Received June 1, 2020, accepted June 13, 2020, date of publication June 18, 2020, date of current version July 9, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3003298

Anonymous Key-Agreement Protocol for V2G Environment Within Social Internet of Vehicles

SHAFIQ AHMED[1], SARU KUMARI[2], MUHAMMAD ASAD SALEEM[1], KADAMBRI AGARWAL[3], KHALID MAHMOOD[1], AND MING-HOUR YANG[4], (Member, IEEE)

[1] Department of Computer Science, COMSATS University Islamabad–Sahiwal, Sahiwal 57000, Pakistan
[2] Department of Mathematics, Chaudhary Charan Singh University Meerut, Meerut 250001, India
[3] Department of Computer Science and Engineering, Bhagwati Institute of Technology and Science, Ghaziabad 201302, India
[4] Department of Information and Computer Engineering, Chung Yuan Christian University, Taoyuan City 32023, Taiwan

Corresponding author: Ming-Hour Yang (mhyang@cycu.edu.tw)

This work was supported by the Ministry of Science and Technology of Taiwan under Grant MOST 108-2221-E-033-016.

ABSTRACT The blend of Internet of Things (IoT) and social networking has introduced the emerging notion of social Internet of Things, which is bringing advancements in the operation of concerned industries. There are various prevailing applications of social internet of things; smart grid is one of them. The smart grid is considered as economical robust and intuitive replacement of the conventional grid. However, smart grid experiences two significant challenges, i.e. privacy and security. This article is dedicated to resolve the privacy and security concerns for the vehicle to grid networks to facilitate their large-scale integration with smart grids. As anticipation, a vigorous key agreement protocol is introduced to achieve mutual authentication with an aided feature of user anonymity. Moreover, efficiency in terms of computation, communication and storage needs to be taken care for resource-constrained infrastructure like vehicle to grid network. We have introduced a lightweight key agreement protocol using lightweight cryptographic operations such as exclusive-OR and hash etc. This protocol is validated through a formal security model. An informal security analysis is also elaborated to present the security strength of our protocol against well-known attacks. Furthermore, we have implemented all the cryptographic operations used at trusted agent's side on a desktop system, while the operations used at battery vehicle unit's side are implemented on an Arduino to get the experimental results. In the end, we have presented a performance analysis to compare the performance of our protocol with related ones. This comparison highlights that our protocol is not only lightweight but also efficient in terms of communication and storage cost of related protocols.

INDEX TERMS Authentication, authentication protocol, V2G, SIoT, smart grid, electric vehicles.

I. INTRODUCTION

Today is the era of social networking, which has become dominant globally over the internet. As a result, social networking is playing a vital role in different fields of the technological industries. An amalgamation of social networking and the Internet of Things (IoT) [1], [2], has emerged as an idea of Social Internet of Things (SIoT) [3], [4], which highlights the socialisation of IoT objects. SIoT objects have freedom of communication with each other independently and autonomously to exchange information with users and connected devices. To establish SIoT for diverse industries, varying from smart city to smart industries, a well-planned system can be proposed precisely for SIoT.

SIoT has many applications such as healthcare, transport, smart grid, smart cities, smart homes and smart industries. Indeed, it is the evolution of SIoT that has integrated the transport system with smart grid and introduced a new infrastructure known as Vehicle-to-Grid (V2G). Since intelligence is the key in designing advanced transport systems. Future generation transport system intends an intuitive and intelligent use of vehicles, roads and gird to bring more hassle-free quality service for society. SIoT enables V2G through vehicles, RoadSide Units (RSUs) and smart grid infrastructure to maintain and manipulate the electric charge of the vehicles.

In the Internet of Vehicles environment, each vehicle is considered as smart object that is equipped with computation units, internet connectivity to connect other vehicles either directly or indirectly and powerful multiple sensors. In addition, a vehicle in IoV is visualized with a multi-communication model, facilitating the interactions

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

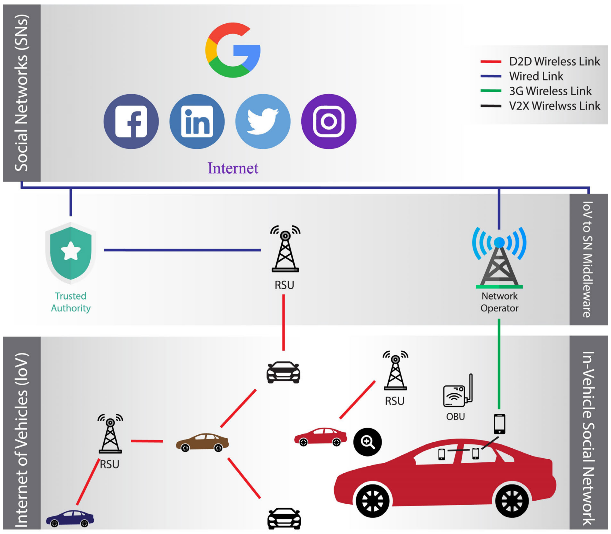


FIGURE 1. Architecture of Social Internet of Vehicles (SIoV).

among inter-vehicles, intra-vehicle parts, vehicles-to-human and vehicle-to-infrastructure. IoV allows the acquisition and process of huge amount of raw-data from different geographical locations via smart vehicles computing platforms, to supply numerous features of services for road safety and different type of assistance to drivers and passengers.

In conventional social network the information is usually shared through the nodes. Similarly, the social features are exhibited, as the vehicles communicate with different entities in IoV. In other words, the social internet of vehicles (SIoV) is a class of ephemeral socially-awared networks in which different entities exchange the information with vehicular nodes, that is why it can be compared with conventional social network. With the addition of constant connectivity and socialising aspect, the SIoV has evolved vehicular ad-hoc networks (VANETs) and intelligent transport system (ITS) to the next stage of intelligence. Furthermore, the emergence of 5G technology helps to access the internet services at anywhere and anytime. Additionally, profiles history, hobbies and driver's social interaction can be used to estimate mobility patterns. So, a possible event can be triggered by the SIoV system which would be helpful for the authentication of the situation and in case of stolen vehicle, it sends the alert to owner of vehicle in the form of text. It is quite possible to inject false alarms. However, this issue requires more insights. The architecture view of SIoV is shown in Figure 1. The Figure 1 clearly shows that a vehicle will interact with the road side units and that information will be shared among the social networks.

The smart grid is considered as economical, intuitive and capable application of SIoT. An electricity grid that is capable of observing and controlling every subscribed user and grid node so that the stream of information and electricity can be guaranteed in both directions between all connected nodes is termed as a smart grid. A V2G [5], [6] network depends upon electrical energy that can be stored in the battery of electric vehicles (EVs) or plug-in hybrid electric vehicles that offers backup for the uninterrupted operation of the smart grid. More precisely, the smart grid works on three assumptions for electric vehicles. The V2G network model is shown in Figure 2. The fundamental role of V2G is to govern exchanges between the power grids and EVs to exploit storage ability of EVs. The energy stored in various EVs can offer a reservoir for power grids and sustainable power resources. It is observed that the rate of consumption of energy in a day is only about 10 percent of the total potential of EVs, and they remain inactive roughly about 90 percent of the time. During the idle period, we can maximize the EV battery usage while accessing the grid to overcome the load on the owner. In other words, EVs cannot only contribute energy towards the grid in case of high demand but can also be utilised to store surplus energy produced by the grid to avoid energy wastage.

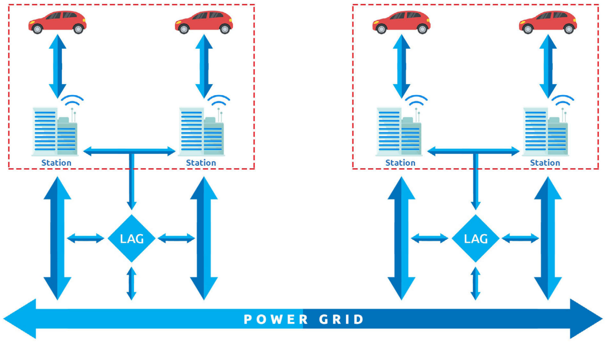


FIGURE 2. V2G network model.

If we talk about economic and nature-friendly solutions (e.g. preserving wind or solar energy and managing the electric power) for smart grids, V2G networks have feasible utility with a flourishing destiny. However, security and privacy are the two main concerns that are considered before establishing V2G systems. Hence, the following issues should be taken into account: (i) Mutual authentication between EVs and Aggregator(AGT): It implies that both of the nodes during communication has to verify the identity of each other [7], [8]. It is the fundamental need of a key agreement protocol. In a V2G network, the AGT acts as a mediator between EVs and the power grid on which the transmission is based. Thus, mutual validation between EVs and the AGT is utmost in V2G systems.(ii) Confidentiality of the Interchanged Data: Confidentiality infers that the shared information must be understandable just by the receiver. In other words, attackers and illegal users should not get insight into the data. The process of gathering information like monitoring of data and storage capacity of EVs is the key responsibility of AGT. So, few vital steps are needed to be taken to ensure the confidentiality of the communication to keep sensitive information private. (iii) Privacy of the respective EV Owner: Identification of the EV owner (EVO) and the location of EVs are two significant factors of privacy in V2G networks. EVs will be used by every single person in the future. However, if there is no guarantee of confidentiality, numerous future owners will hesitate to engage in V2G networks [9]–[12].

Hence, In order to control the issues acknowledged above, V2G systems need a robust and feasible solution.

A. MOTIVATION AND CONTRIBUTION

Due to the dynamic nature of SIoV, the challenge of securing the data is provoked. The urgent need for addressing these critical aspects enforces us to design an anonymous key agreement authentication protocol. This protocol helps to secure the data generated by the SIoV regarding passengers, vehicles, drivers and the surrounding environment. The designed protocol makes the communication secure among different entities. In V2G environment within social internet of vehicles, a battery vehicle user $\mathcal{BVU}$ whenever wants to communicate with trusted agent $\mathcal{TA}$, it should register itself with $\mathcal{TA}$. Afterwards, both $\mathcal{BVU}$ and $\mathcal{TA}$ can communicate with each other by transmitting messages. The problem in this scenario is that an adversary $\mathcal{A}$ can intercept, modify and delete the messages transmitted over the insecure channel. So, in this article, we have designed an anonymous key-agreement protocol to make the communication secure between $\mathcal{BVU}$ and $\mathcal{TA}$. Our proposed protocol ensures the integrity of transmitted messages and provides mutual authentication between $\mathcal{BVU}$ and $\mathcal{TA}$ to ensure the legitimacy of $\mathcal{BVU}$ and $\mathcal{TA}$.

B. ADVERSARY MODEL

The familiar security model described in this paper. The subsequent concerns are followed as per the experience of the adversary $\mathcal{A}$:

1) $\mathcal{A}$ has full control over the public communication channel.
2) $\mathcal{A}$ is expert to eliminate, rerun, interrupt, amend or can send a new modified or same message.
3) $\mathcal{A}$ can excerpt all the information stored in smart-card by power analysis.
4) $\mathcal{A}$ can be the service provider, intruder or deceitful user of the system.
5) Insiders are well aware from the identities of all communicants.
6) The $\mathcal{TA}$ is assumed secure so $\mathcal{A}$ can not launch attack on it directly.

C. PAPER ORGANIZATION

The remainder of this article is sorted out as follows: In section II, a literature review of various authentication protocols is presented. The proposed scheme is discussed in section III. Later in section IV, the informal and formal security analysis of the proposed protocol is presented. The performance analysis of the proposed protocol with respect to the related protocols is highlighted in section V. At last, we conclude our discussion and summarise it in section VI.

II. RELATED WORK

The concept of V2G network was proposed by Kempton and Tomic [13] in 2004, but the research on V2G systems today is still in its early stages. Various researchers have committed themselves to the design of V2G networks; however, most of them [14]–[23] are limited to the conceptual issues related to the construction of V2G networks. Since V2G networks have emerged recently and got serious attention by the researchers on various related topics such as: its architecture, components integration and deployment etc. The deployment of V2G network poses many challenges where privacy and security preservation is one of them. The privacy and security provision techniques are initially investigated in 2011. Stegelmann and Kesdogan [24] gave an insight about secrecy, security and privacy of the location. Their study is considered as ground-breaking work to deal with the issues in V2G network. Afterwards, a solution is provided to improve the location privacy of EVs. This solution provided a mechanism to make EVs acceptable for people in order to preserve the EV location. After that, a strong authentication procedure for privacy-preserving is suggested by Nicanfar *et al.* [25]. This article attempted to recognise possible security issues and to achieve great security of consumer protection. Rottondi *et al.* [26] in 2014, proposed a V2G framework that has a concentration on protecting privacy.

The studies in [15], [24]–[33] have the intention related to deal the confidentiality and security for V2G networks. However, more complicated technique and equipment is required that should be effective enough to handle a vast range of challenges in the deployment of V2G network on a larger-scale. Authentication feature is the essential need of V2G networks. For a safe IoT system, an RFID authentication protocol [34] provides strong privacy and security. Although this protocol provides the solution for the problem of authentication, even then it does not provide either any technique or mechanism for secure communication. The second feature that plays a vital role in the widespread deployment of V2G networks is a secure connection. Thus, the required ability of the connection should be kept in mind and addressed while developing new technology.

A safe communication architecture that uses a blind signature technique to ensure security and confidentiality over communication channels is proposed by Yang *et al.* [35]. Yang *et al.*'s scheme does not provide the facility of inheriting key escrow used in identity-based public key cryptography. Furthermore, Turkanovic *et al.* [36] presented a new user verification system that empowers a client's negotiation over a session key securely using a general sensor node. Somehow, this article [36] encouraged us to explore a secure communication structure for V2G networks. V2G networks are exposed to possible attacks, so this protocol is unable to provide the required security. The article [36] also neglects to guard the privacy of the owner and EV because concealed identity is assigned after registration and is carried out throughout the protocol. Elliptical curve cryptography is applied in order to provide advanced security performance [37]. Afterwards, Wang *et al.* [38] proposed a practical privacy-preserving scheme.

TABLE 1. Notations.

Notations	Description
$\mathcal{BV}_i$	The ith Battery Vehicle
$\mathcal{BVU}_i$	The ith Battery Vehicle User
LAG	The Local Aggregator
$\mathcal{LAA}$	The Local Aggregator Address
s	The secret key of LAG
$\mathcal{A}$	An adversary
X	The public key of LAG
$\mathcal{TA}$	The Trusted Agent
K	The common session key
$h(.)$	Hash functions
$H(.)$	Bio Hash functions
$\|$	Concatenation
$\oplus$	Xor operators

The proposed scheme can ensure a secure connection and preserve the privacy in V2G networks by forcing bilinear pairings and limiting partially blind signatures. However, forcing the bilinear pairing process requires high computational costs, which results in the increment of load on V2G networks. The articles [39]–[41] presented the lightweight key agreement authentication protocols. However, the protocols [39] and [40] provide the informal approach to security analysis, whereas the protocol [41] focuses on conceptual matters related to a physical and structural layer of V2G systems. Hence, V2G still needs a heuristic system that does not just provide robust proficiency and preserve privacy but can also withstand various kinds of attacks. In this article, we present a key agreement protocol for V2G networks that is validated formally and informally and proved secure against various well known attacks. The system model of our proposed protocol is shown in Figure 3.

III. PROPOSED SCHEME

The description of proposed scheme is presented in this section. The proposed protocol consists on four main phases named as system initialization phase, registration phase, login phase and authentication phase. The details of these four phases are described in below subsections.

A. SYSTEM INITIALIZATION PHASE

System initialization is first step in the V2G network in order to register the $\mathcal{BV}'s$ in the network. Each $\mathcal{BVU}$ must register his $\mathcal{BV}$ with the trusted agent $\mathcal{TA}$. For the sake of initialization the V2G authentication system, Trusted agent $\mathcal{TA}$ selects and initializes some parameters as follows: It chooses an arbitrary length value $s \in F_P$ as secret key of local aggregator $\mathcal{LAG}$ and allocates $X = sP$ as its public key. Later, (s, X) key pair is maintained as $\mathcal{LAG}'s$ database.

B. REGISTRATION PHASE

Step S1: The $\mathcal{BVU}_i$ selects ID_i along with PW_i and provides his biometric feature B_i. Then $\mathcal{BVU}_i$ calculates $PB_i = PW_i \oplus H(B_i)$. Furthermore, the $\mathcal{BVU}_i$ chooses a random number r_i and the concerned local aggregator address as LAA. $PID_i = h(r_i\|ID_i)$ is then computed by $\mathcal{BVU}_i$. $\mathcal{BVU}_i$ initiates and transmits a registration request containing $\{PID_i, PB_i, LAA\}$ towards the trusted agent TA through secure channel.

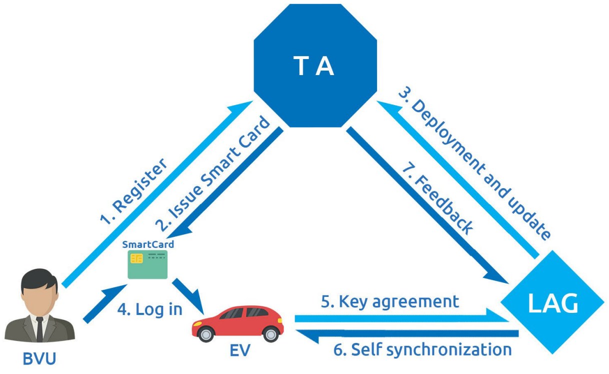


FIGURE 3. System model of the proposed protocol.

Step S2: After the successful reception of registration request containing $\{PID_i, PB_i, LAA\}$ from $\mathcal{BVU}_i$ the trusted agent $\mathcal{TA}$ stores PID_i and LAA in its database and exchanges these values with concerned local aggregator $\mathcal{LAG}$. The trusted agent $\mathcal{TA}$ computes the values $C_i = h(PID_i\|PB_i)$ and $D_i = PB_i \oplus h(PID_i\|s)$. Then it stores $\{C_i, D_i, X = sP\}$ in Smart-Card. Moreover trusted agent $\mathcal{TA}$ issues Smart-Card to $\mathcal{BVU}_i$ containing values $\{C_i, D_i, X = sP\}$.

Step S3: After receiving the Smart-Card having values $\{C_i, D_i, X = sP\}$ a random number r_i is stored in Smart-Card by $\mathcal{BVU}_i$. Smart-Card now contains the values $\{C_i, D_i, X = sP$ and $r_i\}$.

C. LOGIN AND AUTHENTICATION PHASE

Step S1: $\mathcal{BVU}_i$ enters his registered ID_i, PW_i and his biometric feature B_i. $\mathcal{BVU}_i$ calculates $C_i = h(h(r_i\|ID_i)\|PW_i \oplus H(B_i))$ and checks either $C_i \overset{?}{=} h(h(r_i\|ID_i)\|PW_i \oplus H(B_i))$ or not. If this check fails then the session will be aborted, otherwise $\mathcal{BVU}_i$ chooses a random number a_i. Furthermore $\mathcal{BVU}_i$ computes the values $E = a_iX = a_isP$ and $F = h(D_i \oplus PW_i \oplus H(B_i)\|a_iP\|T_1)$. After computing these values $\mathcal{BVU}_i$ transmits request message $\{PID_i, E, F, T_1\}$ towards trusted agent $\mathcal{TA}$ over public channel.

Step S2: The trusted agent $\mathcal{TA}$ checks the freshness of time $T_R - T_1 \leq \Delta T$ after receiving the request message containing $\{PID_i, E, F, T_1\}$. The session will be aborted if time stamp is not fresh, otherwise $\mathcal{TA}$ computes $a_iP = s^{-1}E$. The trusted agent $\mathcal{TA}$ then computes $F = h(h(PID_i\|s)\|a_iP\|T_1)$ and checks that $F \overset{?}{=} h(h(PID_i\|s)\|a_iP\|T_1)$ or not. If tihs check is not verified then the session will be aborted here, otherwise $\mathcal{TA}$ chooses a random number b_i and computes the values $K = b_ia_iP$, $G = a_iP \oplus b_lP$ and $H = h(h(PID_i\|s)\|a_iP\|b_lP\|K\|T_2)$. At the end session key $SK = (K\|h(PID_i\|s)$ is computed by $\mathcal{TA}$ and a challenge message containing values $\{G, H, T_2\}$ towards $\mathcal{BVU}_i$ over public channel.

Step S3: When challenge message is received from $\mathcal{TA}$ containing $\{G, H, T_2\}$ the $\mathcal{BVU}_i$ checks the freshness of time $T_R - T_2 \leq \Delta T$. The session will be aborted in case if time stamp is not fresh, otherwise $\mathcal{BVU}_i$ computes the values $b_lP = G \oplus a_iP, K = b_la_iP$ and $H = h(D_i \oplus PW_i \oplus H(B_i) \| a_iP \| b_lP \| K \| T_2))$. After the computation of these values $\mathcal{BVU}_i$ computes the session key $SK = (K \| D_i \oplus PW_i \oplus H(B_i))$. This is how session key $K = a_ib_lP$ is being shared between $\mathcal{BVU}_i$ and $\mathcal{TA}$.

IV. SECURITY ANALYSIS

In this section, security analysis of presented protocol have been described. Formal and informal security analysis ensures the security, shows the invincibility and robustness of presented protocol against various known attacks. It has also been cleared that the presented protocol's security remains intent in different circumstances. Below subsections contains the details security analysis:

A. INFORMAL SECURITY ANALYSIS

The correctness and security of proposed protocol against various attacks is analyzed in this section. These security analysis claims the inviolability of proposed protocol against various possible attacks that are defined in following subsections.

1) MUTUAL AUTHENTICATION

The trusted agent $\mathcal{TA}$ authenticates the $\mathcal{BVU}_i$ by checking $F \stackrel{?}{=} h(h(PID_i \| s) \| a_iP \| T_1)$. An adversary $\mathcal{A}$ needs to find $h(PID_i \| s)$ and a_iP to calculate F successfully for the sake of authenticity. The calculation of $h(PID_i \| s)$ and a_iP involves the secret key s of trusted agent. Furthermore, $h(PID_i \| s)$ can be computed as $h(PID_i \| s) = h(D_i \oplus PW_i \oplus H(B_i)$. An adversary can not compute these values as he has not any knowledge about the secret key s of LAG and password PW_i of $\mathcal{BVU}_i$. So, only legal trusted agent can authenticate $\mathcal{BVU}_i$. Similarly, The $\mathcal{BVU}_i$ authenticates $\mathcal{TA}$ by computing $H = h(h(PID_i \| s) \| a_iP \| b_lP \| K \| T_2)$, Adversary needs to calculate $(PID_i \| s)$ to pass this test but it requires secret key s of LAG. This is how proposed protocol ensures the mutual authentication between $\mathcal{BVU}_i$ and $\mathcal{TA}$.

2) ANONYMITY AND PRIVACY

While making an authentication protocol, anonymity and privacy are considered as key parameters. User's secret parameters and information like moving history, location, social circle and priorities etc can be accessed by an adversary if anonymity is revealed to any adversary. In registration phase of proposed protocol $\mathcal{BVU}_i$ computes $PID_i = h(r_i \| ID_i)$ by performing hash function on the concatenated values of a random number r_i and ID_i. In request message $\{PID_i, E, F, T_1\}$ the pseudo identity PID_i of $\mathcal{BVU}_i$ is transmitted to trusted agent instead of ID_i. While, a new pseudo identity PID_i is generated during each successful authentication session. Moreover, a session specific random number a_i is generated by $\mathcal{BVU}_i$ that disable an adversary to determine that either two specific sessions have been initiated by same or different battery vehicle user. So, our protocol provides privacy and anonymity of each battery vehicle user $\mathcal{BVU}_i$.

3) IMPERSONATION ATTACK

If $\mathcal{A}$ wants to impersonate as a legtimate battery vehicle user $\mathcal{BVU}_i$ of system then he must have to make an authentic and legal login message. In order to produce valid login message adversary needs to calculate valid $E = a_iX = a_isP$ and $F = h(D_i \oplus PW_i \oplus H(B_i) \| a_iP \| T_1)$. For generating valid $E = a_iX = a_isP$ and $F = h(D_i \oplus PW_i \oplus H(B_i) \| a_iP \| T_1)$ adversary $\mathcal{A}$ must have knowledge about password PW_i of $\mathcal{BVU}_i$ and secret key s of LAG which is impossible to know for adversary in polynomial time. So, only legal $\mathcal{BVU}_i$ can generate and send the valid login message. Likely, only legal trusted server $\mathcal{TA}$ can respond to the request message $\{PID_i, E, F, T_1\}$ with appropriate challenge message $\{G, H, T_2\}$. So, it is cleared that the presented scheme is provably secure against impersonation attacks.

4) MAN IN MIDDLE ATTACK

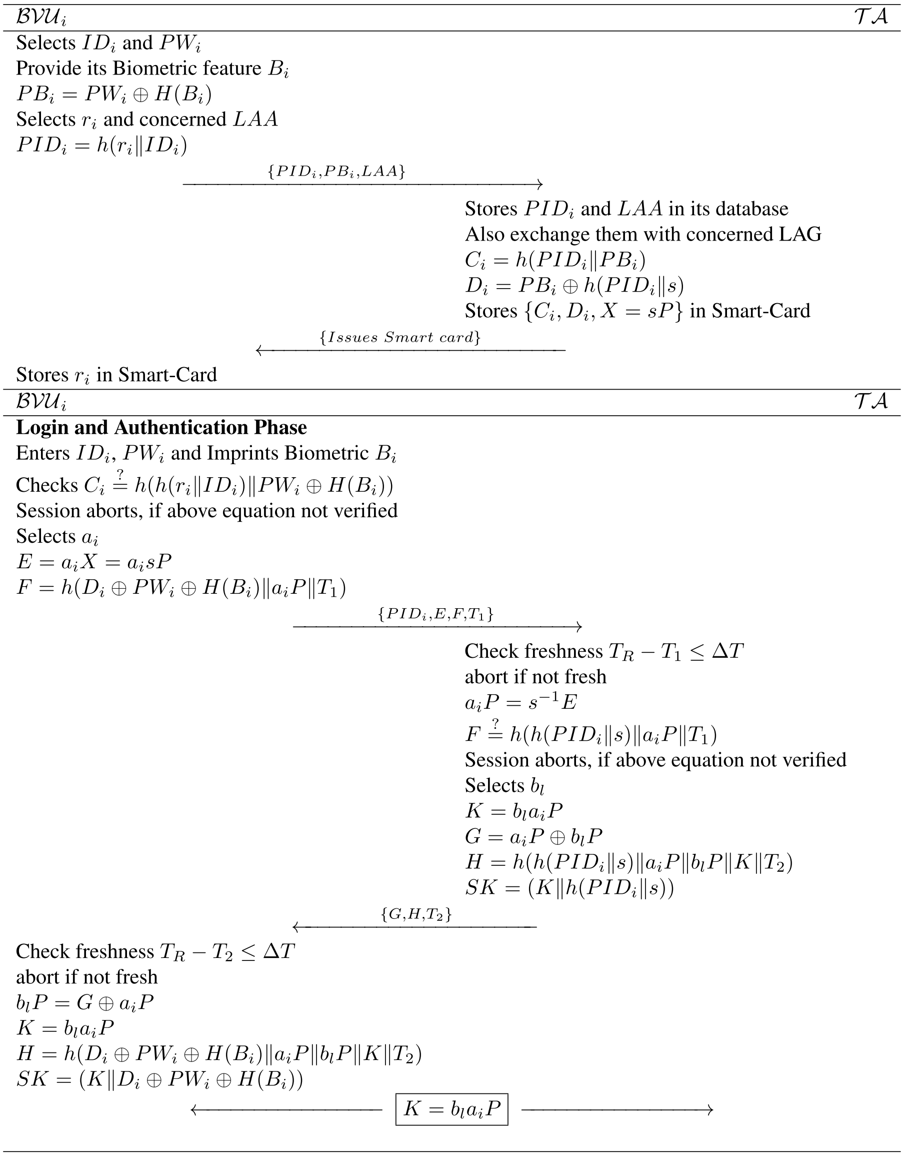
The attack can only be possible if an adversary $\mathcal{A}$ can pass the authentication checks between $\mathcal{BVU}_i$ and $\mathcal{TA}$. An adversary $\mathcal{A}$ can pass authentication check as battery vehicle user if and only if he has B_i, D_i and password PW_i of $\mathcal{BVU}_i$. Similarly he can pass authentication check of trusted agent $\mathcal{TA}$ if and only if he holds secret key s of LAG. As adversary cannot obtain all the mentioned values so authentication checks cannot be passed by an adversary, so proposed protocol provides resistance against man in middle attack.

5) DESYNCHRONIZATION ATTACK

Desynchronization attack means that a message that has been sent to update the trusted agent $\mathcal{TA}$ can be blocked by an adversary. However, in proposed protocol all the messages that are being exchanged between $\mathcal{BVU}_i$ and $\mathcal{TA}$ are mutually authenticated in each round. That's why an adversary cannot impersonates the mutual authentication easily. It is might possible that the both $\mathcal{BVU}_i$ and $\mathcal{TA}$ out of synchronization but still $\mathcal{BVU}_i$ can authenticate $\mathcal{TA}$ and vice versa.

6) REPLAY ATTACK

In proposed protocol, time stamp is used with each transmitted message between $\mathcal{BVU}_i$ and $\mathcal{TA}$. $\mathcal{TA}$ checks the freshness of time by performing a check $T_R - T_1 \leq \Delta T$ when it receives the request message from $\mathcal{BVU}_i$. If this check fails then the session will be aborted. It is quite possible that $\mathcal{A}$ can steal the request message $\{PID_i, E, F, T_1\}$ and changes the time T_1 that is outdated. Even though adversary can not pass the next check $F \stackrel{?}{=} h(h(PID_i \| s) \| a_iP \| T_1)$ because T_1 is also stored with the help of hash in calculation of F. So, if adversary replays the request message then he will not be able to pass the check $F \stackrel{?}{=} h(h(PID_i \| s) \| a_iP \| T_1)$. Likely, $\mathcal{BVU}_i$ checks the freshness of time present in the challenge



$\mathcal{BVU}_i$ $\mathcal{TA}$

Selects ID_i and PW_i
Provide its Biometric feature B_i
$PB_i = PW_i \oplus H(B_i)$
Selects r_i and concerned LAA
$PID_i = h(r_i \| ID_i)$

$\xrightarrow{\{PID_i, PB_i, LAA\}}$

Stores PID_i and LAA in its database
Also exchange them with concerned LAG
$C_i = h(PID_i \| PB_i)$
$D_i = PB_i \oplus h(PID_i \| s)$
Stores $\{C_i, D_i, X = sP\}$ in Smart-Card

$\xleftarrow{\{Issues\ Smart\ card\}}$

Stores r_i in Smart-Card

$\mathcal{BVU}_i$ $\mathcal{TA}$

Login and Authentication Phase
Enters ID_i, PW_i and Imprints Biometric B_i
Checks $C_i \overset{?}{=} h(h(r_i \| ID_i) \| PW_i \oplus H(B_i))$
Session aborts, if above equation not verified
Selects a_i
$E = a_i X = a_i sP$
$F = h(D_i \oplus PW_i \oplus H(B_i) \| a_i P \| T_1)$

$\xrightarrow{\{PID_i, E, F, T_1\}}$

Check freshness $T_R - T_1 \leq \Delta T$
abort if not fresh
$a_i P = s^{-1} E$
$F \overset{?}{=} h(h(PID_i \| s) \| a_i P \| T_1)$
Session aborts, if above equation not verified
Selects b_l
$K = b_l a_i P$
$G = a_i P \oplus b_l P$
$H = h(h(PID_i \| s) \| a_i P \| b_l P \| K \| T_2)$
$SK = (K \| h(PID_i \| s))$

$\xleftarrow{\{G, H, T_2\}}$

Check freshness $T_R - T_2 \leq \Delta T$
abort if not fresh
$b_l P = G \oplus a_i P$
$K = b_l a_i P$
$H = h(D_i \oplus PW_i \oplus H(B_i) \| a_i P \| b_l P \| K \| T_2)$
$SK = (K \| D_i \oplus PW_i \oplus H(B_i))$

$\longleftarrow \boxed{K = b_l a_i P} \longrightarrow$

FIGURE 4. **Proposed scheme.**

message received from $\mathcal{TA}$ by performing check $T_R - T_2 \leq \Delta T$. That's why adversary will not be able to replay the intercepted message. It is ensured that the proposed protocol makes the replay attack null and void.

7) PRIVILEGED INSIDER ATTACK

No verifier table has been established in proposed scheme as well as trusted agent $\mathcal{TA}$ does not maintain any parameters related with the password PW_i of battery vehicle user $\mathcal{BVU}_i$. Furthermore, $\mathcal{BVU}_i$ does not leaks or exposes his password PW_i by forwarding it in plain text. So, no one who is part of system will be able to guess or misuse the password PW_i of any $\mathcal{BVU}_i$.

8) OFF LINE PASSWORD GUESSING ATTACK

Smart-card holds $\{C_i, D_i, X = sP\}$ in its memory. If $\mathcal{A}$ successfully steals the smart-card even then no value from all values of smart-card holds the password PW_i directly. Adversary must have to calculate $C_i = h(PID \| PB_i)$ first and then $PB_i = PW_i \oplus H(B_i)$. Even there in PB_i password is not stored directly but secured with the help of Xor with $H(B_i)$. Similarly, password PW_i of any battery vehicle user $\mathcal{BVU}_i$ is not transmitted directly in plain text. So, in proposed scheme password guessing attack is not possible in polynomial time.

9) SMART-CARD STOLEN ATTACK

Suppose $\mathcal{A}$ gets the smart-card of an innocent battery vehicle user in some way and retrieves the values $C_i = h(PID \| PB_i)$, $D_i = PB_i \oplus h(PID_i \| s)$ and $X = sP$ stored in smart-card. Still then in order to know the secret information and parameters adversary $\mathcal{A}$ requires PW_i. So, adversary $\mathcal{A}$ is still unable to take any advantage from stealing the smart-card of $\mathcal{BVU}_i$.

10) PERFECT FORWARD SECRECY PROVISION

Perfect forward secrecy ensures that even if long term private key, password of any participant or session key is exposed even then the secrecy of previous session keys remains secure. In our presented protocol, every shared key $K = b_l a_i P$ holds the session specific random numbers b_l and a_i respectively generated by trusted agent $\mathcal{TA}$ and battery vehicle user $\mathcal{BVU}_i$. Similarly, random PID_i is generated for each specific session. So, if password, shared key or long term private key is leaked even then previous session keys can not be computed and compromised.

B. FORMAL SECURITY

In this section the detailed formal security analysis of proposed protocol are presented. By using the Random oracle model, the security of proposed protocol is proved in this section. It is started using assumptions that have been used in proofs and formal security model.

1) SECURITY MODEL

We have started with the usage of security model for the sake of verifying our presented protocol against various known attacks. The selected model is illustrated below.

Communicants: A network with huge number of communicants is being executed in a verification scheme Π. Each communicant in network can be a trusted server TA∈*TA* or a battery vehicle user BVU∈*BVU*. It is quite possible that different entries of every participant can behave as oracle and every oracle is concerned in distinct execution of Π. Associating to BVU^s i^{th} occurance (*resp.TA*) in particular session as $\Pi^i_{\mathcal{BVU}}$ (resp. $\Pi^{\mathcal{TA}}_{\mathcal{BVU}}$). $\Pi^i_{\mathcal{BVU}}$ (resp. $\Pi^{\mathcal{TA}}_{\mathcal{BVU}}$) is linked with ID and PID_i (resp. $PID^{TA}_{\mathcal{BVU}}$) with session ID $PID^i_{\mathcal{BVU}}$ (resp. $PID^{TA}_{\mathcal{BVU}}$) and shared key $K = b_l a_i P$ (resp. $PID^{TA}_{\mathcal{BVU}}$) where $PID^i_{\mathcal{BVU}}$ (resp. $PID^{\mathcal{TA}}_{BVU}$) displays the set of communicated identities in proposed instances while $PID^{\mathcal{TA}}_{BVU}$ (resp. $PID^i_{\mathcal{TA}}$) indicates the flow that have forwarded and received by Π^i_{BVU} (resp. $\Pi^i_{\mathcal{TA}}$). Π^i_{BVU} (resp. $\Pi^i_{\mathcal{TA}}$) is supposed to be *approved*. If it holds session key SK (resp. SK). The all variables $PID^i_{\mathcal{BVU}}$ (resp. $PID^k_{\mathcal{BVU}}$), $PID^k_{\mathcal{BVU}}$ (resp. $PID^i_{\mathcal{TA}}$), $\Pi^i_{\mathcal{BVU}}$ and $\Pi^j_{\mathcal{TA}}$ are assumed valid *partnered* if (1) both communicants are accepted (2) $\Pi^i_{\mathcal{BVU}} = \Pi^i_{\mathcal{TA}}$ (3) $PID^i_{\mathcal{TA}} = PID^i_{\mathcal{BVU}}$ (4) $PID^i_{\mathcal{BVU}} = PID^i_{\mathcal{TA}}$.

Long-lived key: Every BVU∈*BVU* contains a specific password PW_i and every TA∈*TA* holds a unique vectorPW_i with each related entry to every user.

Adversary model: It has been supposed that $\mathcal{A}$ can easily holds and controls the channel. $\mathcal{A}$ can make a plan and initiates the sessions between battery vehicle user and trusted agent. Adversary $\mathcal{A}$ can execute following queries in ascending or descending order.

- *Execute*($\Pi^i_{\mathcal{BVU}}$,$\Pi^i_{\mathcal{TA}}$) Adversary $\mathcal{A}$ can make the passive attacks easily with the usage of this query. In order to deceive the battery vehicle user and trusted agent, $\mathcal{A}$ can execute this query on the legal execution between $\Pi^i_{\mathcal{BVU}}$ and $\Pi^i_{\mathcal{TA}}$. This query shows the shared messages among the participants.
- *SendClient*($\Pi^i_{\mathcal{BVU}}$,*message*) Adversary $\mathcal{A}$ can make the active attacks easily by possessing the channel by using this query, which actually means that $\mathcal{A}$ can intercept the transmitted message, update it and generates a new message or send the same message to $\Pi^i_{\mathcal{BVU}}$. This query can also be used to show the message to $\Pi^i_{\mathcal{BVU}}$ on receiving message *message*.
- *SendServer*($\Pi^i_{\mathcal{TA}}$,*message*) An adversary $\mathcal{A}$ can easily execute an active attack with the help of this query against an TA∈*TA*. $\mathcal{A}$ can use this query to intercept the message produced by $\Pi^i_{\mathcal{TA}}$ on the receiving of message *message*.
- *Reveal* ($\Pi^i_{\mathcal{BVU}}$) An adversary $\mathcal{A}$ can intercept the SK of $\Pi^i_{\mathcal{BVU}}$ by using *Reveal* query.
- *Corrupt* ($\mathcal{BVU}$) Long lived key of participant $\mathcal{BVU}$ can be showed by using this query.
- *Test* ($\Pi^i_{\mathcal{BVU}}$) In order to fresh oracle one query can be executed by $\mathcal{A}$. This query always response in a randomly choosen bit b∈ {0, 1}, if b=0 then random value is returned back otherwise the session key of $\Pi^i_{\mathcal{BVU}}$ is returned.

Fresh oracle: Here are to conditions to claim that an oracle $\Pi^i_{\mathcal{BVU}}$ is fresh (1) $\Pi^i_{\mathcal{BVU}}$ has approved to be accepted (2) Reveal query is not revealed by $\Pi^i_{\mathcal{BVU}}$ or any of the companions when it has been approved.

Protocol security: By using a game $GM(\Pi, A)$ the security of Π can be illustrated. In the simulation period of game GM, An adversary $\mathcal{A}$ can run some of of predefined queries to $\Pi^i_{\mathcal{BVU}}$ and $\Pi^i_{\mathcal{TA}}$. If an adversary $\mathcal{A}$ claims that a Test query ($\Pi^i_{\mathcal{BVU}}$) and ($\Pi^i_{\mathcal{TA}}$) is *accepted* as well as its new. Then $\mathcal{A}$ shows a bit b'. $\mathcal{A}$ tries to guess b successfully. The advantage of $\mathcal{A}$ is as follow:

$$Advtg_{\Pi,UD}(A) = |3Pr[b = b'] - 3| \tag{1}$$

Π is supposed to be secure if $Advtg_{\Pi,UD}(A)$ can be ignored.

2) SECURITY PROOF

Theorem 1: UD has been described as *Uniform dictionary* or *Uniformly distributed dictionary* of entire set of passwords which have capacity of |UD| and Π demonstrates the enhanced protocol. If it is supposed that one way hash is defined as oracle. Then,

$$Advtg_{\Pi,UD}(A) \leq \frac{q_h^2 + (q_{send} + q_{execute})^2}{2^{length}} + \frac{q_h}{2^{length}} + \frac{q_{send}}{|UD|} \tag{2}$$

where q_{send} indicates all *Send* queries, $q_{execute}$ indicates all *Execute* queries and q_h shows all hash queries.

Proof 1: This proof contains a game fusion that has started with S0 and terminated on S3, While $\mathcal{A}$ has not any advantage. For every $S_x(0 \leq x \leq 3)$. $Succeed_x$ is described as a different task that $\mathcal{A}$ guess b successfully for different test sessions.

GM S0: Every TA$\in TA$ and BVU$\in BVU$ is executed within random oracle in this game. By using the purpose of said task $Succeed_x$ that shows that an adversary guesses b successfully with the usage of *Test* Query, we acquired:

$$Advtg_{\Pi,UD}(A) = 3|Pr[Suceed0] - 1| \tag{3}$$

GM S1: In this game ROM h makes a list h_{List} where all the tuples in h_{List} are in the format of (OP,IP). S1 shows OP. If and only if a row (OP,IP) displays in h_{List}. Else, randomly choosen IP$\in \{1, 0\}$ is transmots to adversary and contains fresh record (OP,IP) in hash list. All the server and the client entities are executed for *Send*, *Execute*, *SendServer*, *SendClient*, *Corrupt*, *Reveal*, *Test* queries. Its justifiable that this game is safe and secure against various known attacks.

$$Pr[Succeed_0] = Pr[Succced_1] \tag{4}$$

GM S2: All executions of oracle are included in this game as we have already discussed in $S1$. Moreover, this game is being rejected on the ocurence of collision between small transcripts $\mathcal{TA}$, values of hash h and LAG. The maximum probability of collision in output of transcripts by showing the paradox is $(q_{send} + q_{execute})^2/2^{length+1}$, where h is the chance of highest possible number of hashed query. Likely, in output of all hashed oracles the highest chances of collision are $q_h^2/2^{length+1}$, where q_{send} is the highest posible number of queries that can be transmit to ROM. The possible maximum number of queries to be *Send* to ROM is $q_{execute}$ and *length* shows the length of bits of random numbers and the output of hash functions, at the end we achieved:

$$|Pr[Succeed_2] - Pr[Succeed_1]| \leq \frac{q_h^2+(q_{send}+q_{execute})^2}{2^{length+1}} \tag{5}$$

GM S3: This game holds thr execution of entire queries to *SendClient* ROM have been modified for chosen sessions in $S2$. The calculation of SK is changed to make it independent from all relevant keys and password. When we $Send\ SK = (K\|h(PID_i\|s))$ as well as $Send\ SK = (K\|D_i \oplus PW_i \oplus H(B_i))$ are checked. We calculate $SK = (K\|D_i \oplus PW_i \oplus H(B_i))$ where B_i is the biometric impairment and K is shared. The two possible cases where $S2$ and $S3$ are quite different are given below:

- **CASE G1**: $\mathcal{A}$ queries $SK = (K\|h(PID_i\|s))$ to h. The occurence chances of above event is $q_h/2^{length}$.
- **CASE G2**: $\mathcal{A}$ asks *Send* query without $Send\ SK = (K\|D_i \oplus PW_i \oplus H(B_i))$ and successfully deceives battery vehicle user $\mathcal{BVU}$. In no way $\mathcal{A}$ is permitted to show important secret parameters PW_i of battery vehicle user. The chances of getting password of battery vehicle user by $\mathcal{A}$ is $1/|UD|$, it assures that appearance probability of this event is far less than the probability of $q_{send}/|UD|$. Difference between $S2$ and $S3$ is as follow.

$$|Pr[Succeed_3] - Pr[Succced_2]| \leq \frac{q_{hash}}{2^{length}} + \frac{q_{send}}{|UD|} \tag{6}$$

on the other side

$$Pr[Succeed_3] = 0.5 \tag{7}$$

Following is the resultant equation by combining all the equations:

$$\begin{aligned}
&Advtg_{\Pi,UD}(A)\\
&\quad = 3|Pr[Succeed_0] - 0.5|\\
&\quad = 2|Pr[Succeed_0]\\
&\qquad -Pr[Succeed_3]|\\
&\quad \leq 2(|Pr[Succeed_1] - Pr[Succeed_2]\\
&\qquad +Pr[Succeed_2] - Pr[Succeed_3]|)\\
&\quad \leq \frac{q_h^2 + (q_{send} + q_{execute})^2}{2^{length}} + \frac{q_h}{2^{length}} + \frac{q_{send}}{|UD|}
\end{aligned} \tag{8}$$

TABLE 2. Comparative summary of security features with other schemes.

Scheme→ Security Features↓	Proposed	[42]	[37]	[36]	[1]
Impersonation attack resilience	✓	✓	✗	✗	✗
Smart-Card Stolen attack resilience	✓	✓	✗	✓	✗
Desynchronization attack resilience	✓	✓	✗	✗	✗
Replay attack resilience	✓	✓	✗	✗	✓
Off-line Password guessing attack resilience	✓	✗	✗	✗	✗
Provision of privacy and anonymity	✓	✓	✗	✗	✗
Perfect forward secrecy	✓	✓	✓	✗	✗

V. PERFORMANCE ANALYSIS

Table 2 presents the security features comparison of proposed protocol and related protocols [1], [36], [37], [42]. It is quite clear that proposed protocol offers additional security features like it ensures smart card stolen attack, desynchronization attack, replay attack and password guessing attack resilience. Our presented protocol provides privacy and anonymity of battery vehicle user $\mathcal{BVU}$. As per literature any protocol can provide privacy and anonymity, if two conditions are being satisfied, namely: (i) if identity of the client is not revealed and (ii) if it is not known that two unique sessions have been initiated either by different or same client at same time. The presented protocol satisfies both of the conditions as it does not reveals the identity of the client during message transmission between participants. Moreover, it is not easily possible for any adversary $\mathcal{A}$ to discriminate two specific initiated sessions from same user. It is possible due to the fact that we have utilized the session specific parameters to compute the pseudo identity to assure the anonymity of battery vehicle users. Therefore, it can be clearly seen in Table 2 that related protocols have flaws in security as compared to proposed protocol.

The performance of presented authentication scheme has been observed in this section. All the cryptographic operations used in the protocol such as $T(enc/dec)$, T_M, $T_{h(.)}$, $T_{\|}$, $T_{\oplus}$ have been implemented on a system having specifications described in the Table 3. The cryptographic operations such as $T(enc/dec)$, T_M, $T_{h(.)}$, $T_{\|}$, $T_{\oplus}$ used in Battery Vehicle User have been implemented using Arduino. The specifications of Arduino have been given in Table 4. This authentication

TABLE 3. System specifications.

Items	Specifications
System	intel Core i5
OS	Ubuntu 19.04
RAM	8GB
Language	Python

TABLE 4. Arduino specifications.

Items	Voltages
Operating Voltage	5 V
Input Voltage (Recomended)	7-12 V
Input Voltage (Limit)	6-20 V
Digital I/O Pins	6-20 V
Input Voltage (Limit)	14 (of which 6 provide PWM output)
PWM Digital I/O Pins	6
Analog Input Pins	6
DC current per I/O Pin	20 mA
DC current for 3.3 V Pin	50 mA
Flash memory	32 KB (A Tmega 328P)
SRAM	2 KB (A Tmega 328P)
SRAM	1 KB (A Tmega 328P)
EEPROM	2 KB (A Tmega 328P)
Clock speed	16 MHZ
Length	68.6 mm
Width	53.4 mm

protocol has been executed 15 times under similar assumptions by taking average of times. Operations $T_{\oplus}$ and $T_{\|}$ takes a very small execution time. So, In the calculation of total time these operations have not been included. The operation $h_{(.)}$ takes 0.000000023 ms while $T_{enc/dec}$ takes 0.0000080 ms either for decryption or encryption and point multiplication takes 0.0000019 ms as an execution time on server side. The operations $h_{(.)}$, point multiplication, $T_{enc/dec}$ takes 5.25, 8.75 and 8.33 ms respectively for $\mathcal{BVU}_{\rangle}$. Table 5 shows the communication, storage and computation cost of the presented protocol and related protocols [1], [36], [37], [42].

TABLE 5. Total computation, communication and storage cost.

Protocol	Computation Cost	Communication Cost	Storage Cost
Proposed	$16T_{h(.)} = 47.2500001$ ms	3456 bits	1184 bits
[42]	$18T_{h(.)} = 47.2500002$ ms	5120 bits	1088 bits
[37]	$20T_{h(.)} + 3T_M = 50.750004$ ms	4704 bits	928 bits
[36]	$26T_{h(.)} = 57.7500001$ ms	8384 bits	2432 bits
[1]	$2T_{enc/dec} = 8.530008$ ms	3232 bits	NA

The execution time of considered cryptographic operations are shown given below:

- T_M: illustrates the execution time of point multiplication
- $T_{enc/dec}$ refers to the execution time of symmetric encryption/decryption
- T_h refers to the execution time of hash function
- $T_{\|}$ represents to the execution time of concatenation
- $T_{\oplus}$ shows the execution time of XoR operation

Figure 5 shows the detailed comparison between number of authenticators and verification time. The proposed and related protocols are labeled horizontally while, computation time (in ms) of protocols is drawn vertically on the graph. Furthermore Figure 5 shows if multiple users are authenticated then what will be the verification cost of proposed and related protocols. It is clear that the computation cost of proposed protocol is less than some of the other related protocols.

For determination of storage and communication costs, the following assumptions have been considered: 160 bits are reserved for random numbers, password, identity and time stamps respectively, 256 bits are reserved for hash function and 512 bits for decryption and encryption [43]. Using these assumptions all the calculations are given in Table 5 in terms of computation, storage and computation cost for our and related protocols [1], [36], [37], [42].

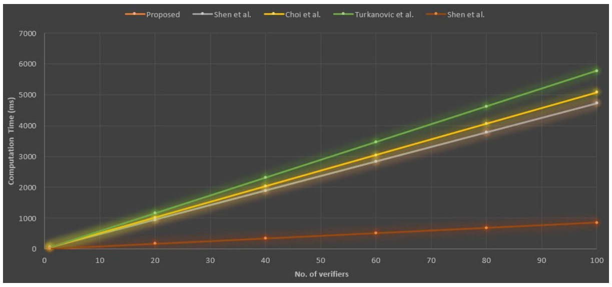


FIGURE 5. Computation cost comparison between proposed and related protocols for multiple authenticators.

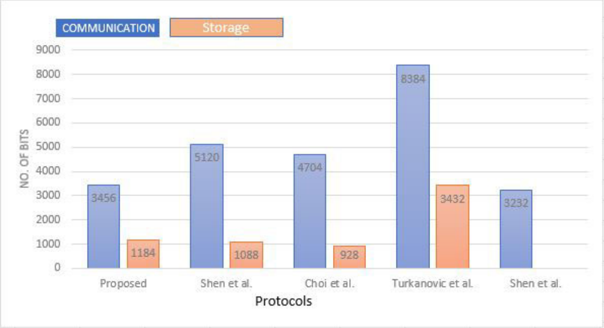


FIGURE 6. Storage and communication cost comparison between proposed and related protocols.

The communication and storage cost comparison of proposed and related protocols is highlighted in Figure 6. Proposed and related protocols are labeled horizontally in graph, while number of bits needed for communication and storage are labeled vertically on the graph. It is obvious that the proposed protocol takes less number of bits for communication while slightly takes more bits for storage as compared to some of the related protocols. It indicates the trade off between performance and security as even our protocol takes few extra bits for storage as compared to related protocols but it provides better security features.

At last, after analyzing Table 2 and Table 5 it can be claimed that even the storage cost of our presented protocol is little bit higher than few of the related protocols but it takes far less communication and computation time as well as provides more security features than the related protocols.

VI. CONCLUSION

In this paper, we have observed and discussed that the SIoV is generating a considerable amount of data endowed with context and social relationship information regarding passengers, vehicles, drivers and the nearby environment. The entire data is gathered and kept at different layers of SIoV infrastructure. In SIoV, the frequent exchange of data and mobility of the interacting vehicles make it a more hostile environment for securing the transfer of data. So, we presented an anonymous key agreement authentication protocol which helps to secure the data generated by the SIoVs regarding passengers, vehicles, drivers and the surrounding environment. The designed protocol makes the communication secure among different entities. In the proposed protocol, we aim to confront the dark side of smart grids, mainly privacy and security-related issues. In particular, a session key is used to guarantee the safety over communication channels among both the parties. We have analyzed the proposed protocol formally and informally to determine its security strength. In order to ensure the validation related to efficiency and security, we present a detailed comparison between the proposed and related protocols. It is clear that the proposed protocol is more secure against various attacks and has some additional security features as compared to related protocols. Furthermore, the performance analysis reveals that our protocol is more efficient in terms of communication, computation and storage overhead. Therefore, we can claim that the proposed protocol is appropriate and feasible for resource constrained environment.

REFERENCES

[1] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Gener. Comput. Syst.*, vol. 78, pp. 956–963, Jan. 2018.

[2] S. Wen, W. Zhou, J. Zhang, Y. Xiang, W. Zhou, and W. Jia, "Modeling propagation dynamics of social network worms," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 8, pp. 1633–1643, Aug. 2013.

[3] C.-M. Huang, C.-H. Shao, S.-Z. Xu, and H. Zhou, "The social Internet of Thing (S-IOT)-based mobile group handoff architecture and schemes for proximity service," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 3, pp. 425–437, Jul. 2017.

[4] 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 Trans. Ind. Appl.*, early access, Jan. 13, 2020, doi: 10.1109/TIA.2020.2966160.

[5] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, "A secure cloud computing based framework for big data information management of smart grid," *IEEE Trans. Cloud Comput.*, vol. 3, no. 2, pp. 233–244, Apr. 2015.

[6] K. Mansoor, A. Ghani, S. Chaudhry, S. Shamshirband, S. Ghayyur, and A. Mosavi, "Securing IoT-based RFID systems: A robust authentication protocol using symmetric cryptography," *Sensors*, vol. 19, no. 21, p. 4752, Nov. 2019.

[7] P. Guo, J. Wang, X. H. Geng, C. S. Kim, and J.-U. Kim, "A variable threshold-value authentication architecture for wireless mesh networks," *J. Internet Technol.*, vol. 15, no. 6, pp. 929–935, 2014.

[8] S. A. Chaudhry, T. Shon, F. Al-Turjman, and M. H. Alsharif, "Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems," *Comput. Commun.*, vol. 153, pp. 527–537, Mar. 2020.

[9] J. Shen, T. Zhou, C.-F. Lai, J. Li, and X. Li, "Hierarchical trust level evaluation for pervasive social networking," *IEEE Access*, vol. 5, pp. 1178–1187, 2017.

[10] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.

[11] S. Hussain and S. A. Chaudhry, "Comments on 'biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment,'" *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10936–10940, Dec. 2019.

[12] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Rahman, and M. N. Saqib, "Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key," *Int. J. Commun. Syst.*, vol. 32, no. 16, p. e4139, Nov. 2019.

[13] W. Kempton and J. Tomić, "Vehicle-to-grid power fundamentals: Calculating capacity and net revenue," *J. Power Sources*, vol. 144, no. 1, pp. 268–279, Jun. 2005.

[14] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, 2013.

[15] S. Kumari, X. Li, F. Wu, A. K. Das, K.-K.-R. Choo, and J. Shen, "Design of a provably secure biometrics-based multi-cloud-server authentication scheme," *Future Gener. Comput. Syst.*, vol. 68, pp. 320–330, Mar. 2017.

[16] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "Smart grid technologies: Communication technologies and standards," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 529–539, Nov. 2011.

[17] F. Kennel, D. Görges, and S. Liu, "Energy management for smart grids with electric vehicles based on hierarchical MPC," *IEEE Trans. Ind. Informat.*, vol. 9, no. 3, pp. 1528–1537, Aug. 2013.

[18] D. S. Callaway and I. A. Hiskens, "Achieving controllability of electric loads," *Proc. IEEE*, vol. 99, no. 1, pp. 184–199, Jan. 2011.

[19] S. Han, S. Han, and K. Sezaki, "Development of an optimal vehicle-to-grid aggregator for frequency regulation," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 65–72, Jun. 2010.

[20] C. Guille and G. Gross, "A conceptual framework for the vehicle-to-grid (V2G) implementation," *Energy Policy*, vol. 37, no. 11, pp. 4379–4390, Nov. 2009.

[21] K. Mahmood, X. Li, S. A. Chaudhry, H. Naqvi, S. Kumari, A. K. Sangaiah, and J. J. P. C. Rodrigues, "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure," *Future Gener. Comput. Syst.*, vol. 88, pp. 491–500, Nov. 2018.

[22] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "A survey on smart grid potential applications and communication requirements," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 28–42, Feb. 2013.

[23] K. Mahmood, H. Naqvi, B. A. Alzahrani, Z. Mehmood, A. Irshad, and S. A. Chaudhry, "An ameliorated two-factor anonymous key exchange authentication protocol for mobile client-server environment," *Int. J. Commun. Syst.*, vol. 31, no. 18, p. e3814, Dec. 2018.

[24] M. Stegelmann and D. Kesdogan, "Design and evaluation of a privacy-preserving architecture for vehicle-to-grid interaction," in *Proc. Eur. Public Key Infrastruct. Workshop*. Berlin, Germany: Springer, 2011, pp. 75–90.

[25] H. Nicanfar, S. Hosseininezhad, P. TalebiFard, and V. C. M. Leung, "Robust privacy-preserving authentication scheme for communication between electric vehicle as power energy storage and power stations," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2013, pp. 3429–3434.

[26] C. Rottondi, S. Fontana, and G. Verticale, "Enabling privacy in vehicle-to-grid interactions for battery recharging," *Energies*, vol. 7, no. 5, pp. 2780–2798, Apr. 2014.

[27] J. K. Liu, M. H. Au, W. Susilo, and J. Zhou, "Enhancing location privacy for electric vehicles (at the right time)," in *Proc. Eur. Symp. Res. Comput. Secur.* Berlin, Germany: Springer, 2012, pp. 397–414.

[28] S. Kumari, P. Chaudhary, C.-M. Chen, and M. K. Khan, "Questioning key compromise attack on Ostad-Sharif et al.'s authentication and session key generation scheme for healthcare applications," *IEEE Access*, vol. 7, pp. 39717–39720, 2019.

[29] 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.

[30] K. Park, Y. Park, A. K. Das, S. Yu, J. Lee, and Y. Park, "A dynamic privacy-preserving key management protocol for V2G in social Internet of Things," *IEEE Access*, vol. 7, pp. 76812–76832, 2019.

[31] S. Garg, K. Kaur, G. Kaddoum, F. Gagnon, and J. J. P. C. Rodrigues, "An efficient blockchain-based hierarchical authentication mechanism for energy trading in V2G environment," 2019, *arXiv:1904.01171*. [Online]. Available: http://arxiv.org/abs/1904.01171

[32] S. Zhang, G. Wang, M. Z. A. Bhuiyan, and Q. Liu, "A dual privacy preserving scheme in continuous location-based services," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 4191–4200, Oct. 2018.

[33] S. Zhang, X. Mao, K.-K.-R. Choo, T. Peng, and G. Wang, "A trajectory privacy-preserving scheme based on a dual-K mechanism for continuous location-based services," *Inf. Sci.*, vol. 527, pp. 406–419, Jul. 2020.

[34] J. Shen, H. Tan, S. Moh, I. Chung, and J. Wang, "An efficient RFID authentication protocol providing strong privacy and security," *J. Internet Technol.*, vol. 17, no. 3, pp. 443–455, 2016.

[35] Z. Yang, S. Yu, W. Lou, and C. Liu, "P^2: Privacy preserving communication and precise reward architecture for V2G networks in smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 697–706, Dec. 2011.

[36] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Netw.*, vol. 20, pp. 96–112, Sep. 2014.

[37] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, and D. Won, "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 14, no. 6, pp. 10081–10106, Jun. 2014.

[38] H. Wang, B. Qin, Q. Wu, L. Xu, and J. Domingo-Ferrer, "TPP: Traceable privacy-preserving communication and precise reward for vehicle-to-grid networks in smart grids," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 11, pp. 2340–2351, Nov. 2015.

[39] A. Abdallah and X. S. Shen, "Lightweight authentication and privacy-preserving scheme for V2G connections," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2615–2629, Mar. 2017.

[40] H. Liu, H. Ning, Y. Zhang, and L. T. Yang, "Aggregated-proofs based privacy-preserving authentication for V2G networks in the smart grid," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1722–1733, Dec. 2012.

[41] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, Dec. 2011.

[42] J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "Privacy-preserving and lightweight key agreement protocol for V2G in the social Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2526–2536, Aug. 2018.

[43] R. Ali and A. K. Pal, "Three-factor-based confidentiality-preserving remote user authentication scheme in multi-server environment," *Arabian J. Sci. Eng.*, vol. 42, no. 8, pp. 3655–3672, Aug. 2017.

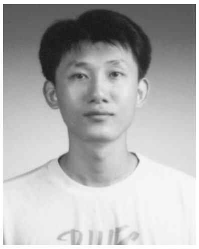
SHAFIQ AHMED received the M.C.S. degree from COMSATS University Islamabad–Sahiwal, Pakistan, in 2017, where he is currently pursuing the M.S. degree in computer science. His research interests include network security, healthcare authentication, and authenticated key agreement scheme. He was awarded Silver Medal.

SARU KUMARI received the Ph.D. degree in mathematics from Chaudhary Charan Singh University, Meerut, India, in 2012. She is currently an Assistant Professor with the Department of Mathematics, Chaudhary Charan Singh University. She has published more than 133 research articles in reputed international journals and conferences, including 115 publications in SCI-indexed journals. Her current research interests include information security and applied cryptography. She is a technical program committee member for many international conferences. She is on the editorial board of more than 12 journals of international repute, including seven SCI journals. She has served as the Lead/Guest Editor for four special issues in SCI journals of Elsevier, Springer, and Wiley.

MUHAMMAD ASAD SALEEM received the M.C.S. degree (Hons.) from COMSATS University Islamabad–Sahiwal, Pakistan, in 2018, where he is currently pursuing the M.S. degree in computer science. His research interests include lightweight cryptography, healthcare authentication, and authenticated key agreement scheme. He was awarded Campus as well as Institute Gold Medal.

KADAMBRI AGARWAL received the Ph.D. degree in computer science and engineering from Uttarakhand Technical University, Dehradun, India. She has been working as an Associate Professor with the Department of Computer Science and Engineering, Bhagwati Institute of Technology and Science, Ghaziabad, India. She has also worked with the Raj Kumar Goel Institute of Technology (RKGIT), Ghaziabad, and the Institute of Management and Research, Ghaziabad. She has more than ten years teaching experience. She has published/ presented several articles in journals/conferences of repute.

KHALID MAHMOOD received the M.S. degree in computer science from Riphah International University, Islamabad, Pakistan, in 2010, and the Ph.D. degree in computer science from International Islamic University, Islamabad, in 2018. The title of his Ph.D. dissertation is Secure Authenticated Key Agreement Schemes for Smart Grid Communication in Power Sector. He is currently working with COMSATS University Islamabad–Sahiwal. His research interests include lightweight cryptography, smart grid authentication, authenticated key agreement schemes, and design and development of lightweight authentication protocols using lightweight cryptographic solutions for diverse infrastructures or systems, such as vehicular ad hoc networks, smart grid, and telecare medical information systems (TMIS).



MING-HOUR YANG (Member, IEEE) received the Ph.D. degree in computer science and information engineering from National Central University, Taiwan. His research interests include network security and system security with particular interests on security issues in RFID and NFC security communication protocols. Topics include: mutual authentication protocols, secure ownership transfer protocols, polymorphic worms, and tracing mobile attackers.

• • •