}, ID_V^*, n_4, t_6)$ and if it's true, the V computes $M_4 = h(n_1, n_4^*, ID_V^*)$, $TID_V^+ = S_{15} \oplus M_4$, $K_s = h(n_1, n_4^*, P_{K_s})$ and $P_{K_s}^+ = h(n_1, n_4^*, K_s)$. Finally, V updates (TID_V, X_V, P_{K_s}) with $(TID_v^+, X_V^+, P_{K_s}^+)$.

6. **The Comparisons.** In this section, we illustrate the performance comparison of the proposed scheme with Xu et al.'s scheme [36] using the computation, communication costs, and running time as the metrics. We consider the running time as per the experiment conducted in [22], where the running time is computed through Ubuntu 16.0-LTS OS, on an Elite-Book model 8460-P, with 2.7-GHz processor and 4-GB RAM, model Core-i7 2620M intel (R). We denote T_h as the computation cost of execution of a hash operation

Table 2. Performance Comparisons

Scheme	V	RSU	TA	C_1	C_2	C_3
Xu et al. [36]	$6T_h$	$14T_h$	$7T_h$	$27T_h$	0.108	440
Proposed	$6T_h$	$15T_h$	$10T_h$+$4T_e$	$31T_h$+$4T_e$	0.156	496

Note: T_h: hash operations; T_e: Encryption or decryption Operations; C_1: Aggregate Computation Cost; C_2: Aggregate Running Time in ms; C_3: Communication cost in Bytes;

and T_e as the computation cost of execution of an encryption/decryption operation. Referring Hussain et al.'s experiment [22], the running time of a hash operations $T_h \approx 0.004$ milli-seconds (ms) and symmetric block encryption/decryption $T_e \approx 0.008$ ms. During execution of an authentication cycle of the proposed scheme, the V, RSU and TA execute $6T_h$, $15T_h$ and $10T_h + 4T_e$ operations, respectively. Therefore, the total computation cost of a single authentication cycle in the case of the proposed scheme is $31T_h + 4T_e$ and the running time as per the experiment performed in [22] is 0.156 milli-seconds (ms). The computation cost of Xu et al.'s scheme is $27T_h$, and a single round of authentication completes in 0.108 ms.

For communication cost comparisons, we consider identities to be 8 bytes long, the timestamps are taken 4 bytes of length. We consider SHA-1 with the length of 20 bytes, random numbers are also fixed as 20 bytes length. We use AES encryption algorithm with 18 bytes block size. For completion of an authentication round during execution of the proposed scheme, six (6) messages are exchanged between communicating entities. The first message $R_1 = \{t_1, S_2, TID_V, S_1\}$ communicates from V to RSU. The length of $t_1 = 4$, $S_2 = 20$, $S_1 = 20$; whereas, $TID_V = E_{K_{TA}}(ID_V, r)$, where length of $ID_V = 8$ and length of $r = 16$, therefore, TID_V requires 2 blocks of AES encryption each with size 16 bytes. So, the size of $TID_V = 32$ bytes. This employs that total size of $R_1 = \{4+20+32+20\} = 76$ bytes. Using the same analogy, the size of $R_2\{TID_R, S_3, t_2, TID_V, S_4\}$ transmitted from RSU to TA is $R_2 = \{32 + 20 + 4 + 32 + 20\} = 108$ bytes. The third message $R_3 = \{S_5, t_3, S_7, S_6\}$ is sent from TA to RSU and the length is $R_3 = \{20 + 4 + 20 + 20\} = 64$ bytes. Fourth message $R_4 = \{S_8, t_4, S_9, S_{10}\}$ is transmitted from RSU to TA and the length is $R_4 = \{20 + 4 + 20 + 20\} = 64$ bytes. The fifth message $R_5 = \{S_{11}, t_5, S_{12}, S_{13}\}$ is sent from TA to RSU and the length is $R_5 = \{32 + 4 + 32 + 20\} = 88$ bytes. The last message $R_6 = \{S_{14}, t_6, S_{15}, S_{16}, S_{17}\}$ is transmitted from RSU to TA and the length is $R_6 = \{20 + 4 + 32 + 20 + 20\} = 96$. The total communication cost of the proposed scheme is $496 = \{76 + 108 + 64 + 64 + 88 + 96\}$ bytes. The communication cost of the scheme of Xu et al. [36] is 440 bytes.

Although, the comparisons show that the proposed scheme has introduced some extra communication and computation costs as compared with Xu et al.'s scheme, unlike the proposed scheme, the scheme of Xu et al. is prone to identity de-synchronization. The comparisons are also shown in Table 2.

7. **Conclusions.** Although, the symmetric-key based authentication schemes are more suitable for resource and time-constrained devices; however, many of the recent symmetric-key based authentication schemes are prone to Identity de-synchronization (ID-S). In this article, we emphasized the causes and pitfalls of ID-S. As a case study, we reviewed and analyzed a recent symmetric-key based authentication scheme for IoV by Xu et al. We showed that the scheme of Xu et al. is prone to ID-S. We also provided the countermeasures to avoid ID-S in symmetric-key-based authentication schemes and based on the countermeasures we proposed an improved authentication scheme using symmetric-key

primitives for IoV. The performance analysis shows that the proposed scheme introduced some extra communication and computation costs, provides user anonymity, and is free of any design flaw leading to ID-S. The proposed scheme is presented with an aim to avoid such design flaws in the future.

REFERENCES

[1] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[2] C.-K. Chan and L.-M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 4, pp. 992–993, 2000.

[3] C.-C. Chang and T.-C. Wu, "Remote password authentication with smart cards," *IEE Proceedings E (Computers and Digital Techniques)*, vol. 138, no. 3, pp. 165–168, 1991.

[4] Z. Ali, A. Ghani, I. Khan, S. A. Chaudhry, S. H. Islam, and D. Giri, "A robust authentication and access control protocol for securing wireless healthcare sensor networks," *Journal of Information Security and Applications*, vol. 52, p. 102502, 2020.

[5] A. Irshad, H. Naqvi, S. Ashraf Chaudhary, M. Usman, M. Shafiq, O. Mir, and A. Kanwal, "Cryptanalysis and improvement of a multi-server authenticated key agreement by chen and lee's scheme," *Information Technology and Control*, vol. 47, no. 3, pp. 431–446, 2018.

[6] S. A. Chaudhry, "Correcting "palk: Password-based anonymous lightweight key agreement framework for smart grid"," *International Journal of Electrical Power & Energy Systems*, vol. 125, 106529, 2021.

[7] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic id-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 629–631, 2004.

[8] E.-J. Yoon and K.-Y. Yoo, "Improving the dynamic id-based remote mutual authentication scheme," in *International Conferences on the Move to Meaningful Internet Systems (OTM'06)*, pp. 499–507, Springer, 2006.

[9] I.-E. Liao, C.-C. Lee, and M.-S. Hwang, "Security enhancement for a dynamic id-based remote user authentication scheme," in *International Conference on Next Generation Web Services Practices (NWeSP'05)*, IEEE, 2005. https://doi.org/10.1109/NWESP.2005.67.

[10] F. Wen and X. Li, "An improved dynamic id-based remote user authentication with key agreement scheme," *Computers & Electrical Engineering*, vol. 38, no. 2, pp. 381–387, 2012.

[11] Y.-F. Chang, W.-L. Tai, and H.-C. Chang, "Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update," *International Journal of Communication Systems*, vol. 27, no. 11, pp. 3430–3440, 2014.

[12] S. A. Chaudhry, M. S. Farash, H. Naqvi, S. Kumari, and M. K. Khan, "An enhanced privacy preserving remote user authentication scheme with provable security," *Security and Communication Networks*, vol. 8, no. 18, pp. 3782–3795, 2015.

[13] S. D. Kaul and A. K. Awasthi, "Security enhancement of an improved remote user authentication scheme with key agreement," *Wireless Personal Communications*, vol. 89, no. 2, pp. 621–637, 2016.

[14] M. Rana, A. Shafiq, I. Altaf, M. Alazab, K. Mahmood, S. A. Chaudhry, and Y. B. Zikria, "A secure and lightweight authentication scheme for next generation iot infrastructure," *Computer Communications*, vol. 165, pp. 85–96, 2021.

[15] S. Banerjee, V. Odelu, A. K. Das, J. Srinivas, N. Kumar, S. Chattopadhyay, and K.-K. R. Choo, "A provably secure and lightweight anonymous user authenticated session key exchange scheme for internet of things deployment," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8739–8752, 2019.

[16] B. A. Alzahrani, S. A. Chaudhry, A. Barnawi, W. Xiao, M. Chen, and A. Al-Barakati, "Ilas-iot: An improved and lightweight authentication scheme for iot deployment," *Journal of Ambient Intelligence and Humanized Computing*, 2020. https://doi.org/10.1109/JIOT.2019.2931372.

[17] M. Wazid, A. K. Das, V. Bhat, and A. V. Vasilakos, "Lam-ciot: Lightweight authentication mechanism in cloud-based iot environment," *Journal of Network and Computer Applications*, vol. 150, 102496, 2020.

[18] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4900–4913, 2018.

[19] S. A. Chaudhry, A. Irshad, K. Yahya, N. Kumar, M. Alazab, and Y. B. Zikria, "Rotating behind privacy: An improved lightweight authentication scheme for cloud-based iot environment," *ACM Transactions on Internet Technology*, vol. 21, no. 3, pp. 1–19, 2021.

[20] J. Qi, M. Zhuo, M. Jianfeng, and L. Guangsong, "Security enhancement of robust user authentication framework for wireless sensor networks," *China Communications*, vol. 9, no. 10, pp. 103–111, 2012.
[21] S. Yu, N. Jho, and Y. Park, "Lightweight three-factor based privacy-preserving authentication scheme for iot-enabled smart homes," *IEEE Access*, vol. 9, pp. 126186–126197, 2021.
[22] 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*, vol. 15, no. 3, pp. 4431–4438, 2021.
[23] S. Hussain, K. Mahmood, M. K. Khan, C.-M. Chen, B. A. Alzahrani, and S. A. Chaudhry, "Designing secure and lightweight user access to drone for smart city surveillance," *Computer Standards and Interfaces*, vol. 80, 103566, 2022.
[24] 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.
[25] 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.
[26] 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.
[27] 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.
[28] 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.
[29] 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.
[30] 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.
[31] 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.
[32] 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.
[33] 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.
[34] S. A. Chaudhry, "Designing an efficient and secure message exchange protocol for internet of vehicles," *Security and Communication Networks*, vol. 2021, 5554318, 2021.
[35] J. Mahmood, Z. Duan, Y. Yang, Q. Wang, J. Nebhen, and M. N. M. Bhutta, "Security in vehicular ad hoc networks: Challenges and countermeasures," *Security and Communication Networks*, vol. 2021, 9997771, 2021.
[36] Z. Xu, X. Li, J. Xu, W. Liang, and K.-K. R. Choo, "A secure and computationally efficient authentication and key agreement scheme for internet of vehicles," *Computers and Electrical Engineering*, vol. 95, 107409, 2021.
[37] 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.
[38] A. Irshad, M. Sher, H. F. Ahmad, B. A. Alzahrani, S. A. Chaudhry, and R. Kumar, "An improved multi-server authentication scheme for distributed mobile cloud computing services," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 10, no. 12, pp. 5529–5552, 2016.
[39] C. Peng, M. Luo, L. Li, K.-K. R. Choo, and D. He, "Efficient certificateless online/offline signature scheme for wireless body area networks," *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 14287–14298, 2021.
[40] M. N. Aman, U. Javaid, and B. Sikdar, "A privacy-preserving and scalable authentication protocol for the internet of vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1123–1139, 2021.
[41] 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. https://doi.org/10.1109/JSYST.2020.3036425.

[42] X. Li, J. Tan, A. Liu, P. Vijayakumar, N. Kumar, and M. Alazab, "A novel uav-enabled data collection scheme for intelligent transportation system through uav speed control," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 4, pp. 2100–2110, 2021.