IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 10, 2019, accepted October 2, 2019, date of publication October 8, 2019, date of current version October 24, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2946241

LSPP: Lightweight and Secure Payment Protocol for Dynamic Wireless Charging of Electric Vehicles in Vehicular Cloud

MOJTABA TAJMOHAMMADI[1], SAYYED MAJID MAZINANI[1], MORTEZA NIKOOGHADAM[1], AND ZAHRAA AL-HAMDAWEE[2]

[1]Department of Computer Engineering and Information Technology, Imam Reza International University, Mashhad 553-91735, Iran
[2]Department of Electrical Engineering, Imam Reza International University, Mashhad 553-91735, Iran

Corresponding author: Sayyed Majid Mazinani (smajidmazinani@imamreza.ac.ir)

ABSTRACT Dynamic wireless charging as viable alternative to plug-in vehicles has contributed to a substantial reduction in stopping time at the charging station. Nevertheless, the sequential charging of electric vehicles can reveal the user's personal information, including their location, by using bill and payment systems. Not only do these systems need to support location privacy, but they also should be traceable by trusted authority when cars are stolen. In this paper, a lightweight and secure payment protocol for dynamic wireless charging of electric vehicles in vehicular cloud have been proposed. In addition, payment system requirements and wireless charging of electric vehicles, including architecture, security, speed, location privacy, anonymity, price flexibility and resistance to possible attacks have been described. Low-cost operations like XOR and concatenation have been used to achieve security and speed. The performance and security of LSPP, based on both formal analysis using AVISPA tool and informal analysis considering probable attack scenarios have been analyzed and compared with past methods. In conclusion, with regard to security and efficiency, payment system proposed works well and fulfills the requirements of the wireless charging of electric vehicles.

INDEX TERMS Secure payment system, wireless charging, vehicular cloud, location privacy, dynamic wireless power transfer.

I. INTRODUCTION

In 2010, the first commercial dynamic wireless charging (DWC) electric vehicle (EV), the online electric vehicle project at KAIST, was selected as one of the best innovations to be a step forward in protecting the environment and preventing contamination [1].

In this project, EV can be charged with on-road energy segments while they are on the move and can reduce the time of recharging [2]. Electric engines are practical alternatives to combustion engines in order to eliminate pollution problems. Today, air pollution is of more concern for people than it was; therefore, increased fossil fuel consumption in combustion engines is criticized more than ever. The most important reason to substitute electric engines for combustion engines is their high efficiency.

Combustion engines consume only 30% of their tank fuel energy and lose most energy through heat [3]. While the dynamic charging project has reached 80% energy efficiency at a distance of 10 cm between the energy segment and EV [2]. However, the battery capacity of EV is much less than that of the combustion engine tank; therefore, EV travels shorter distance. Due to smaller battery employed in plug-in EV methods such as [4] and [5], recharging times at certain intervals at designated stations have increased.

Some of the disadvantages associated with plug-in EV method include lack of charging stations and increased stopping times for charging vehicles. Therefore, although the DWC scheme can be a viable alternative compared with plug-in EV scheme, this scheme still needs to be charged continuously throughout the day, causing a negative effect on the user's privacy. In other words, the EV's location history as well as the places of interest could be collected and linked together. The information collected can be used for crimes such as kidnapping or vehicle theft. For instance, when

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

a vehicle theft is committed, the drivers wants to trace the stolen vehicles. Moreover, unauthorized vehicles must be traceable with no restriction by a trusted authority (TA), like the police.

When it comes to using DWC, EV is often essential to be charged along the way. Therefore, there should be a proper bill and payment scheme to control the authentication and charge between the energy segment and the EV. In addition, this scheme should protect the location privacy of the EV's users and if there is a problem, unauthorized users can be tracked down by TA. There are several payment methods for DWC [6]–[9], yet they have security weaknesses. The methods proposed have a high computational cost, which is not appropriate for EVs bill and payment schemes; since they are moving fast, the payment system should be fast. In this paper, we have designed fast and secure payment system that is suitable for DWC of EVs, satisfying the requirements and expectations mentioned.

Our Contributions:

Our contributions can be summarized in three aspects as follows:

- We present a lightweight and secure payment method for DWC of EV that (a) it uses low-cost operations including concatenation, XOR and symmetric cryptography rather than costly operations which has been used in previous methods, (b) it withstands the known attacks and ensured security, traceability, privacy and anonymity, (c) it is far better than the recent methods in terms of efficiency and speed, (d) it has a network model compatible with advanced technologies.
- We simulate security in the open source fixed point model checker (OFMC) backend model and verify the validity by using widely accepted automated validation of internet security protocols and applications (AVISPA) tool.
- We implement the proposed method with high level protocol specification language (HLPSL) language.

II. RELATED WORK

There is no firm agreement on how to categorize the payment charging system for EVs from the perspective of operations. We categorizes payment charging system for EVs into static charging payment and dynamic charging payment system. These are defined as follows:

A. STATIC CHARGING PAYMENTS

Important payment methods for plug-in (static) EVs have been found in two methods: 1. Au et al method [5] and 2. Nicanfar et al method [4]. In Au et al method [5], a new payment system has been proposed in order to increase privacy in EVs. In this way, the authors equip the EVs with a chipset that is a read-only memory during the initial registration process. During the registration process, the user must meet the supplier to open an account and deposit a minimum amount of D dollars and save it on his account. In the charging process, the vehicle chipset implements an interactive protocol in order to establish communication between the energy segment and supplier to check the amount of deposit anonymously. In this method [5] bilinear pairing and zero-knowledge proofs have been used to validate user accounts for the service provider. The charging process lasts 10 seconds, hence it is not suitable for DWC.

In Nicanfar et al method [4] it has been used the smart grid as a trusted entity. Since EVs need to be authenticated with an energy segment, they have used a nickname that only the smart grid can authenticate the EVs. EVs must change their nickname after using the smart grid. Despite all the advantages attributed to this method EVs user may pay the charge without being assigned the charge by smart grid so that the EVs cannot complain. Further, this method cannot track the illegal users.

B. DYNAMIC CHARGING PAYMENTS

Hossein *et al.* [6], [7] has proposed a payment method for DWC of EV. He provides two mutual authentication mechanisms, namely a hash-based authentication and direct authentication to confirm the communication between EV and energy segment that can be used for various EV speeds. By using the game theoretical approach, he has proposed a wireless energy transfer with security and privacy. In the next method, Zhao *et al.* [8] suggests a secure and privacy-preserving bill scheme for DWC in which users are able to purchase electrical energy from the power provider and recharge their EVs in an anonymous and un-linkable way. It has been assumed that each energy segment transmits a constant amount of energy to the EV. Rezaeifar *et al.* [9] puts forward a new payment system to minimize communication costs and system complexity. In order for anonymity and privacy, she uses a different token model that cannot be tracked in this payment method. The method is based on user accounts and the token does not have any specific value. Users can spend any amount of money needed on their deposits. In this method, the ELGAMAL-ECC protocol is used for secure communication between the EV and the bank. The purpose of this protocol is to create a secure key among the parties. After the secure key has created, all messages are encrypted with this key and then transmitted to the destination through the network. The proposed work of Rezaeifar [9] has four phases: Setup Phase, Token Withdrawal Phase, Charging Phase and Redeeming Phase. All setup and registrations take place over secure channel and each entity receives the parameters and makes their own keys. This method follows the ECC method for encryption and decryption and the binary authentication tree (BAT) method for the signature. As the author described BAT in section 4.2, the BAT signature uses bilinear pairing to achieve verification. After initial authentications, the user can make an account with the bank to receive tokens that can be used for charging services on the road. Users who have a valid account connect to the bank through VANET. For the requested token, they send the message contained the public key +Kj, the identity PIDj, and the root of hash chain w_0 then the bank will give them a token. The token consists of new public key +Kj, new w_0 , new PIDj and T_b related to this token. User sends these parameters and N segments it need to service provider. Service provider after authenticates the user, sends hash values to it. User spends first value of the hashes for first segment, after receiving a charge from the first segment, the user reveals another value of the hash chain to receive a charge from the next segment. This process will continue until the user receives a charge from the N^{th} segment. In last phase, the service provider sends a message contains hash values and its identity to bank for redeeming token.

The disadvantage of methods [6], [7] is the poor protection. Therefore, energy segment can link all authentication data and track down EV which is in contrast to the principle of privacy. The objection to method [8] is that it cannot detect double spending, so EV can charge twice as much money as it paid and receive some free charge. Method [9] has a man in the middle attack. In ELGAMAL-ECC protocol, two entities Alice and Bob, after concluding an agreement on the initial parameters of the elliptic curve cryptography, they choose private keys and agree on a secret shared key. In this protocol, mutual authentication is not performed, thus occurring man in the middle attack. This attack occurs in the setup phase of Rezaeifar *et al.* [9]. The major disadvantage for all the methods mentioned above is high computational costs, making them be inappropriate for fast payment systems.

Therefore, in this paper, we propose a lightweight and secure payment protocol for dynamic wireless charging of electric vehicles in vehicular cloud (LSPP). This system meets the requirements, including security, speed, privacy, anonymity and resistance to possible attacks. It also has the ability to track stolen cars. In order to improve the quality of the communication between different entities, we have suggested using the 5G network and vehicular cloud instead of vehicular ad hoc network (VANET) and roadside unit (RSU) because of its advantages.

III. PRELIMINARIES

In this section, we briefly review the relevant knowledge in order to better understand our scheme.

A. WIRELESS CHARGING TECHNOLOGY

The wireless charging system consists of the following components [2]:

1. An electricity supplier from the power grid system transfers energy to the energy segment.

2. An energy segment consists of a cable module installed on the road, which is responsible for transporting energy to the EV.

3. A pickup module for wireless power transmitter (WPT) that is installed under EV that has the task of transferring and charging the EV.

4. The duty of the regulator is to charge the battery while driving.

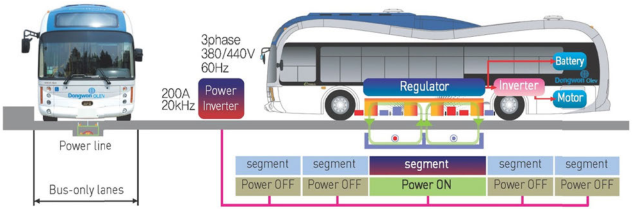


FIGURE 1. Wireless charging [2].

Figure 1 shows the general scheme of the wireless charging system. EV receives power wirelessly through the shaped magnetic field in resonance (SMFIR) technology [10]. This inductive charging system technology safely delivers high amounts of energy to an EV while it is stationary or in motion [11]. This technology is one transmitter to one receiver. Wireless charging occurs when the EV is moving on the road with an underground power supply. The numerous number of energy segments can be installed anywhere on the road; furthermore, the battery can be well energized. The charge transfer operation will continue depending on the battery level until the charge is completed. In the system defined in this paper, it is possible to charge the variable, depending on the need and the amount of money the person has. The energy segment is only turned on when the EV is authenticated and is immediately turned off after delivering the charge, disallowing the EV behind to be charged. The underground power system creates a two-dimensional magnetic field by moving the EV, which meets international regulations, including safety.

In [12], the authors discussed regulatory safety issues related to cable module, pickup module, electromagnetic field (EMF), electromagnetic interference (EMI) and carried out practical safety experiments. According to their research, they have concluded that the system is immune to disturbance. In the method [13], a detailed review of wireless power transmission has been carried out and covered many aspects, including the distance between the transmitter and receiver and the cost of technology. In [14] the authors succeeded in achieving 90.34% efficiency for wireless power transmission and the system works continuously without faults. Also in [15] by measuring output power, the authors have shown that more than 11 W can be transmitted using a 2mm aluminum plate for the first generation of DWC. In fact, it has three generation [11]: 1. Electric small cart, 2. Bus and 3. SUV. The unique characteristic of SMFIR technology is the ability to transmit high power more than 100 KW for heavy vehicles [12].

B. 5G NETWORK TECHNOLOGY

As a result of increasing the number of vehicles and traffic load on vehicular networks such as VANET, wireless charging payment technology requires a strong network to withstand heavy traffic. Thus, the LSPP uses the 5G cellular network for the exchange of heavy traffic. The 5G requires a major and special change in the architecture of the wireless

TABLE 1. Comparison between different generations of cellular networks.

Technology Feature	1G	2G	3G	4G	5G
Start/Deployment	1970-1980	1990-2004	2004-2010	Now	Soon(probably 2020)
Data Bandwidth	2Kbps	64Kbps	2Mbps	1Gbps	Higher than 1Gbps
Technology	Analog Cellular	Digital Cellular	CDMA2000, UMTS, EDGE	Wi-max LTE Wi-Fi	wwww
Service	Mobile Telephony (Voice)	Digital Voice, SMS, Higher capacity packetized data	Integrated high quality audio, video and data	Dynamic Information access, wearable devices	Dynamic Information access, wearable devices with AI Capabilities
Multiplexing	FDMA	TDMA,CDMA	CDMA	CDMA	CDMA
Switching	Circuit	Circuit, Packet	Packet	All Packet	All Packet
Core Network	PSTN	PSTN	Packet N/W	Internet	Internet

cellular to meet the needs of users to solve the system's future challenges .16]. According to the cisco corporation, the data volume has doubled between 2010 and 2011 and traffic is expected to increase by 1,000 times until 2020 [17]. Due to having advanced features [18], the 5G network will become the top technology in the near future. The 5G network architecture consists of a user terminal and a number of independent and self-organized radio access technologies [19]. There are various dimensions for comparing different generations. But what determines the policies and investment of this field is the speed of data transfer, latency, the technology used in the transfer and the type of service provided to users in each generation. Implementing techniques to provide a system supporting the following specifications is the main goal of the 5G [18]:

- Increasing data volume in each area up to 1000 times.
- Increasing the number of connected devices 10 to 100 times.
- Increasing user data by 10 to 100 times.
- Increasing battery life by up to 10 times for power-assisted devices.
- In the end-to-end communication, the delay reduction is up to 5 times.

5G capabilities:

- **High Speed**

The fifth generation of wireless systems should significantly increase the speed of data transfer and, on the contrary, reduce the cost of telecommunication services as much as possible. Most estimations predict at least 10 Gb / s and 800 Gb / s data transfer rates for 5G networks [17].

- **Network Reliability and Availability**

One of the features that are predicted for the 5G technology is reliability and availability. 5G brings a widespread global wireless web, the real wireless world with no access restrictions and regional issues, so the user can connect to multiple wireless networks and move in them without interruption [18]. As a result, connecting to all networks and transferring data on multiple paths will be possible [23].

- **Reducing Latency**

In the 5G technology, the latency is estimated to be only 1ms (about 50 times faster than 4G) and its reliability should be so high that cars without drivers and other tools that will connect to the network will continue to work without problems [15], [24].

- **Reducing Energy Consumption**

In 5G systems, due to the increased battery life of the used terminals and the appropriate coverage in the environment, the output power of the antenna is reduced, resulting in an increase in the shelf life of the equipment [19].

In fact, users expect that the fifth generation of mobile cellular networks will streamline information at higher speeds, provide better quality services, minimize delays and automate the provision of better quality service, while all these requirements should be provided at a cheaper price [20].

- **Security**

Resistance to a variety of attacks is a feature of the fifth-generation network. In [21], [22] The authors have done a thorough security analysis on 5G. They have investigated possible attacks and provided Intrusion Detection System to deal with them. Table 2 shows these possible attacks:

TABLE 2. 5G attacks.

Attacks	Description
Distributed Denial of Service	Resources or bandwidth of the target system is flooded by multiple systems.
Ping flood	Resources or bandwidth of the target system is flooded by multiple systems.
IP port scan	Target system is scanned for available active ports and the possible vulnerabilities.
SYN flood	SYN packets are transmitted by attacker in succession making the system busy and unavailable for legitimate user.
SQL injection	Malicious SQL statements are injected for execution to make unauthorized changes.
DNS hijacking	Redirecting DNS queries to malicious server.
Fraggle attack	Sending spoofed UDP packets for broadcast in the network.
Bandwidth Spoofing	Flooding a network to an extent that they start affecting legitimate traffic
IP spoofing	Creation of IP packets with forged IP address to conceal source identity

C. VEHICULAR CLOUD TECHNOLOGY

Vehicular cloud are promising and futuristic technology due to its special features such as traffic management, road safety and etc.

The increasing number of vehicles involves an increase in their requirements. There are different proposed plans to satisfy these requirements, namely the Vehicular Cloud, an integration of the two concepts Vehicular Network and Cloud Computing [30], which has attracted many researchers.

Since the payment system plan needs to be always online and scalable in order to handle many users and to prevent it from being bottlenecked, we too propose our secure payment system based on vehicular cloud.

D. PAYMENT SYSTEM REQUIREMENT

The general requirements of online payment systems include security, reliability and scalability to support users and merchants without reducing performance, anonymity, flexibility, convergence and efficiency. In wireless charging payments of EV, some of the requirements are more important such as security, performance and anonymity.

- **Security**

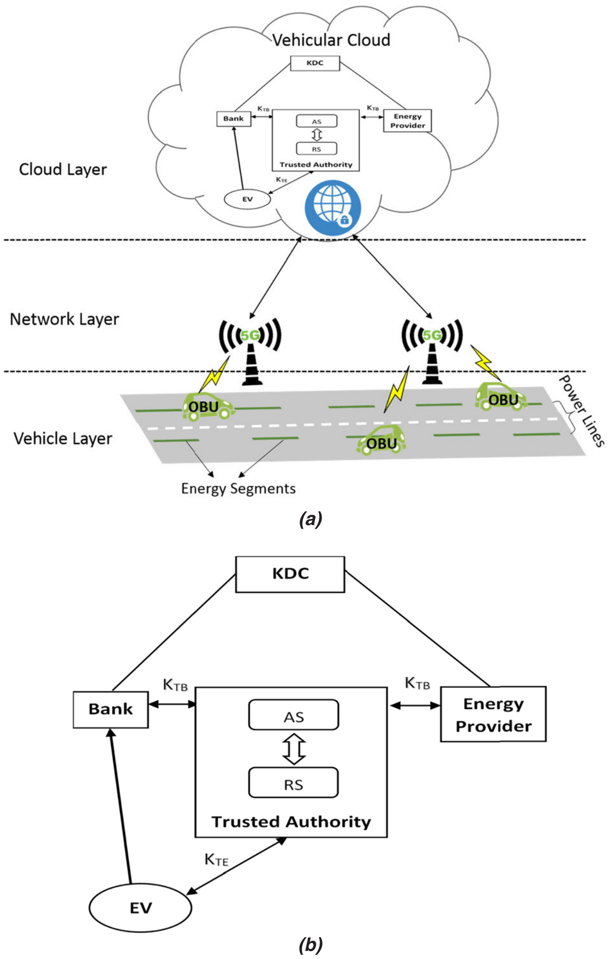
The payment method must be safe to protect users against possible attacks that may occur in public network such as sniff, reply attack and etc.

- **Fast Authentication** One of the most important features of the wireless charging payment of EV is that the payment system must be fast because the vehicles are moving at high speed.
- **Anonymity & Location Privacy** The EV needs to be charged several times during the day, which leads to revelation concerning the user's location privacy. Consequently, user's location privacy and anonymity are two important security requirements to be provided.
- **Traceability** Tracking is another issue that should be considered because the TA should be able to remove illegal user from the system. This entity should be able to trace it anonymously at any time, even without user permission.
- **Price Flexibility** The payment method must guarantee the changeable price. An electronic payment method should support changeable prices that allows users to spend as much money as they need

IV. SYSTEM MODEL

In our method, we assume three layers of the vehicle layer, network layer and cloud layer. In vehicle layer, as we explained in section III.A, the EVs receive the charge wirelessly on the move. As shown in figure 2, network layer has the duty to communicating between layers by 5G technology. Cloud layer consist of five entities as we described below:

- **Key Distribution Center (KDC)** In symmetric cryptosystems, KDC is a trusted third party that has duty to establish a shared secret key between two entities.
- **Energy provider (EP)** The EP is a company that supplies electricity of EVs.
- **Bank** The bank is trusted entity that has duty to opening an account with EVs credentials and the amount of money they are supposed to deposit in that account.
- **TA** The TA is a trusted authority entity consist of two parties, register server (RS) and authentication server (AS). This entity has the duty to registering and authenticating EVs.
- **EV** This entity has the role of user.



(a)

(b)

FIGURE 2. (a) The Proposed system model (b) vehicular cloud entities.

V. LSPP CONSTRUCTION

In this section, our proposed method is carefully explained.

The LSPP process has been performed in 5 phases. These phases are pre-registration, registration, authentication, charging and payment. All communications between entities are established through the 5G high-speed network and linked through each other. In figure 2, the general system model has been presented. In the following subsections, the details of the method have been expressed. Moreover, Table 3 shows notations with their meanings.

A. PRE-REGISTRATION PHASE

The LSPP is implemented on a public 5G network and vehicular cloud which requires safe access to this network. At this phase, each entity should get the symmetric key from the KDC for its future communications. There are currently strong protocols for this part such as the Kerberos version 5 [26], the best option is to use the standard protocols that have high security. In order to communicate with the TA, the bank agrees on K_{TB} symmetric key with the KDC, the EP agrees on K_{TP} symmetric key with the KDC and the EV agrees on K_{TE} with KDC. From here, they will be

TABLE 3. Notation and their meanings.

Notation	Meaning
TA	Trusted Authority
KDC	Key Distribution Center
EV	Electric Vehicle
EP	Energy Provider
OBU	On-Board Unit
K_{TB}	Symmetric Key Between Bank & TA
K_{TE}	Symmetric Key Between EV & TA
K_{TP}	Symmetric Key Between EP & TA
SK	Symmetric Secure Key
ID_x	Identifier of Entity x
e,b,x	Random Numbers
s	Initial Point of PRBG
PRBG	Pseudo Random Bit Generator
D	EV Deposit Money in Dollars
a	Number of Chunks Purchased
d	Price of Each Chunk
P	Price of Each Segment
T_x	Timestamp of Entity x
N	Number of Requested Energy Segments
q	Number of Chunks Bought
r	Number of Chunks For Each Energy Segment
nonce	One-time Number
h()	One-way Hash Function
EK()	Symmetric Encryption With Key K
DK()	Symmetric Decryption With Key K
‖	Concatenation Operation
⊕	XOR Operation

able to transfer messages using these keys with symmetric cryptography.

Given that entities are dynamic, if the number of these entities is increased or decreased, the task of the KDC becomes more important. In case that an EP company which has disbanded, the KDC should deal with it and remove the relevant keys. When it comes to adding a new entity, KDC must make and distribute the corresponding keys. As mentioned previously, the Kerberos version 5 perfectly fulfills these features and is very reliable.

B. REGISTRATION PHASE

This phase has two steps, the general schema of the registration phase has been shown in the figure 3:

First Section: After each entity receives its symmetric keys, the EV users go to the bank to open an account and sign up for LSPP with a valid identification. Since the user has a face-to-face visits to the bank, it is securely communicated. But the bank must register the user in the TA for registration in the LSPP. Follow the steps below:

Step 1 : The EV user first chooses two random numbers e, r and compute $sj = e \bigoplus r$, then generates a hash according to formula $W = h(j \parallel r)$. By showing their credentials ID_E and giving D dollars for deposit and parameter W, the bank opens an account with their credentials and the amount of money they are supposed to deposit in that account.

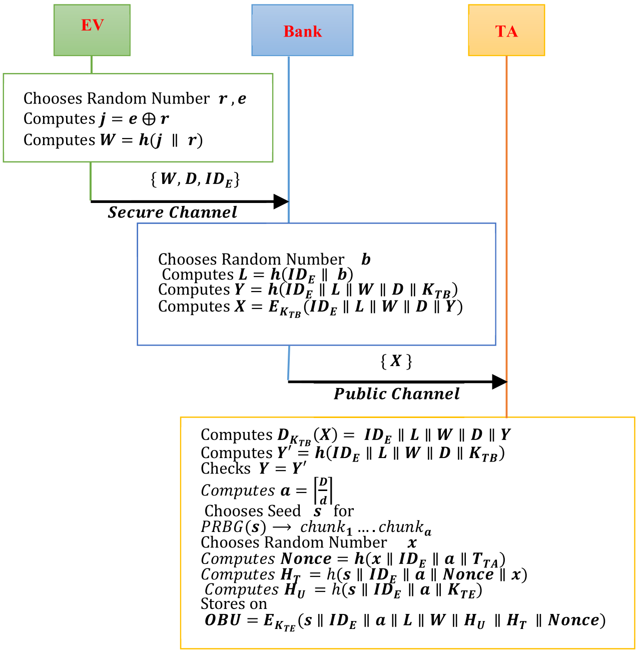

EV
Bank
TA
Chooses Random Number r, e
Computes $j = e \oplus r$
Computes $W = h(j \parallel r)$
$\{W, D, ID_E\}$
Secure Channel
Chooses Random Number b
Computes $L = h(ID_E \parallel b)$
Computes $Y = h(ID_E \parallel L \parallel W \parallel D \parallel K_{TB})$
Computes $X = E_{K_{TB}}(ID_E \parallel L \parallel W \parallel D \parallel Y)$
$\{X\}$
Public Channel
Computes $D_{K_{TB}}(X) = ID_E \parallel L \parallel W \parallel D \parallel Y$
Computes $Y' = h(ID_E \parallel L \parallel W \parallel D \parallel K_{TB})$
Checks $Y = Y'$
Computes $a = \left\lceil \frac{D}{d} \right\rceil$
Chooses Seed s for
$PRBG(s) \longrightarrow chunk_1 \ldots . chunk_a$
Chooses Random Number x
Computes $Nonce = h(x \parallel ID_E \parallel a \parallel T_{TA})$
Computes $H_T = h(s \parallel ID_E \parallel a \parallel Nonce \parallel x)$
Computes $H_U = h(s \parallel ID_E \parallel a \parallel K_{TE})$
Stores on
$OBU = E_{K_{TE}}(s \parallel ID_E \parallel a \parallel L \parallel W \parallel H_U \parallel H_T \parallel Nonce)$

FIGURE 3. The proposed registration phase.

Step 2 : After the bank opens the account with the amount of money D for the EV user, it performs the following tasks:

a. The bank chooses a random number b.

b. The bank computes $L = h(ID_E \parallel b)$, $Y = h(ID_E \parallel L \parallel W \| D \parallel K_{TB})$, $X = E_{K_{TB}}(ID_E \| L \parallel W \parallel D \parallel Y)$

c. The bank sends X via public channel to TA for registration in LSPP.

Step 3 : After receiving the parameters, TA tries to authenticate them in accordance with the following steps:

a. The TA computes $D_{K_{TB}}(X) = ID_E \parallel L \parallel W \| D \parallel Y$, $Y' = h(ID_E \parallel L \parallel W \| D \parallel K_{TB})$

b. The TA checks $Y = Y'$.

Step 4 : When TA ensures the accuracy of the data, it divides the deposit amount D dollars into the price of each chunk that is equal to d dollars. According to the formula $a = \lceil \frac{D}{d} \rceil$, this will determine how many chunks the TA should allocate to the user. If this value is equal to a, then the number of a chunks is assigned to that user. In the following:

a. The TA computes $a = \lceil \frac{D}{d} \rceil$.

b. The TA chooses seed s for $PRBG(s) \longrightarrow chunk_1 \ldots chunk_a$.

c. The TA chooses random number x.

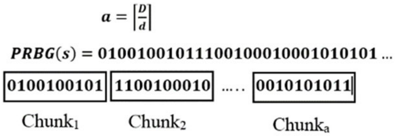

$a = \lceil \frac{D}{d} \rceil$
$PRBG(s) = 0100100101110010001000101010 1 \ldots$
0100100101
1100100010
.....
0010101011
Chunk₁
Chunk₂
Chunkₐ

FIGURE 4. Chunk definition.

d. The TA computes $H_T = h(s \parallel ID_E \| a \parallel Nonce \parallel x)$, $H_U = h(s \| ID_E \parallel a \parallel K_{TE})$ and $Nonce = h(x \parallel ID_E \| a \parallel T_{TA})$.

After completing the steps above, the TA stores the $E_{K_{TE}}(s \parallel ID_E \| a \parallel L \parallel W \parallel H_U \parallel H_T \parallel Nonce)$ values as encrypted on OBU.

Definition: The TA selects the initial value s then generates a pseudo random bit by the PRBG function. The TA separates every 10 bits (each amount that is agreed) and names them as chunk. In order to calculate the amount of the user's money in terms of chunk, formula $a = \lceil \frac{D}{d} \rceil$ is used. If this value is equal to a, then the number of a chunks is assigned to that user. figure 4 shows the definition:

Second Section: In this section, the user of the EV will go to the TA and after checking the accuracy of W and the ID_E, he/she will install the OBU on his/her vehicle. If the user needs to charge, he/she sends a request to EP then the OBU will decrypt the relevant parameters and continue the process.

C. AUTHENTICATION PHASE

Before the EV reaches the energy segments and the charging operation begins, it must be authenticated to illuminate the relevant segment for charge transfer. To do this, EV will see the EPs categorized by quality parameters on the vehicle display and then select the number of required energy segments. These quality parameters can be based on stars. These stars are based on surveys of users who receive previous charges over an EP, which reflects user satisfaction.

After selecting the EP and the number of requested energy segment (N), the authentication protocol starts as shown in figure 5. The value of N is encrypted so the EP fails to make a change and only the TA can alter it. Sending parameters starts the charging session as follows:

Step 1 : After choosing the number of segments N and timestamp T_E, EV start producing $F = N \bigoplus H_U \bigoplus K_{TE}$ and $R = E_{K_{TE}}(s \| ID_E \parallel ID_P \parallel a \| T_E)$ then sends $\{F, R, H_T, Nonce\}$ parameters to EP via a public network.

Step 2 : After receiving the charge request and the parameters, EP chooses the price of each segment (P) and then produces parameter $A = h(K_{TP} \| ID_P \| H_T \parallel P)$. Then sends $/F, R, H_T, Nonce, /A, P$ parameters via the public channel to TA for authenticate.

Step 3 : When TA receives parameters, it performs the following steps for authenticating.

a. The TA decrypts the parameter R and obtains the values of $D_{K_{TE}}(R) = s \| ID_E \parallel ID_P \parallel a \| T_E$.

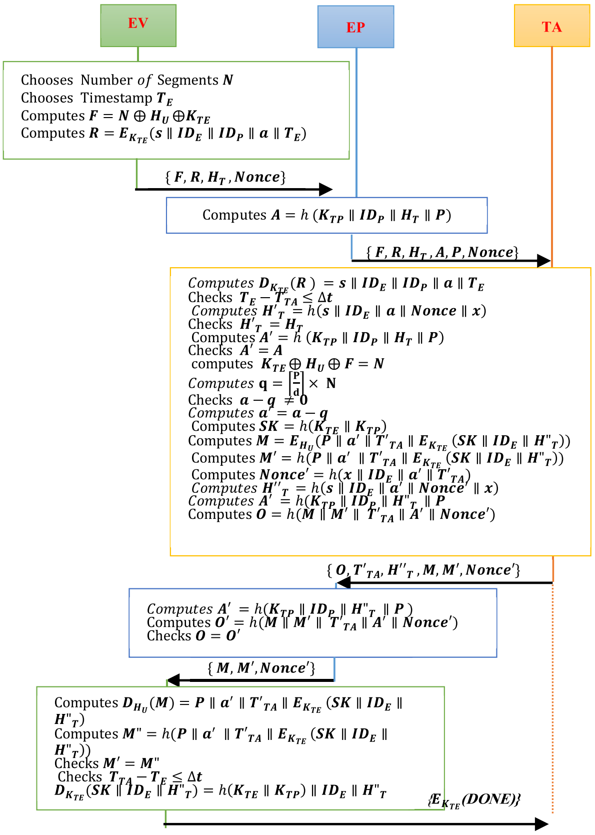

EV
EP
TA
Chooses Number of Segments N
Chooses Timestamp T_E
Computes $F = N \oplus H_U \oplus K_{TE}$
Computes $R = E_{K_{TE}}(s \parallel ID_E \parallel ID_P \parallel a \parallel T_E)$
$\{F, R, H_T, Nonce\}$
Computes $A = h\,(K_{TP} \parallel ID_P \parallel H_T \parallel P)$
$\{F, R, H_T, A, P, Nonce\}$
Computes $D_{K_{TE}}(R) = s \parallel ID_E \parallel ID_P \parallel a \parallel T_E$
Checks $T_E - T_{TA} \leq \Delta t$
Computes $H'_T = h(s \parallel ID_E \parallel a \parallel Nonce \parallel x)$
Checks $H'_T = H_T$
Computes $A' = h\,(K_{TP} \parallel ID_P \parallel H_T \parallel P)$
Checks $A' = A$
computes $K_{TE} \oplus H_U \oplus F = N$
Computes $\mathbf{q} = \lceil \frac{P}{d} \rceil \times N$
Checks $a - q \neq 0$
Computes $a' = a - q$
Computes $SK = h(K_{TE} \parallel K_{TP})$
Computes $M = E_{H_U}(P \parallel a' \parallel T'_{TA} \parallel E_{K_{TE}}(SK \parallel ID_E \parallel H"_T))$
Computes $M' = h(P \parallel a' \parallel T'_{TA} \parallel E_{K_{TE}}(SK \parallel ID_E \parallel H"_T))$
Computes $Nonce' = h(x \parallel ID_E \parallel a' \parallel T'_{TA})$
Computes $H''_T = h(s \parallel ID_E \parallel a' \parallel Nonce' \parallel x)$
Computes $A' = h(K_{TP} \parallel ID_P \parallel H"_T \parallel P$
Computes $O = h(M \parallel M' \parallel T'_{TA} \parallel A' \parallel Nonce')$
$\{O, T'_{TA}, H''_T, M, M', Nonce'\}$
Computes $A' = h(K_{TP} \parallel ID_P \parallel H"_T \parallel P)$
Computes $O' = h(M \parallel M' \parallel T'_{TA} \parallel A' \parallel Nonce')$
Checks $O = O'$
$\{M, M', Nonce'\}$
Computes $D_{H_U}(M) = P \parallel a' \parallel T'_{TA} \parallel E_{K_{TE}}(SK \parallel ID_E \parallel H"_T)$
Computes $M" = h(P \parallel a' \parallel T'_{TA} \parallel E_{K_{TE}}(SK \parallel ID_E \parallel H"_T))$
Checks $M' = M"$
Checks $T_{TA} - T_E \leq \Delta t$
$D_{K_{TE}}(SK \parallel ID_E \parallel H"_T) = h(K_{TE} \parallel K_{TP}) \parallel ID_E \parallel H"_T$
$\{E_{K_{TE}}(DONE)\}$

FIGURE 5. The proposed authentication phase.

b. To checks the freshness of the message, the TA checks the timestamp $T_E - T_{TA} \leq \Delta t$, if the timestamp passes through the specified value (Δt), the message is invalid.

c. The TA uses the decrypted parameters from R and computes $H'_T = h(s \| ID_E \parallel a \parallel Nonce \| x)$ then compares it with H_T received through public channel. If $H'_T = H_T$, then the EV is authorized and authenticated. Otherwise the message is tampered and the session will be closed.

d. If the EV is authorized, the TA uses the decrypted parameters from R and computes $A' = h(K_{TP} \parallel ID_P \parallel H_T \| P)$ then compares with A received via the public channel. If $A' = A$, the EP is authorized and there is no problem for charging.

Step 4 : After ensuring the accuracy of the transmitted data and the authentication of the entities, the TA calculates the charge price and checks the EV account balance. Continue as follows:

a. The TA gets the number of requested segment charges according to $K_{TE} \bigoplus H_U \bigoplus F = N$.

b. The TA calculates the total cost of the charge by the formula $q = \lceil \frac{P}{d} \rceil \times N$.

c. To check the account balance, the TA reduces the total cost from the account balance. If the answer to the equation $a - q \neq 0$ is not zero, the balance of the account is sufficient. If there is not enough, the message "Account balance is not enough" will appear.

d. The TA calculates new account balance $a' = a - q$.

Step 5 : After the processing of the EV account, the TA computes new parameters.

a. The TA computes $SK = h(K_{TE} \| K_{TP})$, $M = E_{H_U}(P \| a' \| T'_{TA} \| E_{K_{TE}}(SK \| ID_E))$, $M' = h(P \| a' \| T'_{TA} \| E_{K_{TE}}(SK \| ID_E))$, $Nonce' = h(x \| ID_E \| a' \| T'_{TA})$, $H''_T = h(s \| ID_E \| a' \| Nonce' \| x)$, $A' = h(K_{TP} \| ID_P \| H''_T \| P)$ and $O = h(M \| M' \| T'_{TA} \| A' \| Nonce')$.

b. Then the TA sends $\{M, M', H''_T, O, T'_{TA}, Nonce'\}$ via public channel to EP.

Step 6 : When the EP receives parameters, it computes $A' = h\left(K_{TP} \| ID_P \| H''_T \| P\right)$ then $O' = h(M \| M' \| T'_{TA} \| A' \| Nonce')$, if $O = O'$ authentication is performed and the parameters received are correct.

Step 7 : When the EV receives parameters, decrypt $D_{H_U}(M) = P \| a' \| T'_{TA} \| E_{K_{TE}}(SK \| ID_E)$ and then by using the obtained parameters, the value of $M'' = h(P \| a' \| T'_{TA} \| E_{K_{TE}}(SK \| ID_E))$ is computed. To check the authentication, the EV compares M' and M''. If $M' = M''$, authentication is done. Otherwise, the message is tampered or authentication is not done. In the following, EV checks freshness of message $T_{TA} - T_E \leq \Delta t$ and decrypts $D_{K_{TE}}(SK \| ID_E \| H''_T) = h(K_{TE} \| K_{TP}) \| ID_E \| H''_T$ then stores the values that require storage, such as H''_T for future charges. At the end of the message, it sends the message "ok" to the TA to complete the authentication session. Now it is ready to be charged.

Step 8 : In this step EV should calculate the number of chunks required for each energy segment according to formula a $= \left\lceil \frac{P}{d} \right\rceil$, EV then generates hash values proportional to each energy segment as below: $h_1 = h_1(chunk_1 \| \ldots \| chunk_r)$, $h_2 = h_2(chunk_{r+1} \| \ldots \| chunk_{2r})$, $h_3 = h_3(chunk_{2r+1} \| \ldots \| chunk_{3r})$ and $h_N = h_N(chunk_{Nr+1} \| \ldots \| chunk_{Nr})$. Each hash corresponds to the one energy segment and EV spends hashes. h_1 Indicates the costs of segment one, etc.

Step 9 : The TA computes $(h_1, h_2, h_3, \ldots, h_N)$ as step 8 and $h_{total} = (h'_1 \| h'_2 \| h'_3 \| \ldots \| h'_N \| SK)$ then sends encrypt parameters $E_{K_{TP}}\left(h'_1 \| h'_2 \| h'_3 \| \ldots \| h'_N \| SK\right)$, h_{total} to EP. The EP decrypts parameters and authenticates them by computing $h'_{total} = h'_1 \| h'_2 \| h'_3 \| \ldots \| h'_N \| SK$ then comparing with h_{total}, if $h'_{total} = h_{total}$, authentication is done.

D. CHARGING PHASE

At this phase, the EV sends the hash to the charging plate to turn on the first segment to receive the charge.

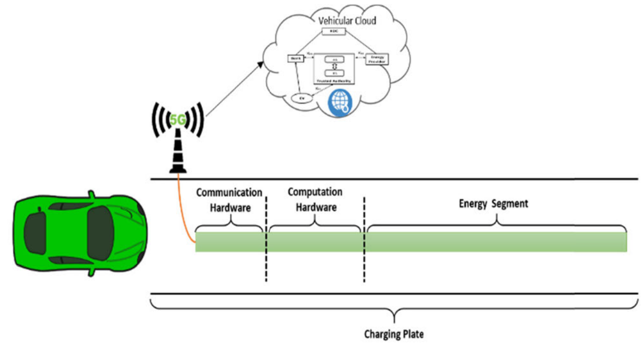


FIGURE 6. The proposed charging plate model. EV can charge its battery while moving after the authentication phase.

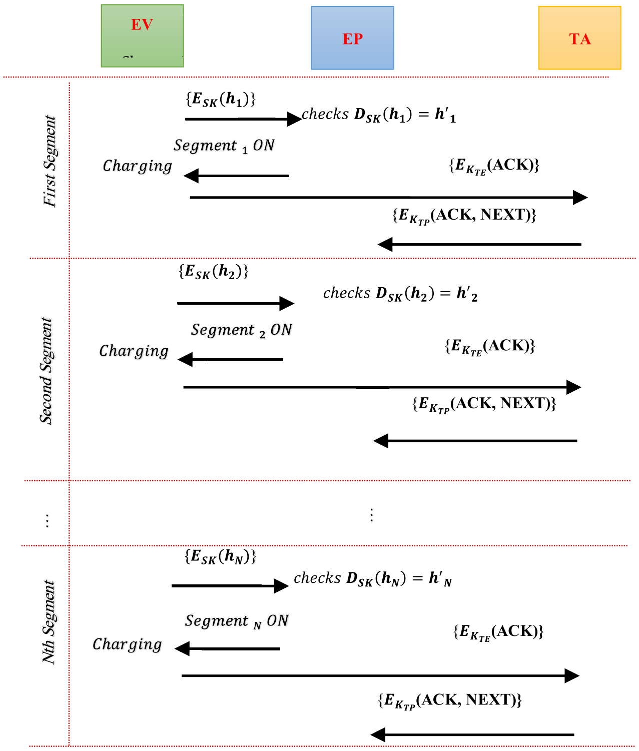

EV
EP
TA
First Segment
$\{E_{SK}(h_1)\}$
checks $D_{SK}(h_1) = h'_1$
Segment $_1$ ON
Charging
$\{E_{K_{TE}}(\text{ACK})\}$
$\{E_{K_{TP}}(\text{ACK, NEXT})\}$
Second Segment
$\{E_{SK}(h_2)\}$
checks $D_{SK}(h_2) = h'_2$
Segment $_2$ ON
Charging
$\{E_{K_{TE}}(\text{ACK})\}$
$\{E_{K_{TP}}(\text{ACK, NEXT})\}$
⋮
⋮
Nth Segment
$\{E_{SK}(h_N)\}$
checks $D_{SK}(h_N) = h'_N$
Segment $_N$ ON
Charging
$\{E_{K_{TE}}(\text{ACK})\}$
$\{E_{K_{TP}}(\text{ACK, NEXT})\}$

FIGURE 7. The proposed charging phase.

After decrypting the hash, the EP compares its value with the amount of hash received from the TA. If the values are equal, the segment switches on and the vehicle charging operation begins. Figure 6 shows how this action occurs using embedded hardware. As shown in figure 7, after receiving the first energy segment, the EV sends the successful charge message to the TA. The TA permits the EP the next charge by receiving this message and the charging process begins for the second segment. Hence, the process will continue to receive the requested charge until the end of last segment.

E. PAYMENT PHASE

When EV receives all N charge segments, it sends $\mathbf{E_{K_{TE}}}$(L) parameter as the last message to TA. After receiving this message, TA finishes the charging session and informs the parties involved. At the end of the charging session, TA in a message sends {the amount of money, the L (expressing EV for the bank) and ID$_{\mathrm{EP}}$} to the bank and sends the money transaction confirmation to both parties and confirms the transaction accuracy.

VI. SECURITY ANALYSIS

Checking the security of payment systems has been carried out in two terms. In formal proof, we simulate LSPP then validation tools have been used and in another, the LSPP resistance to a variety of possible attacks has been discussed.

Algorithm 1 TA Authentication Parameters

```
Input: $F, R, H_T, A, P, Nonce$
Output: $O, T'_{TA}, H''_T, M, M', Nonce'$
$D_{K_{TE}}(R) = s \parallel ID_E \parallel ID_P \parallel a \parallel T_E$;
$H'_T = h\,(s \parallel ID_E \parallel a \parallel Nonce \parallel x)$;
$A' = h\,(K_{TP} \parallel ID_P \parallel H_T \parallel P)$;
if $T_E - T_{TA} \leq \Delta t$ and $H'_T = H_T$ and $\mathbf{A}' = A$ then
    $K_{TE} \bigoplus H_U \bigoplus F = N$;
    $q = \lceil \frac{P}{d} \rceil \times N$
    if $a - q \neq 0$ then
        $SK = h\,(K_{TE} \parallel K_{TP})$;
        $M = E_{H_U}(P \parallel a' \parallel T'_{TA} \parallel E_{K_{TE}}\left(SK \parallel ID_E \parallel H''_T\right))$;
        $M' = h\left(P \parallel a' \parallel T'_{TA} \parallel E_{K_{TE}}\left(SK \parallel ID_E \parallel H''_T\right)\right)$;
        $Nonce' = h(x \parallel ID_E \parallel a' \parallel T'_{TA})$;
        $H''_T = h\left(s \parallel ID_E \parallel a' \parallel Nonce' \parallel x\right)$ [[space]];
        $A' = h(K_{TP} \parallel ID_P \parallel H''_T \parallel P$;
        $O = h(M \parallel M' \parallel T'_{TA} \parallel A' \parallel Nonce')$;
        return $O, T'_{TA}, H''_T, M, M', Nonce'$;
    end
end
```

A. SECURITY SIMULATION CORRECTNESS

Protocol security analysis is vital in the development of secure payment systems to ensure user confidence. Formal security analysis is the method used to validate systems. There are many tools to check and verify protocols. In this subsection, we have simulated security in the OFMC backend model and verified the validity by using widely accepted AVISPA tool [27]. The details are shown in Algorithm 1, 2 and 3. We have implemented LSPP with HLPSL language in which each entity has a role. For the LSPP, the roles have been written in details. Simulation details are presented in the "Appendix". Since the writing of the scripts starts at the beginning of the authentication process in the public channel, pre-register and register phases, which are on the basis of the secure channel have not been implemented. Likewise, KDC has not been implemented due to playing no role in the authentication phase. The EV, known in this language as the user, sends the parameters specified in the protocol to the EP via the SND channel. This results in an alteration in system state from zero to one, thereby running the system. The SND channel type is dy, which represents the public channel. The messages sent through this channel are visible and audible.

Algorithm 2 EP Authentication

```
Input: $O, T'_{TA}, H''_T, M, M', Nonce'$
Output: bool
$A' = h(K_{TP} \parallel ID_P \parallel H''_T \parallel P)$;
$O' = h(M \parallel M' \parallel T'_{TA} \parallel A' \parallel Nonce')$;
if $\boldsymbol{O = O'}$ then
    return 1;
else
    return 0;
end
```

Algorithm 3 EV Authentication

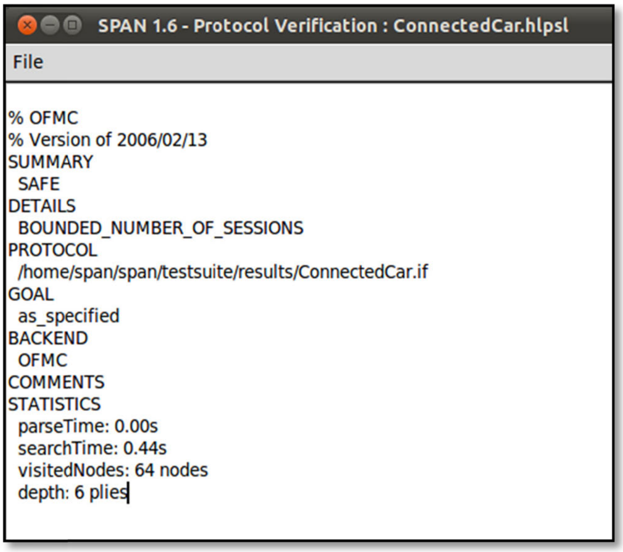
```
Input: $M, M'$
Output: bool
$D_{H_U}(M) = P \parallel a' \parallel T'_{TA} \parallel E_{K_{TE}}\left(SK \parallel ID_E \parallel H''_T\right)$;
$M'' = h(P \parallel a' \parallel T'_{TA} \parallel E_{K_{TE}}\left(SK \parallel ID_E \parallel H''_T\right))$;
if $T_{TA} - T_E \leq \Delta t$ then
    if $M' = M''$ then
        return 1;
    else
        return 0;
    end
else
    return 0;
end
```

After the implementation of entities roles, the session role, stating entities composition, has been implemented. Attacker behavior in this system has been defined as environment role. In the goal section, the objectives of security analysis have been written. In this role, there are three confidential objectives including SK, K_{TE}, and K_{TP} keys. In Appendix, titles sec1, sec2 and sec3 specify these goals. Two goals are also used to prove authentication.

As you can see in figure 8, the result of the simulation is SAFE by AVISPA and the OFMC model. OFMC model allows the implementation of the security attacks such as reply attack, man in the middle, sniffing, attacks on cryptography, attacks on hash function, confidentiality, mutual authentication and etc. AVSIPA tool verifies the validity of the whole system. The LSPP, as a result, would be safe from all requirements.

B. FURTHER SECURITY ANALYSIS

We check the resistance of the system to possible attacks like [29] and other articles [28].



```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/ConnectedCar.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.44s
  visitedNodes: 64 nodes
  depth: 6 plies
```

FIGURE 8. The result of the security analysis of the proposed system with the AVISPA tool.

1) REPLY ATTACK RESISTANCE

The scenario of the attack in this method is that the attacker sniffs the data sent on public channel and resends them again at another time in order to reuse the system and receive a free charge. Of course, in this scenario, the attacker can be the EV. Although it has received the charge, it will again get the charge. The proposed system avoids such attacks, so the EV must use the timestamp ($\mathbf{T_E}$). And the TA at the time of receiving the message calculates the $\mathbf{T_E} - \mathbf{T_{TA}} \leq \Delta\mathbf{t}$ value of the permitted time parameter. If it exceeds the limit, the message is invalid. Now, the question arises: what if an attacker can modify timestamp and actually blunder the TA and carry out the attack? To prevent such a scenario, the timestamp is encrypted when the EV is sent by the $\mathbf{K_{TE}}$ symmetric key, which practically no one can modify.

In another scenario, regardless of the charge it receives, the EV sends the same message with the right timestamp. In such an attack when the nonce produced by the TA is used, TA changes it and replaces the previous one. In practice, the nonce sent to TA is not consistent with nonce previously produced; as a result, this attack can be detected by the TA and eventually ruled out.

2) MIM ATTACK RESISTANCE

This attack occurs when a person is in the middle of communication between two entities. If the person can impersonate each entity, he/she can receive free charge. Because the communications are encrypted between entities and hash function is used for tamper detection, no one can tamper messages. Hence, the system is resistant to a man in the middle attack.

3) INSIDER ATTACK RESISTANCE

This attack occurs when the parameters are stored on the side of the EP; therefore, the insider attacker can gain access to those parameters and use them in the attacks. In the proposed system, no parameters are stored on the server side; accordingly, the attack is not possible.

4) IMPERSONATION ATTACK RESISTANCE

The attack was carried out if the attacker could impersonate himself by authenticated user parameters. In this system, the EV does not use its actual authentication identifier. Instead, it uses the parameter generated by the TA for authentication. These parameters are encrypted and stored on the OBU that is inaccessible. These parameters cannot be generated by anyone except the TA and they can be checked for its accuracy. Therefore, the impersonation attack is blocked and system remains secure.

5) MUTUAL AUTHENTICATION

This important feature must be implemented in security systems because the relationship is based on the principle of trust; therefore, in the absence of trust, authentication between entities is not transparent. In LSPP, trust has an identifier. Since the identity of EV and EP is ambiguous for each other, only the TA can confirm the identity of the two entities. As a result, after the authentication of two entities by the TA, the charge exchange takes place.

6) ANONYMITY

Anonymity is an important principle. In fact, the EP is not supposed to know who is charging in order not to change the quality of its services for each person. The quality of charge services should be the same for the president or an ordinary individual. Also, an affluent and celebrated individual should not be recognized in order to avoid paying more money. Consequently, we have established mutual authentication for the mutual trust of the entities by providing an anonymous system.

7) LOCATION PRIVACY

One of the security features of the EV wireless charging system is that no one can track down the EV by tracking the location of the vehicle for hostile operations such as stealing. This feature is especially important for money carriers. Therefore, in this system, the vehicle does not use its actual authentication ID, instead it uses the authentication identity from the TA ($\mathbf{H_T} = h(\mathbf{s} \| \mathbf{ID_E} \parallel \mathbf{a} \| \mathbf{Nonce} \parallel \mathbf{x})$). Neither EP nor the middle attacker, can track the vehicle. Accordingly, the user's anonymity is well preserved and privacy is protected as well.

8) FREE RIDERS

Free riders charge their vehicles without payment. Free riders could charge by getting closer to authenticated and billed vehicles. To avoid free riders, their battery level should be checked before and after an energy segment. Moreover, vehicles should not be on the same energy segment. All things considered, segment charges should be smaller than the length of the EVs.

TABLE 4. Security requirements comparison.

	Methods					
Required items	[4]	[5]	[6]	[8]	[9]	LSPP
Type	Plug-in EV	Plug-in EV	DWC	DWC	DWC	DWC
Reply Attack	✓	✓	✓	✓	✓	✓
Man in the middle	✓	✓	✓	✓	×	✓
Insider Attack	✓	✓	✓	✓	✓	✓
Impersonation Attack	✓	✓	✓	✓	×	✓
Mutual Authentication	✓	×	✓	✓	×	✓
Double Spending	✓	✓	✓	×	×	✓
Anonymity	✓	✓	✓	✓	✓	✓
Location Privacy	✓	✓	×	✓	✓	✓
Free riders	✓	✓	✓	✓	✓	✓
Fraudulence in charging	×	✓	✓	✓	✓	✓
Price flexibility	not specified	✓	✓	✓	✓	✓
Traceability	✓	×	✓	×	×	✓
Fast Authentication	✓	×	×	×	×	✓

Achieved ✓ Not Achieved ×

C. SECURITY AND FUNCTIONALITY ANALYSIS

Security and functionality comparison For the purpose of comparing the proposed protocol with other protocols, a number of security attacks and functionality requirements are shown in Table 4. As seen in Table 4, the protocol [9] is vulnerable to the MIM attack and the protocols in [5, 8, 9] cannot achieve traceability of stolen vehicles. We have also found the protocol in [6] suffer from the location privacy. Furthermore, the protocols in [5, 6, 8, 9] do not provide fast authentication. Hence, the proposed protocol is more suitable than the previous protocols.

VII. PERFORMANCE ANALYSIS

In order to evaluate the efficiency of the proposed method, we compare the computational cost, communication cost and storage cost of the recent methods with the LSPP.

A. COMPUTATIONAL COST

To compare, it is necessary to estimate the cost of implementing various operations and functions. The average implementation time for various functions in the authentication mechanism is based on the results obtained by researchers [28] in Table 6. Authors in [28] use Samsung galaxy s5 that has a 2.5 GHz ARM Krait processor and 2 GB RAM. Total computational cost of methods has been calculated based on their results. It takes little time to execute the concatenation and XOR operation in comparison with other operators. The LSPP method needs to perform ten hash operations, three symmetric encryptions and three symmetric decryptions. As a result, the proposed method provides the lowest computational cost and extra security features in comparison to the other methods.

In the security protocols, the authentication and key agreement for the evaluation of performance is reviewed. To calculate the computational cost, first the number of each operation in each method should be counted, then the number of each operation should be multiplied by the cost specified in the Table 6 and summed up together. The result of the computational cost has been shown in the Table 5 and figure 9.

TABLE 5. Comparative computational cost.

Methods	Type	Computational cost	Total cost (s)
[4]	Plug-in	$8T_h$	**0.000048**
[5]	Plug-in	$1T_{bp} + 1T_{pm}^{G_1}$	**0.046118**
[6]	DWC	$5T_h + 4T_{mtp}^{G_1} + 2T_s$	**0.134382**
[8]	DWC	$1T_{bp} + 2T_{mul}^{G_1} + 1T_s$	**0.032741**
[9]	DWC	$1T_{bp} + 2T_{mul}^{G_1}$	**0.032729**
LSPP	DWC	$10T_h + 6T_s$	**0.000132**

TABLE 6. Execution time of cryptography elements [28].

Operation	Description	Time (sec)
T_{bp}	The execution time of a bilinear pairing	0.032713
T_h	The execution time of a general hash function	0.000006
T_s	The execution time of a symmetric encryption /decryption	0.000012
$T_{pm}^{G_1}$	The execution time of a point multiplication in G1	0.013405
$T_{mtp}^{G_1}$	The execution time of a map-to-point in G1	0.033582
$T_{mul}^{G_1}$	The execution time of a multiplication in G2	0.000008

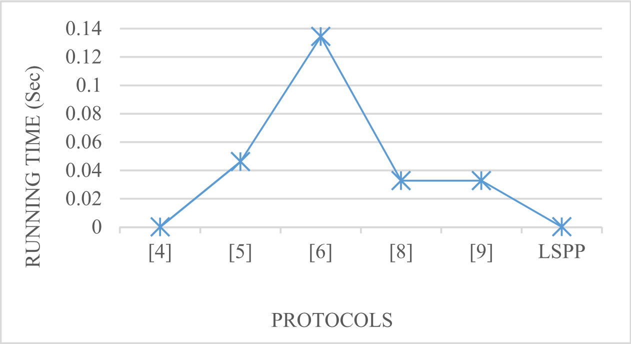


FIGURE 9. Comparative running time.

TABLE 7. Comparative communication cost.

Methods	Type	Number of bits	Number of messages	Storage cost (bits)
[6]	DWC	5984	12	960
[8]	DWC	6864	7	850
[9]	DWC	6224	4	1214
LSPP	DWC	6496	5	740

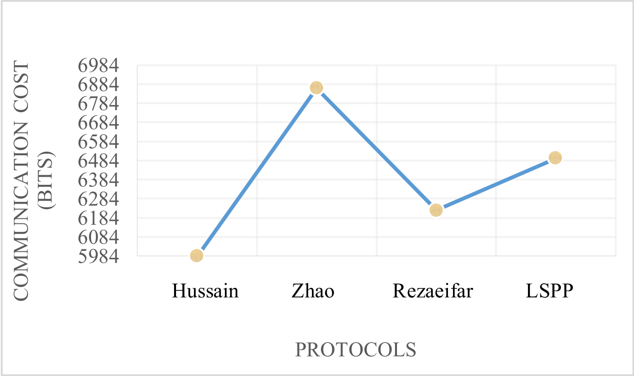


FIGURE 10. Comparative communication cost.

B. COMMUNICATION COST

Table 7 and figure 10 compares the communication cost of the proposed method with other previous methods. To calculate the cost of communication, we have assumed that the length of the random numbers is 160 bits, users' identity is 160 bits and the output (digest) of hash function (for SHA-1) is 160 bits. We consider the elliptic curve cryptosystem with 160-bit security strength, thus RSA cryptosystem are 1024-bits. For example, in the proposed method, the message $\{F, R, H_T, Nonce\}$ requires $(160+1024+160+160) = 1504$ bits. Only DWC payment methods have been reviewed in this subsection. The results have shown that despite a slight increase in communication costs, the proposed method is safer and has less computational costs compared to the other methods. Also, as shown in figure 12, the number of communication messages is normal.

C. STORAGE COST

After completing the registration phase in each method, we have measured the amount of space stored in the OBU. The result has been shown in Table 7 and figure 11. Since the OBU is a tamper proof unit, there is no problem in the amount of data stored.

VIII. EXPRIMENTAL STUDY

In this paper, to get OBU side execution time, we use LPC1788 [31] that has ARM Cortex-M3 and as shown in figure 13, our company board that has intel quad core 2.0GHz, 8GIG RAM, 256 SSD. For our tests, we have opted cryptographic library of ArduinioLibs [32].

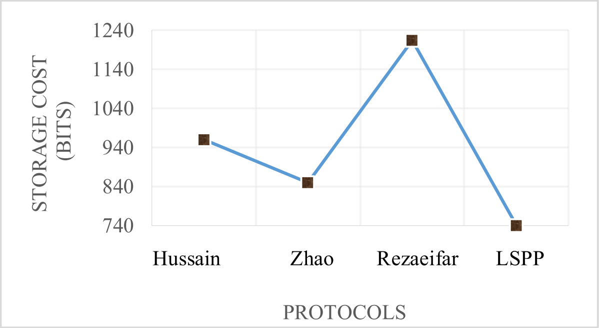


FIGURE 11. Comparative storage cost.

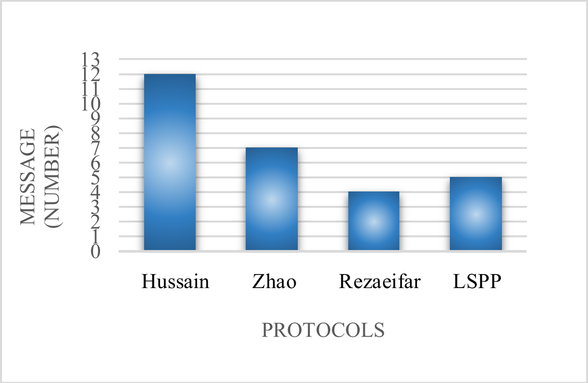


FIGURE 12. Comparative messages count.

TABLE 8. Execution time of different cryptographic operations.

Operations	LPC1788	Our Board
AES128-CBC (16 Bytes)	409 ns	141 ns
AES192-CBC (16 Bytes)	452 ns	166 ns
AES256-CBC (16 Bytes)	55 ns	192 ns
AES128-ECB (16 Bytes)	64.2 μ s	512 ns
AES192-ECB (16 Bytes)	76.8 μ s	607 ns
AES256-ECB (16 Bytes)	165 μ s	703 ns
SHA1 (16 Bytes)	8.7 μ s	230 ns
SHA256(16 Bytes)	13 μ s	255 ns
SHA512 (16 Bytes)	32.2 μ s	369 ns
SHA1(64 Bytes)	16.3 μ s	333 ns
SHA256(64 Bytes)	24 μ s	447 ns
SHA512 (64 Bytes)	43.1 μ s	500 ns

Table 8 shows the obtained execution time of different cryptographic elements on these board. In our scheme, each OBU needs to execute ten hash operations and six encryption operations. Considering the SHA512 for the hash operation,

FIGURE 13. Board from our company we have utilized for our tests.

for the encryption AES256, the total execution time of our scheme is just 4.842e-6 second.

IX. CONCLUSION

In this paper, first we have reviewed the different static and dynamic payment methods and their weaknesses for wireless charging. Then we have outlined the various components of the DWC for EV. With a knowledge of security requirements and cellular networks, we have proposed the LSPP. We have used low-cost operations including hash function, concatenation and symmetric encryption rather than costly operations such as bilinear pairing and multiplication. Alongside security and efficiency, the speed of the method in DWC is of vital importance. We have greatly reduced the time for authentication. We have provided anonymity and location privacy along with traceability which is obtained using the information in the TA. In addition, the security of the LSPP against a variety of attacks has been examined both in formal and informal ways. OFMC model has been used to simulate formal analysis and AVISPA has also been used to verify the validity of the LSPP. In informal analysis, we have considered possible attack scenarios to measure the resistance of LSPP. At the end of the paper, security and cost comparisons with past methods have been discussed. The achieved results have illustrated that the LSPP has a better performance and provides extra security features. It should be pointed out that the servers in this method should be implemented on cloud infrastructure. Since we do not have a point of failure, we need to spend a little more money.

APPENDIX

```
role trustAgent(
        User, EP, TA: agent,
        Kte: symmetric_key,
        H, HF: hash_func,
        SND, RCV: channel(dy)
)
played_by TA
def=
local
        State: nat,
        A, Ht, IDp, P, Nonce, Hpt, S, IDe, X, Ktp, N, Hu, F, Q, D,
Aa, Aap, SK, Ktu, M, Tpta, Mp, Noncep, Hzt, Ap, O, OK, Te, Tta, DT,
Htotal, Hp1n: text
```

```
const
        sec1, sec2, sec3, u_t_Te, t_u_Tpta: protocol_id
init
        State := 2
transition
        1. State = 2 /\ RCV(F', {S'.IDe'.A'.Te'}_Kte, A', Ht', IDp',
P', Nonce') /\ HF(Te'.Tta)=DT /\ Ht'=H(S'.IDe'.Aa.Nonce'.X) /\
A'=H(Ktp.IDp'.Ht'.P') =|>
          State' := 5
          /\ Tpta' := new()
          /\ N' := xor(Kte, xor(Hu,F'))
          /\ Q' := HF(P'.D.N')
          /\ Aap' := HF(Aa.Q')
          /\ SK' := H(Ktu.Ktp)
          /\ M' := {P'.Aap'.Tpta'.({SK'.IDe'}_Kte)}_Hu
          /\ Mp' := H(P'.Aap'.Tpta'.({SK'.IDe'}_Kte))
          /\ Noncep' := H(X.IDe'.Aap'.Tpta')
          /\ Hzt' := H(S'.IDe'.Aap'.Noncep'.X)
          /\ Ap' := H(Ktp.IDp.Hzt'.P')
          /\ O' := H(M'.Mp'.Tpta'.Ap'.Noncep')
          /\ SND(O', Tpta', Hzt',
{P'.Aap'.Tpta'.({SK'.IDe'}_Kte)}_Hu, Mp', P', Noncep')
          /\ secret(Kte, sec1, {User, TA})
          /\ secret(Ktp, sec2, {EP, TA})
          /\ secret(SK, sec3, {User, EP, TA})
          /\ witness(TA, User, t_u_Tpta, Tpta')
          /\ request(TA, User, u_t_Te, Te')
        2. State = 5 /\ RCV({OK'}_Kte) =|>
          Htotal' := (Hp1n.SK)
          /\ SND({Hp1n.SK}_Ktp, Htotal')
end role
```

```
role energyProvider(
        User, EP, TA: agent,
        Kte: symmetric_key,
        H: hash_func,
        SND, RCV: channel(dy)
)
played_by EP
def=
local
        State: nat,
        A, F, R, Ht, Nonce, Ktp, IDp, P, O, Tpta, Hzt, M, Mp,
Noncep, V, S, IDe, Te, Hp1n, SK, Htotal, Aap, Hu: text
const
        sec2, sec3: protocol_id
init
        State := 1
transition
        1. State = 1 /\ RCV(F', {S'.IDe'.A'.Te'}_Kte, Ht', Nonce')
=|>
          State' := 3
          /\ A' := H(Ktp.IDp.Ht'.P)
          /\ SND(F', {S'.IDe'.A'.Te'}_Kte, A', Ht', IDp, P, Nonce')
          /\ secret(Ktp, sec2, {EP, TA})
        2. State = 3 /\ RCV(O', Tpta', Hzt',
{P'.Aap'.Tpta'.({SK'.IDe'}_Kte)}_Hu, Mp', P', Noncep')
          /\
O'=H(({P'.Aap'.Tpta'.({SK'.IDe'}_Kte)}_Hu).Mp'.Tpta'.H(Ktp.IDp.Hzt
'.P').Noncep') =|>
          State' := 6
          /\ V' :=
H(({P'.Aap'.Tpta'.({SK'.IDe'}_Kte)}_Hu).Mp'.Hzt'.Noncep')
          /\ SND(Hzt', {P'.Aap'.Tpta'.({SK'.IDe'}_Kte)}_Hu, Mp',
Tpta', V', Noncep')
          /\ secret(SK, sec3, {User, EP, TA})
        3. State = 6 /\ RCV({Hp1n'.SK'}_Ktp, Htotal') /\ Htotal' =
(Hp1n'.SK') =|>
          State' := 8
end role
```

```
role session(
                User, EP, TA: agent,
                Kte: symmetric_key,
                H, HF: hash_func
)
def=
local
                SU, RU, SE, RE, ST, RT: channel(dy)
composition
                vehicle(User, EP, TA, Kte, H, SU, RU)
                /\ energyProvider(User, EP, TA, Kte, H, SE, RE)
                /\ trustAgent(User, EP, TA, Kte, H, HF, ST, RT)
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%
role environment()
def=
const
                user, eP, tA: agent,
                kte: symmetric_key,
                h, hf: hash_func,
                f, r, ht, nonce, a, iDp, p, o, tpta, hzt, m, mp, noncep, v,
htotal: text,
                sec1, sec2, sec3, u_t_Te, t_u_Tpta: protocol_id
intruder_knowledge = {user, eP, tA, h, hf, f, r, ht, nonce, a, iDp, p, o,
tpta, hzt, m, mp, noncep, v, htotal}
composition
                session(user, eP, tA, kte, h, hf)
                /\ session(i, eP, tA, kte, h, hf)
                /\ session(user, i, tA, kte, h, hf)
                /\ session(user, eP, i, kte, h, hf)
end role
```

```
role vehicle(
                User, EP, TA: agent,
                Kte: symmetric_key,
                H: hash_func,
                SND, RCV: channel(dy)
)
played_by User
def=
local
                State: nat,
                N, Te, F, Hu, R, S, IDe, A, Ht, Nonce, Hzt, M, Mp, Tpta, V,
Noncep, OK, P, Aap, SK: text
const
                sec1, sec3, u_t_Te, t_u_Tpta: protocol_id
init
                State := 0
transition
                1. State = 0 /\ RCV(start) =|>
                   State' := 4
                   /\ N' := new()
                   /\ Te' := new()
                   /\ F' := xor(N', xor(Hu, Kte))
                   /\ R' := {S.IDe.A.Te'}_Kte
                   /\ SND(F', {S.IDe.A.Te'}_Kte, Ht, Nonce)
                   /\ secret(Kte, sec1, {User, TA})
                   /\ witness(User, TA, u_t_Te, Te')
                2. State = 4 /\ RCV(Hzt',
                {P'.Aap'.Tpta'.({SK'.IDe'}_Kte)}_Hu, Mp', Tpta', V',
                Noncep') /\
                H({{P'.Aap'.Tpta'.({SK'.IDe'}_Kte)}_Hu}_Hu)=Mp'
                   /\
H(({P'.Aap'.Tpta'.({SK'.IDe'}_Kte)}_Hu).Mp'.Hzt'.Noncep')=V' =|>
                   State' := 7
                   /\ SND({OK}_Kte)
                   /\ secret(SK, sec3, {User, EP, TA})
                   /\ request(User, TA, t_u_Tpta, Tpta')
end role
```

REFERENCES

[1] J. Huang, Y. Zhou, Z. Ning, and H. Gharavi, "Wireless power transfer and energy harvesting: Current status and future prospects," *IEEE Wireless Commun.*, vol. 26, no. 4, pp. 163–169, Aug. 2019.

[2] A. A. Mohamed, A. Meintz, and L. Zhu, "System design and optimization of in-route wireless charging infrastructure for shared automated electric vehicles," *IEEE Access*, vol. 7, pp. 79968–79979, Jun. 2019.

[3] T. R. Hawkins, B. Singh, G. Majeau-Bettez, and A. H. Strømman, "Comparative environmental life cycle assessment of conventional and electric vehicles," *J. Ind. Ecol.*, vol. 17, no. 1, pp. 53–64, Feb. 2013.

[4] H. Nicanfar, S. Hosseininezhad, P. TalebiFard, and V. C. 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.

[5] M. H. Au, J. K. Liu, J. Fang, Z. L. Jiang, W. Susilo, and J. Zhou, "A new payment system for enhancing location privacy of electric vehicles," *IEEE Trans. Veh. Technol.*, vol. 63, no. 1, pp. 3–18, Jan. 2014.

[6] R. Hussain, J. Son, D. Kim, M. Nogueira, H. Oh, A. O. Tokuta, and J. Seo, "PBF: A new privacy-aware billing framework for online electric vehicles with bidirectional auditability," *Wireless Commun. Mobile Comput.*, vol. 2017, Oct. 2017, Art. no. 5676030.

[7] R. Hussain, D. Kim, M. Nogueira, J. Son, A. Tokuta, and H. Oh, "A new privacy-aware mutual authentication mechanism for charging-on-the-move in online electric vehicles," in *Proc. 11th Int. Conf. Mobile Ad-Hoc Sensor Netw. (MSN)*, Dec. 2015, pp. 108–115.

[8] T. Zhao, L. Wei, and C. Zhang, "A secure and privacy-preserving billing scheme for online electric vehicles," in *Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring)*, May 2016, pp. 1–5.

[9] Z. Rezaeifar, R. Hussain, S. Kim, and H. Oh, "A new privacy aware payment scheme for wireless charging of electric vehicles," *Wireless Pers. Commun.*, vol. 92, no. 3, pp. 1011–1028, 2017.

[10] M. Andrei, B. Claudiu, and I. Vadan, "Wireless power transmission—State of the art and applications," in *Proc. 8th Int. Conf. Mod. Power Syst. (MPS)*, May 2019, pp. 1–6.

[11] Y. J. Jang, "Survey of the operation and system study on wireless charging electric vehicle systems," *Transp. Res. C, Emerg. Technol.*, vol. 95, pp. 844–866, Oct. 2018.

[12] N. P. Suh and D. H. Cho, *The On-Line Electric Vehicle: Wireless Electric Ground Transportation Systems*. Asia: Springer, 2017.

[13] D. W. K. Ng, T. Q. Duong, C. Zhong, and R. Schober, "Wireless power transfer," in *Wireless Information and Power Transfer: Theory and Practice*. Hoboken, NJ, USA: Wiley, 2019, pp. 273–295.

[14] Y. Li, R. Mai, L. Lu, T. Lin, Y. Liu, and Z. He, "Analysis and transmitter currents decomposition based control for multiple overlapped transmitters based WPT systems considering cross couplings," *IEEE Trans. Power Electron.*, vol. 33, no. 2, pp. 1829–1842, 2018.

[15] W. Zhou, Y.-G. Su, L. Huang, X.-D. Qing, and A. P. Hu, "Wireless power transfer across a metal barrier by combined capacitive and inductive coupling," *IEEE Trans. Ind. Electron.*, vol. 66, no. 5, pp. 4031–4041, Jul. 2018.

[16] A. Gupta and E. R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," *IEEE Access*, vol. 3, pp. 1206–1232, Jul. 2015.

[17] V. Cisco. (2018). *The Zettabyte Era: Trends and Analysis*. Accessed: Mar. 8, 2018. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11741490.html

[18] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[19] T. Guarda, M. F. Augusto, I. Lopes, J. A. Victor, Á. Rocha, and L. Molina, "Mobile communication systems: Evolution and security," in *Developments and Advances in Defense and Security*. Singapore: Springer, 2020, pp. 87–94.

[20] M. N. Irshad, L. Du, I. A. Khoso, T. B. Javed, and M. M. Aslam, "A hybrid solution of SDN architecture for 5G mobile communication to improve data rate transmission," in *Proc. 28th Wireless Opt. Commun. Conf. (WOCC)*, May 2019, pp. 1–5.

[21] A. Mukherjee, "Energy efficiency and delay in 5G ultra-reliable low-latency communications system architectures," *IEEE Netw.*, vol. 32, no. 2, pp. 55–61, Mar./Apr. 2018.

[22] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2017.

[23] J. Mendes, X. Jiao, A. Garcia-Saavedra, F. Huici, and I. Moerman, "Cellular access multi-tenancy through small-cell virtualization and common RF front-end sharing," *Comput. Commun.*, vol. 133, pp. 59–66, Jan. 2019.

[24] J. Moysen and L. Giupponi, "From 4G to 5G: Self-organized network management meets machine learning," *Comput. Commun.*, vol. 129, pp. 248–268, Sep. 2018.

[25] A. Gupta, R. K. Jha, P. Gandotra, and S. Jain, "Bandwidth spoofing and intrusion detection system for multistage 5G wireless communication network," *IEEE Trans. Veh. Technol.*, vol. 67, no. 1, pp. 618–632, Jan. 2018.

[26] M. R. Sutradhar, N. Sultana, H. Dey, and H. Arif, "A new version of kerberos authentication protocol using ECC and threshold cryptography for cloud security," in *Proc. Joint 7th Int. Conf. Inform., Electron. Vis. (ICIEV) 2nd Int. Conf. Imag., Vis. Pattern Recognit. (icIVPR)*, Jun. 2018, pp. 239–244.

[27] T. Genet. (2017). *SPAN+AVISPA for Verifying Cryptographic Protocols*. Accessed: Jun. 24, 2019. [Online]. Available: http://people.irisa.fr/Thomas.Genet/span/present_span.pdf

[28] D. Abbasinezhad-Mood and M. Nikooghadam, "An anonymous ECC-based self-certified key distribution scheme for the smart grid," *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 7996–8004, Oct. 2018.

[29] D. Abbasinezhad-Mood, A. Ostad-Sharif, M. Nikooghadam, and S. M. Mazinani, "A secure and efficient key establishment scheme for communications of smart meters and service providers in smart grid," *IEEE Trans. Ind. Informat.*, to be published.

[30] A. Ashok, P. Steenkiste, and F. Bai, "Vehicular cloud computing through dynamic computation offloading," *Comput. Commun.*, vol. 120, pp. 125–317, May 2018.

[31] *LPC1788*. Accessed: Jun. 19, 2018. [Online]. Available: https://www.nxp.com/docs/en/data-sheet/LPC178X_7X.pdf

[32] *ArduinoLibs: Cryptographic Library*. Accessed: Apr. 11, 2018. [Online]. Available: http://rweather.github.io/Q7597arduinolibs/crypto.html

MOJTABA TAJMOHAMMADI received the B.Sc. degree in computer engineering-software and the M.Sc. degree in information security from Imam Reza International University, Mashhad, Iran, in 2016 and 2018, respectively. His research interests include network security, cryptography, data security, and securtiy protocols.

SAYYED MAJID MAZINANI was born in Mashhad, Iran, in January 1971. He received the bachelor's degree in electronics from Ferdowsi University, Mashhad, in 1994, the master's degree in remote sensing and image processing from Tarbiat Modarres University, Tehran, Iran, in 1997, and the Ph.D. degree in wireless sensor networks from Ferdowsi University, in 2009. He was with IRIB, from 1999 to 2004. He is currently an Assistant Professor at the faculty of Engineering, Imam Reza International University. He was the Head of the Department of Electrical and Computer Engineering, from 2009 to 2012. His research interests include computer networks, wireless sensor networks, and smart grids.

MORTEZA NIKOOGHADAM received the B.Sc. degree from the University of Sajjad, Iran, in 2006, and the M.Sc. and Ph.D. degrees from Shahid Beheshti University, Iran, in 2008 and 2012, respectively. He is currently an Assistant Professor with the Department of Computer Engineering and Information Technology, Imam Reza International University, Mashhad, Iran. His research interests include data security, cryptography, and sensor network security. His current research interest is reconfigurable architectures for multipliers under Galois field.

ZAHRAA AL-HAMDAWEE received the B.Sc. degree in electrical engineering from the University of Baghdad. She is currently pursuing the master's degree with the Imam Reza International University, Mashhad, Iran, where she is also a Researcher. Her research interests include cloud computing, workflow scheduling, meta-heuristic and heuristic algorithms, particle swarm optimization, and genetic algorithm.