Lightweight Mutual Authentication Protocol for V2G Using Physical Unclonable Function

Gaurang Bansal[1], Naren[1], Vinay Chamola[1], Biplab Sikdar[2] and Neeraj Kumar[3]
[1] Department of Electrical and Electronics Engineering, BITS-Pilani, Pilani Campus, India,
[2] Department of Electrical and Computer Engineering, National University of Singapore, Singapore,
[3] Department of Computer Science, Thapar University, Patiala, India.

***Abstract*—EVs have been slowly replacing conventional fuel based vehicles since the last decade. EVs are not only environment- friendly, but when used in conjunction with a smart grid, opens up new possibilities and a Vehicle-Smart Grid ecosystem, commonly called V2G can be achieved. This would not only encourage people to switch to environment-friendly EVs or Plug-in Hybrid Electric Vehicles (PHEVs), but it could positively aid in load management on the power grid, and present new economic benefits to all the entities involved in such an ecosystem. Nonetheless, privacy and security concerns remain the serious concerns of smart grids. The devices used in V2G are tiny, inexpensive, and resource constrained, which renders them susceptible to multiple attacks. Any protocol designed for V2G systems must be secure, lightweight, and must protect the privacy of the vehicle owner. Since EVs and charging stations are usually unguarded, physical security is also a must. To tackle these issues, we propose Physical Unclonable Functions (PUF) based Secure User Key-Exchange Authentication (SUKA) protocol for V2G systems. The proposed protocol uses PUFs to achieve a two-step MA between an EV and the Grid Server. It is lightweight, secure, and privacy preserving. SUKA has identity protection, privacy protection, message integrity, and location security. Simulations show that SUKA performs better and provides more security features than state-of-the-art V2G protocols. Using a formal security model and analysis, we have shown that our protocol is secure.**

***Index Terms*—V2G, PUF, security, smart grid, authentication, networks, privacy**

I. INTRODUCTION

The batteries within EVs enable the functionality of V2G networks. The purpose of V2G is to manage the energy trading amidst battery-powered electric vehicles and the power grid to use the grid's energy more efficiently [1]. The electrical energy stored in the EV batteries can serve as a source for the power grid and other energy deficient EVs. When the load on the grid is high, the energy stored in the batteries of EVs could be used to pump power into the grid, and when the load on the grid is low, the excess power in the grid could be used to charge the EV batteries and avoid wastage [2]. V2G networks could also be used for power regulation [3] or for storing power generated by renewable sources such as wind power [4]. Thus, in todays time and age, V2G for smart grids presents great practical applications.

The worldwide demand for electrical power is predicted to climb 82% by the year 2030. Power grids are aiming to reduce the number of additional generators required. They employ demand-response techniques [5] to reduce consumption and increase efficiency. Although such techniques offer many benefits, security and privacy issues remain the significant downsides [6]. A lot of information is communicated during energy exchange between a vehicle and a service provider. However, an adversary could compromise this flow of information, either by tampering with it or capturing it entirely. This could lead to unfair or imbalanced energy transactions between the two parties. Moreover, the victims information which was captured could be used in criminal activities and targeted advertisements. The devices used in V2G are inexpensive, small, and simple [7]. The EVs are usually parked in locations which are easy to access, which means an adversary could easily capture the V2G devices on these vehicles. Therefore, making V2G physically secure becomes compulsory. For instance, an adversary could access security keys stored in the device memory and initiate various attacks. PUFs have emerged as a promising solution for protection against physical attacks. PUFs eliminate the need to store secret keys in the memory of the devices and rely on the exchange of challenge-response pairs. The challenge-response mechanism of PUFs exploits the inherent fabrication or manufacturing process variabilities involved in making integrated circuits (ICs) [8]. The response or output of a PUF depends on both the input as well as the physical microstructure [9] of the device. The physical randomness induced through fabrication process variations makes each PUF device unique, i.e., two identical copies can never be made.

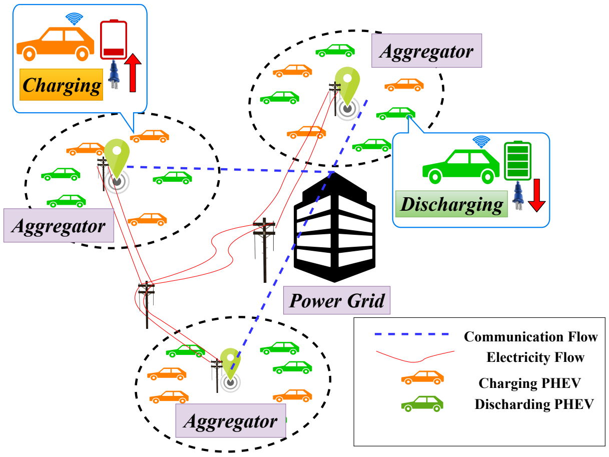

Fig. 1: System model

In V2G systems, an aggregator is a charging station which acts as a mediator between the EVs and the power grid. There has to be authentication between the EVs and the aggregator, between aggregator and the grid and between EVs and the grid as well. SUKA achieves the authentications mentioned above using a two-stage process. Using Pseudonym IDs (PID), the identity of the vehicle is masked to protect the vehicle owner's identity and location. Two different session keys are established in SUKA, one between aggregator and grid, and one between EV and the aggregator. These session keys are a function of the PUFs installed on the aggregator and the EV respectively. This ensures the secrecy of communication and eliminates the need to store any secret keys in memory. The proposed protocol uses simple cryptographic operations, which makes it lightweight and energy efficient. The number of message exchanges is also limited, which results in less communication overhead.

The rest of the paper is organized as follows. Section II discusses the related works in V2G systems. In Section III, we have given a quick introduction to PUFs. The network model, security goals, and assumptions for the V2G system and the notations used in our paper are discussed in Section IV. In Section V, we present our MA protocol (SUKA) based on PUFs. In Section VI, we subject our protocol to formal security analysis. We analyse the performance analysis of our protocol and compare it with state-of-the protocols in Section VII and finally deduce conclusions to the paper in Section VIII.

II. Related Works

Kempton and Tomic [10] first conceived the idea of V2G in the year 2004. Before the protocols for V2G networks could be made, the structure of a V2G network had to be well defined, and the impact of V2G on the power grid had to be analyzed. This work was carried out by the authors in [11, 12, 13, 14, 15] . Saxena et al. have presented specific security, privacy requirements, and challenges for V2G networks [16]. Privacy, secure communication, and efficiency are the most important aspects of a V2G protocol. Many such works were carried out for privacy preserving in V2G since 2011 by authors in [17, 18, 19, 20]. Yang et al. have presented a protocol P^2 in [17] which achieves privacy for individual electric vehicles (EVs) and the rewarding scheme which is crucial for proper implementation of V2G. Liu et al. present their scheme $AP3A$ [18] which is capable of identifying whether a EV is in the home or visiting network. $AP3A$ communicates the aggregated power status of the vehicles connected to an aggregator instead of revealing individual power status, thus achieving privacy for each individual EV. Liu et al. have presented a scheme [20] which identifies the different roles played by an individual EV i.e., customer, storage or generator. In each role, their scheme $ROPS$ addresses different privacy concerns. Tsai and Lo achieve mutual authentication and identity protection with the use of one private key which is given by a third-party anchor. This enables the smart-meters to quickly authenticate with the service provider. Abdallah and Shen propose a computationally less intensive privacy-preserving scheme in [22]. They identify that the authentication of the EV in the V2G system is specifically problematic. Therefore, the power grid takes the responsibility of ensuring the confidentiality and integrity of the communication. By reducing the number of exchanged messages, they achieve less overhead. Odelu et al. present a secure authenticated key agreement scheme [23] under the Canett-Krawczyk adversary (CK-adversary) model for smart grids. Shen et al. propose a privacy-preserving key agreement protocol for V2G networks in [24]. Their protocol ensures security by the use of a session key and ensures privacy using a self-synchronization mechanism. Some of the important V2G authentication schemes were proposed in [25, 26, 27]. Saxena and Choi have presented an authentication scheme for wide V2G networks where vehicles move from their home network to other networks as visitors in [28]. They propose a mutual authentication scheme which protects against impersonation, key-based and data-based attacks. Tao et al. have presented capacity-aware protocol $AccessAuth$ in [29] which takes into consideration the capacity limitations of each V2G network domain, of the EVs, and the mobility of the EVs for admission control. Based on prior information of trust between V2G network domains, they present a high-level authentication model and procedure to ensure that only authorized entities conduct the sessions. Gope and Sikdar have used one-way noncollision hash functions to propose a lightweight mutual authentication protocol [30]. Fouda et al. have proposed a lightweight message authentication scheme in [31]. In their scheme, smart meters at different levels in the smart-grid achieve mutual authentication among themselves, and a shared session key is established. They achieve lightweight message authentication using this shared session key along with a hash-based authentication code mechanism. Although this scheme was presented for smart grid communications, it can very well be extended to V2G networks. While many privacy-preserving, mutual authentication, lightweight and key establishment protocols exist for V2G systems, all of which claim to provide several security and privacy features, it cannot be said that any of them provide all the required security and privacy features along with protection against all types of attacks, especially protection against physical attacks. If a protocol does provide perfect security, then it either requires resource-heavy hardware or is very slow.

III. Preliminary Background

A PUF is based on a unique physical property of a device. It is similar to and as unique as the biometrics of a human being. The unique attribute of a PUF is that it relies on a physical basis, making it impossible to reproduce a PUF using cryptographic primitives. Additionally, the term "physical unclonable" indicates that it is computationally infeasible or tough to produce a physically same PUF [32]. By using PUFs in an interconnected system such as IOT or V2G systems, every single device can have its own unique "fingerprint" which cannot be cloned or reproduced. A PUF behaves like a mathematical function whose input (challenge) and output(response) are both in the form of a string of bits. A PUF function can be represented as:

$$Response = PUF(Challenge) \tag{1}$$

$$K = PUF(C) \tag{2}$$

where the challenge C is given as input and response, K is corresponding output to that challenge.

All PUFs behave in the following manner with respect to their input C and output R.

1) If an input C is given to the same PUF many times, it produces the same response R with a very high likelihood.
2) If the same input C is given to different PUFs, the responses obtained from each PUF differ greatly from each other with a very high likelihood.

IV. System Model

A. Network Model

Figure 1 depicts the system model. This model consists of three entities: Electric Vehicles (EVs), Aggregators (or Mediator), and Grid. An aggregator is a charging/discharging station where many vehicles can come to charge/discharge their batteries. It acts as a mediator between the EVs and the grid. EVs and aggregators have limited resources, while the grid has significantly larger resources. Aggregators and EVs have similar capabilities, but aggregators have slightly larger memory and computation power. As can be seen in Figure 1, multiple vehicles are connected to an aggregator, and multiple aggregators connect to the power grid. The device on every vehicle and aggregator is equipped with a PUF. Since a vehicle does not communicate directly with the grid, to achieve mutual authentication (MA) between these two non-communicating parties, all the intermediary nodes must be authenticated. Thus, MA between grid and vehicle can be divided as MA between aggregator and grid along with MA between vehicle and aggregator. We assume here that there is no shared key between a vehicle and its corresponding aggregator or between an aggregator and the grid. Whenever a new vehicle wants to register on the network, it's (C, R) pair is stored in the grid server once. The grid is the only trusted authority, and therefore, (C, R) pairs for all vehicles are stored only in the grid. Nothing else is assumed in further communication.

The server on the power grid starts with a single (C, R) pair for each EV. The grid server acquires this initial (C, R) pair at the time of initialization. To deploy a new vehicle on the roads, initialization involves the initial (C, R) pair to be sent to the power grid server using a secure channel. After this exchange, the vehicle can function on its own without needing any technical personnel or secure channel. The grid server stores the actual identity ID_V, and the (C_i, R_i) pair for each vehicle, while the vehicle itself does not store anything. Later this ID_V is replaced with pseudo-identities in further exchanges.

We assume that an adversary can get hold of any communication that is happening between the EV and the aggregator or the aggregator and grid. An adversary has the power to change, manipulate, and hide the data. It can inject new packets, store the old messages, initiate a session, or pretend to be a valid device. The objective of an attacker or adversary is to gain access to the grid without being noticed. If an unauthorized or potentially dangerous entity manages to authenticate with the grid server, it may disrupt energy transactions and cause economic damage. Therefore, this paper proposes an MA protocol that is resistant to various attacks such as replay attacks, man-in-the-middle attack, impersonation attacks, etc.

B. Security Goals

1) **Confidentiality:** The energy transaction data must not be visible to any unauthorized entity. For this, communication must be secret throughout, i.e., end-to-end. If an unauthorized entity from either within the system such as vehicles authenticated with other aggregators or the currently connected aggregator gains accesses to the messages which contain energy transaction details, it must be impossible to make sense of it.
2) **Message Integrity:** It must be possible for the smart grid server to verify if the message it receives from the aggregator has been tampered with or compromised. Because EVs and the grid server do not communicate directly, the aggregator must also be able to do the same for the messages received from the EVs.
3) **Identity privacy:** It must be impossible for an unauthorized entity to get hold of any personal information of the vehicle owner of an EV. Even if an unauthorized entity eavesdrops on the data exchanged within the V2G system, it must not be able to figure out that the data is from a particular vehicle or that two transactions are from the same vehicle.
4) **Authentication:** Before any energy transaction can be made, the aggregator must be authenticated with the grid server. The aggregator must also be authenticated with the vehicle, thus preventing any false energy exchanges.

C. Assumptions

The assumptions made in this paper are as follows:

- PUF is a small hardware component that is present with each participating device and is unique.
- The communication between a device and its PUF is secure and tamper-proof.
- The grid is considered as a trusted authority and has sufficient resources. On the other hand, vehicles and aggregators have limited resources in terms of memory and computation power.

D. Notations

Table I lists the notations used in this paper and their descriptions.

V. Proposed Mutual Authentication Protocol

This section presents the proposed mutual authentication protocol between the vehicle and the grid. Mutual authentication between the vehicle and the grid can be divided as mutual authentication between:

- Aggregator and grid.
- Vehicle and aggregator.

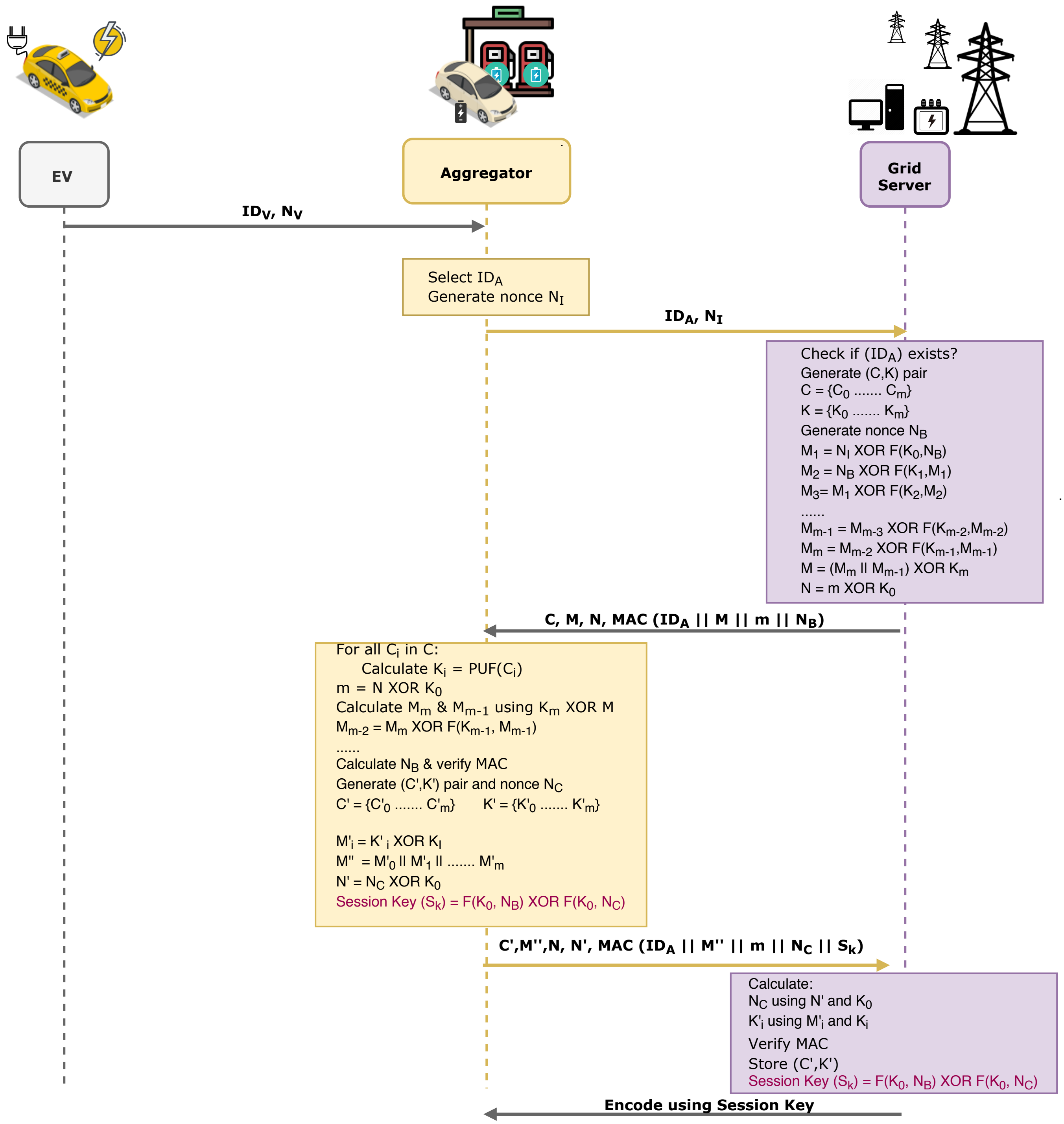
EV
Aggregator
Grid Server
ID_V, N_V
Select ID_A
Generate nonce N_I
ID_A, N_I
Check if (ID_A) exists?
Generate (C,K) pair
C = {C_0 .... C_m}
K = {K_0 .... K_m}
Generate nonce N_B
M_1 = N_I XOR F(K_0,N_B)
M_2 = N_B XOR F(K_1,M_1)
M_3= M_1 XOR F(K_2,M_2)
......
M_{m-1} = M_{m-3} XOR F(K_{m-2},M_{m-2})
M_m = M_{m-2} XOR F(K_{m-1},M_{m-1})
M = (M_m II M_{m-1}) XOR K_m
N = m XOR K_0
C, M, N, MAC (ID_A || M || m || N_B)
For all C_i in C:
Calculate K_i = PUF(C_i)
m = N XOR K_0
Calculate M_m & M_{m-1} using K_m XOR M
M_{m-2} = M_m XOR F(K_{m-1}, M_{m-1})
......
Calculate N_B & verify MAC
Generate (C',K') pair and nonce N_C
C' = {C'_0 .... C'_m}
K' = {K'_0 .... K'_m}
M'_i = K'_i XOR K_i
M'' = M'_0 II M'_1 II .... M'_m
N' = N_C XOR K_0
Session Key (S_k) = F(K_0, N_B) XOR F(K_0, N_C)
C',M'',N, N', MAC (ID_A || M'' || m || N_C || S_k)
Calculate:
N_C using N' and K_0
K'_i using M'_i and K_i
Verify MAC
Store (C',K')
Session Key (S_k) = F(K_0, N_B) XOR F(K_0, N_C)
Encode using Session Key

Fig. 2: Mutual authentication between aggregator and power grid server.

A. Mutual Authentication Between Aggregator and Grid Server

1) When a vehicle wants to make a transaction, the aggregator must authenticate the vehicle. The vehicle sends its ID (ID_V) along with a randomly generated nonce (N_V) to the aggregator with $Msg_{V2A} = \{ID_V, N_V\}$.
2) The aggregator generates another random number (nonce) (N_I) and sends it along with its ID (ID_A) to the grid server with $Msg_{M2G} = \{ID_M, N_I\}$.
3) The first stage of our protocol begins with the aggregator authenticating with the power grid server. This is shown in Figure2. The grid server receives a message ($Msg_{M2G} = \{ID_M, N_I\}$) from the aggregator. It checks if ID_M exists in its memory and whether N_I is fresh. If either of the conditions fails, the authentication request initiated by aggregator is terminated. Using ID_M, it finds the corresponding challenge-response pair (C, K) in its memory:

$$C = (C_0, C_1, C_2......C_m)$$
$$K = (K_0, K_1, K_2......K_m)$$

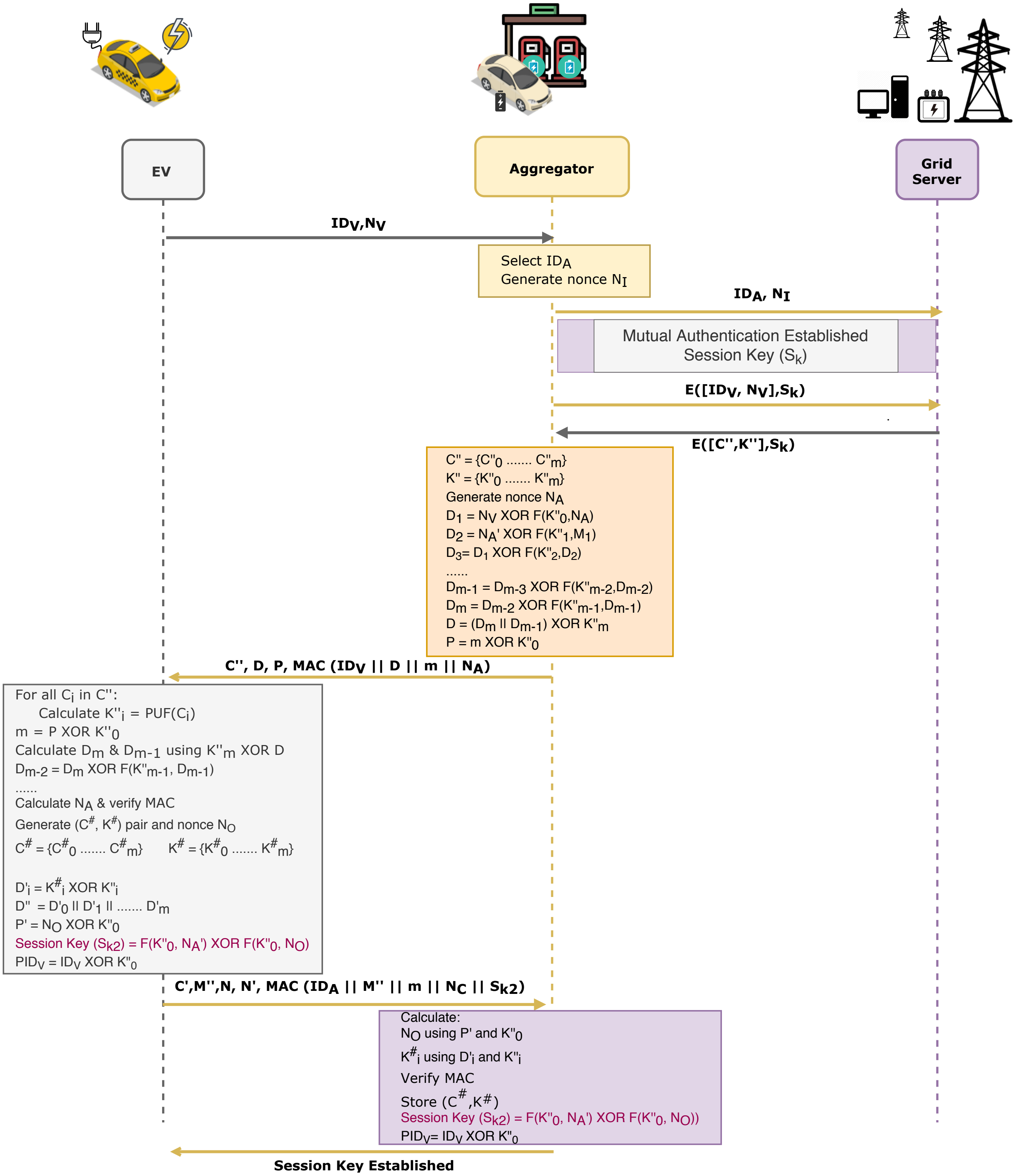
EV
Aggregator
Grid Server
ID_V, N_V
Select ID_A
Generate nonce N_I
ID_A, N_I
Mutual Authentication Established
Session Key (S_k)
$E([ID_V, N_V], S_k)$
$E([C'', K''], S_k)$
$C'' = \{C''_0 \ldots\ldots C''_m\}$
$K'' = \{K''_0 \ldots\ldots K''_m\}$
Generate nonce N_A
$D_1 = N_V$ XOR $F(K''_0, N_A)$
$D_2 = N_A'$ XOR $F(K''_1, M_1)$
$D_3 = D_1$ XOR $F(K''_2, D_2)$
......
$D_{m-1} = D_{m-3}$ XOR $F(K''_{m-2}, D_{m-2})$
$D_m = D_{m-2}$ XOR $F(K''_{m-1}, D_{m-1})$
$D = (D_m \,||\, D_{m-1})$ XOR K''_m
$P = m$ XOR K''_0
C'', D, P, MAC (ID_V || D || m || N_A)
For all C_i in C'':
Calculate K''_i = PUF(C_i)
m = P XOR K''_0
Calculate D_m & D_{m-1} using K''_m XOR D
$D_{m-2} = D_m$ XOR $F(K''_{m-1}, D_{m-1})$
......
Calculate N_A & verify MAC
Generate ($C^\#$, $K^\#$) pair and nonce N_O
$C^\# = \{C^\#_0 \ldots\ldots C^\#_m\}$ $K^\# = \{K^\#_0 \ldots\ldots K^\#_m\}$
$D'_i = K^\#_i$ XOR K''_i
$D'' = D'_0 \,||\, D'_1 \,||\, \ldots\ldots D'_m$
$P' = N_O$ XOR K''_0
Session Key (S_{k2}) = $F(K''_0, N_A')$ XOR $F(K''_0, N_O)$
$PID_V = ID_V$ XOR K''_0
C',M'',N, N', MAC (ID_A || M'' || m || N_C || S_{k2})
Calculate:
N_O using P' and K''_0
$K^\#_i$ using D'_i and K''_i
Verify MAC
Store ($C^\#$,$K^\#$)
Session Key (S_{k2}) = $F(K''_0, N_A')$ XOR $F(K''_0, N_O)$)
$PID_V = ID_V$ XOR K''_0
Session Key Established

Fig. 3: Mutual authentication between electric vehicle and the aggregator.

It also generates a nonce (N_B). To encrypt the message, the server uses a block-based encryption mechanism. Let F be any non-linear function which is public to everyone. Thus, even an adversary can know what F is. It can be verified that the security of the protocol does not depend on F. The grid server then computes the following:

$$M_1 = N_I \oplus F(K_0, N_B) \tag{3}$$

$$M_2 = N_B \oplus F(K_1, M_1) \tag{4}$$

$$M_3 = M_1 \oplus F(K_2, M_2) \tag{5}$$

TABLE I: Notations

Notation	Description
V, ID_V	Vehicle and its ID
M, ID_M	Aggregator(mediator) and its ID
G	Grid Server
$\|\|$	Concatenation operator
$\oplus$	XOR operation
F	A public non-linear function
$\{Msg\}_k$	Message Msg is encrypted using key k
Msg_{P2Q}	Message Msg is sent from V2G entity P to Q
$MAC(X)$	Message authentication code (MAC) of X
N_A, N_B, N_C N_I, N_O, N_V	Nonces generated at different stages
$(C, K), (C', K')$ $(C'', K''), (C^{\#}, K^{\#})$	Challenge-response pairs of PUF

$$M_i = M_{i-2} \oplus F(K_{i-1}, M_{i-1}), \ 3 \leq i \leq m \tag{6}$$

$$M_m = M_{m-1} \oplus F(K_{m-1}, M_{m-1}) \tag{7}$$

$$M = (M_{m-1}||M_m) \oplus K_m \tag{8}$$

$$N = m \oplus K_0. \tag{9}$$

4) The grid server sends C, M, N along with a MAC (message authentication code) to the aggregator ID_M as shown just after the first block under grid Server in Figure 2. The MAC is used to verify a few security essentials. The first parameter in the MAC is to identify the correct aggregator. Data integrity is ensured by the second and third parameters. The freshness of the source (grid server in this case) is identified by N_B, which is the last parameter. We use the same approach in the later stages of the protocol as well.
5) On receiving the message from the grid server, aggregator ID_M generates the key K as given in (2) using received challenge C as the input to its PUF. Then, the aggregator calculates m, as shown below:

$$m = N \oplus K_0 \tag{10}$$

6) Using m and K, it finds N_B as shown in the following equations by applying the same transformations used in the encryption equations equations (6), (8) and (9):

$$M_{m-1}||M_m = M \oplus K_m$$
$$M_{i-2} = M_i \oplus F(K_{i-1}, M_{i-1}), \ 3 \leq i \leq m$$
$$N_B = M_2 \oplus F(K_1, M_1)$$
$$N_I = M_1 \oplus F(K_0, N_B).$$

The aggregator uses the MAC to verify the source of the message, checks if its integrity has been compromised, and determines whether the message is fresh or not. If it fails to verify these security traits, authentication is terminated by the aggregator. Else, a nonce N_C is generated. For future authentication, it generates a random challenge response pair (C', K') using its PUF:

$$C' = (C'_0, C'_1, C'_2......C'_m)$$
$$K' = (K'_0, K'_1, K'_2......K'_m).$$

It then calculates M', M'', N' and session key S_k as follows:

$$M'_i = K'_i \oplus K_i$$
$$M'' = M'_0||M'_1||.....||M'_m$$
$$N' = N_C \oplus K_0$$
$$(S_k) = F(K_0, N_B) \oplus F(K_0, N_C).$$

7) Then, the aggregator sends C', M'', N, N', as well as the MAC to the grid server. Next, it erases interim variables from its memory. This time the MAC includes a fifth parameter which is the session key S_k. This ensures that both aggregator and grid server have the same session key.
8) On receiving the message from the aggregator, the grid server calculates N_C using N' and K_0:

$$N_C = N' \oplus K_0. \tag{11}$$

Then it calculates K' using M and K:

$$K'_i = M'_i \oplus K_i. \tag{12}$$

The new challenge-response pair (C', K') are stored in its memory. Then it calculates the session Key S_k as shown below and verifies the MAC:

$$(S_k) = F(K_0, N_B) \oplus F(K_0, N_C). \tag{13}$$

With the session key now established, MA between aggregator and grid server has been achieved.

B. Mutual Authentication between Vehicle and Aggregator

1) The previous subsection presented the protocol for aggregator and grid server establishing a session key S_k between themselves. This is shown as a small box in Figure 3. Now, we present the authentication between a vehicle and aggregator.
2) The aggregator sends an encoded message $Msg_{M2G} = E([ID_V, N_V], S_k)$ containing the ID of the vehicle ID_V, and its nonce N_V encoded with S_k to the grid server.
3) The grid server decodes this message using S_k and obtains ID_V and nonce N_V. It checks within its memory if ID_V exists and whether nonce N_V is fresh. If either of the conditions fails, the authentication request by the vehicle is terminated. Using ID_V, the grid server finds the corresponding challenge-response pairs (C'', K'') from its memory:

$$C'' = (C''_0, C''_1, C''_2......C''_m)$$
$$K'' = (K''_0, K''_1, K''_2......K''_m)$$

It then generates a nonce N_A. Similar to the previous subsection, it uses a block based encryption mechanism to encrypt the message.

$$\begin{gathered} D_1 = N_V \oplus F(K_0'', N_A') \\ D_2 = N_A' \oplus F(K_1'', D_1) \\ D_i = D_{i-2} \oplus F(K_{i-1}'', D_{i-1}),\ \ 3 \leq i \leq m \\ D_m = D_{m-2} \oplus F(K_{m-1}'', D_{m-1}) \\ D = (D_m || D_{m-1}) \oplus K_m'') \\ P = m \oplus K_0'' \end{gathered}$$

4) The aggregator sends C'', D, P and the MAC to the EV. Within the MAC, the first parameter verifies the identity of the vehicle. Data integrity is ensured by the second and third parameters. Freshness of the source (aggregator in this case) is identified by N_C which is the last parameter.
5) On receiving the message from the aggregator, the vehicle generates the key K'' by using its PUF for the newly received challenge C'' as given in (2). Then, it calculates m as shown below:

$$m = P \oplus K_0''. \tag{14}$$

Using m and K, it finds N_A as shown:

$$\begin{gathered} D_m || D_{m-1} = K_m'' \oplus D \\ D_{i-2} = D_i \oplus F(K_{i-1}'', D_{i-1}) \\ N_A' = D_2 \oplus F(K_1'', M_1) \\ N_V = D_1 \oplus F(K_0'', N_A). \end{gathered}$$

6) The vehicle uses the MAC to verify the source of the message, checks if its integrity has been compromised, and determines whether the message is fresh or not. If it fails to verify these security traits, authentication is terminated by the vehicle. Else, a nonce N_O is generated by the vehicle. For future authentication it generates a new challenge-response pair using its PUF:

$$\begin{gathered} C^{\#} = (C_0^{\#}, C_1^{\#}, C_2^{\#}......C_m^{\#}) \\ K^{\#} = (K_0^{\#}, K_1^{\#}, K_2^{\#}......K_m^{\#}). \end{gathered}$$

It then calculates D', D'', P' and session key S_{k2} as follows

$$\begin{gathered} D_i' = K_i^{\#} \oplus K_i'' \\ D'' = D_0' || D_1' || .....|| D_m' \\ P' = N_O \oplus K_0'' \\ S_{k2} = F(K_0'', N_A') \oplus F(K_0'', N_O)). \end{gathered}$$

The EV then calculates its new pseudonym or pseudo-ID PID_V to be used the next time it wants to authenticate:

$$PID_V = ID_V \oplus K_0'' \tag{15}$$

This ensures identity protection because an adversary will not be able to Figure out whether a previous transaction belonged to the same EV or not. ID_V then sends C', M'', P, P' and MAC. This time the MAC includes a fifth parameter which is the session key S_{k2}. This ensures that both EV and aggregator have the same session key.
7) On receiving the message from the vehicle, the aggregator calculates N_O using P and K_0'':

$$N_O = P' \oplus K_0''. \tag{16}$$

Then it calculates $K_i^{\#}$ using D_i' and K_i'':

$$K_i^{\#} = D_i' \oplus K_i''. \tag{17}$$

The new challenge-response pair $(C^{\#}, K^{\#})$ are stored in its memory. Then it calculates the session key S_{k2} as shown below and verifies the MAC:

$$S_{k2} = F(K_0'', N_A') \oplus F(K_0'', N_O). \tag{18}$$

The pseudonym or pseudo-ID PID_V is calculated as:

$$PID_V = ID_V \oplus K_0'' \tag{19}$$

PID_V will be encrypted with the already established session key S_k and then sent to the grid server to be updated in its database. Then it is deleted from the aggregator's memory. With the session key now established, MA between vehicle and aggregator has been achieved.

VI. Security Analysis

In this section, we formally show that our MA protocol is secure. We use BAN logic [33] and Mao and Boyd logic [34] which are extensively used for security analysis of protocols. In our analysis, we denote vehicle ID_V, aggregator ID_A, and the grid server by V, M, and G respectively.

A. Mao-Boyd Logic

The basic building blocks of Mao-Boyd Logic listed below are necessary to understand the protocol verification.

1) $A \mid\equiv B$: A believes B is legitimate and that it may function correspondingly.
2) $A \overset{K}{\mid\!\sim} B$: A encrypted B using key K.
3) $A \overset{K}{\triangleleft} B$: A sees B using decipherment key K.
4) $A \overset{K}{\leftrightarrow} B$: K is a valid shared key between entities A and B.
5) $\#(N)$: Nonce N is new and fresh.
6) $sup(P)$: P is a credible and reliable entity.
7) $A \triangleleft \parallel M$: Entity A does not have access to message M.

B. Security Analysis For Protocol

First, let us consider the MA between an EV and the power grid server. In order to prove the security features of our protocol, we justify that the secret information N_B, N_A, and K' are undisclosed to anyone other than V and S.

The primary understanding and assumptions used in the protocol of Figure 2 are listed as follows:

- $M \mid\equiv M \overset{K}{\leftrightarrow} G$ and $G \mid\equiv M \overset{K}{\leftrightarrow} G$: Every EV has a challenge-response pair which is stored in G. Using the challenge, M can use its PUF to get the corresponding response K.
- $M \mid\equiv G^c \triangleleft \parallel N_C$ and $G \mid\equiv M \mid\equiv \{G\}^c \triangleleft \parallel N_C$: N_C is generated by M.

- $G \overset{K}{\mid\!\sim} N_B$: First block under grid server in the protocol of figure 2.
- $M \mid\equiv \#(N_C)$ and $M \mid\equiv \#(N_1)$: M generates a new N_C and N_I each time.
- $G \mid\equiv \#(S_k))$: For each round of authentication, a new session-key S_k is generated by G.
- $M \mid\equiv sup(G)$: G is the most credible and reliable entity with-respect-to the session key S_k.
- $G \mid\equiv sup(M)$: M is the most credible and reliable entity with-respect-to N_C and K'.
- $M \overset{K}{\triangleleft} N_B$ **R** S_k: Second block under aggregator in Figure 2.
- $G \overset{K}{\triangleleft} S_k$ **R** N_C and $G \overset{K}{\triangleleft} S_k$ **R** K': Second block under grid server in Figure 2.
- $M \mid\equiv G \mid\equiv \{M\}^c \triangleleft \| S_k$ and $G \mid\equiv M^c \triangleleft \| S_k$: For each round of authentication, a new session key S_k is generated by G.
- $M \mid\equiv \{G\}^c \triangleleft \parallel K'$ and $G \mid\equiv M \mid\equiv \{G\}^c \triangleleft \parallel K'$ and $M \mid\equiv \#(K')$: For each iteration a new PUF response is generated by M.
- $M \overset{K}{\mid\!\sim} K'$: Second block under aggregator in Figure 2.

The proof that "**M** is convinced that N_C is a valid shared key between **M** and **G**"is shown in Figure 5b. The statement to be proven: $M \mid\equiv M \overset{N_C}{\leftrightarrow} G$ is written at the bottom. By showing that no entity except M and G knows N_C ($M \mid\equiv \{M, G\}^c \triangleleft \parallel N_C$) along with the fact that N_C is a new nonce ($M \mid\equiv \#(N_C)$), we can establish that N_C is a valid secret between entities M and G. By showing that entities M and G have a well-kept secret K ($M \mid\equiv M \overset{K^i}{\leftrightarrow} G$), and G received N_C from M after encryption with K ($M \overset{K}{\mid\!\sim} N_C$), we prove $M \mid\equiv \{M, G\}^c \triangleleft \parallel N_C$. From this, we can deduce the statement to be proven i.e., $M \mid\equiv M \overset{N_C}{\leftrightarrow} G$. In a similar way other necessary statements to verify the security of our protocols are proven in Figures 4 and 5.

VII. Comparison and Analysis

A. Security Goals And Protection Against Various Attacks

A comparison of the security features of our protocol with a different state of the art protocols currently in use in V2G systems is presented in Table II. "Yes" indicates that the protocol possesses a feature or is secure against an attack. "No" indicates that the protocol lacks a feature or is insecure against an attack. All the mentioned protocols provide MA except [22]. Without MA, a participating entity cannot verify if it is sending a message to a trusted entity, neither can it verify if the message it received is from a trusted entity. With MA, both the sending and receiving parties can be sure of each other's authenticity. Identity protection is not provided by the protocol in [21]. Consequently, an attacker may easily figure out the real identity of the EV by looking at the usage data. This means the owner's privacy is compromised. The protocol in [18] and [20] do not provide message integrity. Our protocol uses MAC to ensure this. All the entities EV, aggregator and grid server can easily detect any tampering in the message they receive. The protocol in [18] is vulnerable to man-in-the-middle attacks. An adversary may insert himself between the communication of an EV and aggregator, or between the aggregator and gain control of the communication between them. The protocols in [17], [18] and [20] are vulnerable against impersonation attacks. The protocols in [18] and [20] are not secure against replay attacks. The protocol in [18] and [21] do not provide session key security. Physical security is provided only by SUKA. As mentioned in section IV-B, an attacker who captures an EV device must not be able to gather any secrets. As already mentioned in section I, almost all authentication protocols proposed in the literature necessitate that the EVs store at least one secret in their memory, if not more. Such storing of secrets on any device renders the protocols ineffective and vulnerable to physical attacks. The MA protocol proposed in this paper has two features which make it resistant to any physical attacks: (i) EVs and aggregators need not store any secrets in their memory; (ii) There is secure communication between the EV's microcontroller and its PUF. Because they are both on the same chip [35], even though an attacker may physically capture the device, it would be impossible for them to extract any secret. Therefore, SUKA is resilient against physical attacks. The papers in [17], [18] [20], [22] and [29] do not provide a formal security proof for their proposed protocols.

B. Computation Overhead

In Table III we present a comparison of the computation costs of our protocol with some state-of-the-art protocols which have a similar system model as ours. We show the comparison for the case where one EV is authenticating with the grid.

In Table III, the number of cryptographic operations, pairing operations, encryption/decryption, hash operations,MAC computations and PUF executions are listed for one round of authentication. Our protocol uses only 33 cryptographic operations (which include XOR, addition, scalar multiplication and exponential computation) compared to 37 in [16] and 36 in [18]. Our protocol uses zero pairing operations. While [18] has only 2 encryption/decryption Operations and 4 MAC/HMAC computations, it has 9 Hash function computations while ours has zero. Although [16] has no encryption/decryption operations or MAC/HMAC computations, it has 16 hash computations while ours has none. While there is no physical security in [17],[18] and [16] our protocol is physically secured by the use of PUFs which requires 2 operations. We argue that the overall performance of our protocol is much better due to lesser computation overhead and far superior security features.

VIII. Conclusions

This paper proposed MA protocols for the two stages or steps which arise in a V2G system: (i) For MA between the aggregator and the grid server, And (ii) for MA between EV and aggregator. Our protocol SUKA uses challenge-response architecture, which is enabled by PUFs. This gives our protocols the advantage of not having to store any secret information in EVs and Aggregators. Secrets are stored only in the grid server. Only one challenge-response pair is stored in the server for every EV. Two session keys are established when

$$\dfrac{\dfrac{\dfrac{\dfrac{M \mid\equiv \#(N_I) \wedge \dfrac{M \mid\equiv M \overset{K}{\leftrightarrow} G \wedge M \overset{K}{\triangleleft} N_I}{M \mid\equiv G \overset{K}{\mid\!\sim} N_I}}{M \mid\equiv G \mid\equiv M \overset{K}{\leftrightarrow} G} \wedge M \mid\equiv G \mid\equiv \{M\}^c \triangleleft\| S_k \wedge \dfrac{M \mid\equiv M \overset{K}{\leftrightarrow} G \wedge M \overset{K}{\triangleleft} S_k}{M \mid\equiv G \overset{K}{\mid\!\sim} S_k}}{M \mid\equiv G \mid\equiv \{M,G\}^c \triangleleft\| S_k} \wedge M \mid\equiv sup(G)}{M \mid\equiv \{M,G\}^c \triangleleft\| S_k} \wedge M \mid\equiv sup(G) \wedge \dfrac{M \mid\equiv \#(N_I) \wedge \dfrac{M \overset{K}{\triangleleft} N_I \ \mathbf{R}\ S_k}{M \triangleleft N_I \ \mathbf{R}\ S_k}}{M \mid\equiv \#(S_k)}}{M \mid\equiv M \overset{S_k}{\leftrightarrow} G}$$

(a) Proof for: “**M** is convinced that S_k as a valid shared key between **M** and **G**”.

$$\dfrac{\dfrac{M \mid\equiv M \overset{K}{\leftrightarrow} G \wedge M \mid\equiv G^c \triangleleft\| N_C \wedge M \overset{K}{\mid\!\sim} N_C}{M \mid\equiv \{M,G\}^c \triangleleft\| N_C} \wedge M \mid\equiv \#(N_C)}{M \mid\equiv M \overset{N_C}{\leftrightarrow} G}$$

(b) Proof for: “**M** is convinced that N_C is a valid shared key between **M** and **G**”.

$$\dfrac{\dfrac{\dfrac{\dfrac{G \mid\equiv \#(S_k) \wedge \dfrac{G \mid\equiv M \overset{K}{\leftrightarrow} G \wedge G \overset{K}{\triangleleft} S_k}{G \mid\equiv M \overset{K}{\mid\!\sim} S_k}}{G \mid\equiv M \mid\equiv M \overset{K}{\leftrightarrow} G} \wedge G \mid\equiv M \mid\equiv \{G\}^c \triangleleft\| N_C \wedge \dfrac{G \mid\equiv M \overset{K}{\leftrightarrow} G \wedge G \overset{K}{\triangleleft} N_C}{G \mid\equiv M \overset{K}{\mid\!\sim} N_C}}{G \mid\equiv M \mid\equiv \{M,G\}^c \triangleleft\| N_C} \wedge G \mid\equiv sup(M)}{G \mid\equiv \{M,G\}^c \triangleleft\| N_C} \wedge \dfrac{G \mid\equiv \#(S_k) \wedge \dfrac{G \overset{K}{\triangleleft} S_k \ \mathbf{R}\ N_C}{G \triangleleft S_k \ \mathbf{R}\ N_C}}{G \mid\equiv \#(N_C)}}{G \mid\equiv M \overset{N_C}{\leftrightarrow} G}$$

(c) Proof for: “**G** is convinced that N_C is a valid shared key between **M** and **G**”.

$$\dfrac{\dfrac{G \mid\equiv M \overset{K}{\leftrightarrow} G \wedge G \mid\equiv M^c \triangleleft\| S_k \wedge G \overset{K}{\mid\!\sim} S_k}{G \mid\equiv \{M,G\}^c \triangleleft\| S_k} \wedge G \mid\equiv \#(S_k)}{G \mid\equiv M \overset{S_k}{\leftrightarrow} G}$$

(d) Proof for: “**G** is convinced that S_k is a valid shared key between **M** and **G**”.

$$\dfrac{\dfrac{\dfrac{\dfrac{G \mid\equiv \#(S_k) \wedge \dfrac{G \mid\equiv M \overset{K}{\leftrightarrow} G \wedge G \overset{K}{\triangleleft} S_k}{G \mid\equiv M \overset{K}{\mid\!\sim} S_k}}{G \mid\equiv M \mid\equiv M \overset{K}{\leftrightarrow} G} \wedge G \mid\equiv M \mid\equiv \{G\}^c \triangleleft\| K' \wedge \dfrac{G \mid\equiv M \overset{K}{\leftrightarrow} G \wedge G \overset{K}{\triangleleft} K'}{G \mid\equiv M \overset{K}{\mid\!\sim} K'}}{G \mid\equiv M \mid\equiv \{M,G\}^c \triangleleft\| K'} \wedge G \mid\equiv sup(M)}{G \mid\equiv \{M,G\}^c \triangleleft\| K'} \wedge \dfrac{G \mid\equiv \#(S_k) \wedge \dfrac{G \overset{K}{\triangleleft} S_k \ \mathbf{R}\ K'}{G \triangleleft S_k \ \mathbf{R}\ K'}}{G \mid\equiv \#(K')}}{G \mid\equiv M \overset{K'}{\leftrightarrow} G}$$

(e) Proof for: “**G** is convinced that K' is a valid shared key between **M** and **G**”.

$$\dfrac{\dfrac{M \mid\equiv M \overset{K}{\leftrightarrow} G \wedge M \mid\equiv G^c \triangleleft\| K' \wedge M \overset{K}{\mid\!\sim} K'}{M \mid\equiv \{M,G\}^c \triangleleft\| K'} \wedge M \mid\equiv \#(K')}{M \mid\equiv M \overset{K'}{\leftrightarrow} G}$$

(f) Proof for: “**M** is convinced that K' is a valid shared key between **M** and **G**”.

Fig. 4: Proof for authentication between aggregator and power grid server

$$\dfrac{\dfrac{\dfrac{\dfrac{V \mid\equiv \#(N_V) \wedge \dfrac{V \mid\equiv V \overset{K''}{\leftrightarrow} M \wedge V \overset{K''}{\triangleleft} N_V}{V \mid\equiv M \overset{K''}{\mid\!\sim} N_V}}{V \mid\equiv M \mid\equiv V \overset{K''}{\leftrightarrow} M} \wedge V \mid\equiv M \mid\equiv \{V\}^c \triangleleft\| S_{k2} \wedge \dfrac{V \mid\equiv V \overset{K''}{\leftrightarrow} M \wedge V \overset{K''}{\triangleleft} S_{k2}}{V \mid\equiv M \overset{K''}{\mid\!\sim} S_{k2}}}{V \mid\equiv M \mid\equiv \{V,M\}^c \triangleleft\| S_{k2}} \wedge V \mid\equiv sup(M)}{V \mid\equiv \{V,M\}^c \triangleleft\| S_{k2}} \wedge V \mid\equiv sup(M) \wedge \dfrac{V \mid\equiv \#(N_V) \wedge \dfrac{V \overset{K''}{\triangleleft} N_V \ \mathbf{R}\ S_{k2}}{V \triangleleft N_V \ \mathbf{R}\ S_{k2}}}{V \mid\equiv \#(S_{k2})}}{V \mid\equiv V \overset{S_{k2}}{\leftrightarrow} M}$$

(a) Proof for: “**V** is convinced that S_{k2} as a valid shared key between **V** and **M**”.

$$\dfrac{\dfrac{V \mid\equiv V \overset{K''}{\leftrightarrow} M \wedge V \mid\equiv M^c \triangleleft\| N_O \wedge V \overset{K''}{\mid\!\sim} N_O}{V \mid\equiv \{V,M\}^c \triangleleft\| N_O} \wedge V \mid\equiv \#(N_O)}{V \mid\equiv V \overset{N_O}{\leftrightarrow} M}$$

(b) Proof for: “**V** is convinced that N_O is a valid shared key between **V** and **M**”.

$$\dfrac{\dfrac{\dfrac{\dfrac{M \mid\equiv \#(S_{k2}) \wedge \dfrac{M \mid\equiv V \overset{K''}{\leftrightarrow} M \wedge M \overset{K''}{\triangleleft} S_{k2}}{M \mid\equiv V \overset{K''}{\mid\!\sim} S_{k2}}}{M \mid\equiv V \mid\equiv V \overset{K''}{\leftrightarrow} M} \wedge M \mid\equiv V \mid\equiv \{M\}^c \triangleleft\| N_O \wedge \dfrac{M \mid\equiv V \overset{K''}{\leftrightarrow} M \wedge M \overset{K''}{\triangleleft} N_O}{M \mid\equiv V \overset{K''}{\mid\!\sim} N_O}}{M \mid\equiv V \mid\equiv \{V,M\}^c \triangleleft\| N_O} \wedge M \mid\equiv sup(V)}{M \mid\equiv \{V,M\}^c \triangleleft\| N_O} \wedge \dfrac{M \mid\equiv \#(S_{k2}) \wedge \dfrac{M \overset{K''}{\triangleleft} S_{k2} \ \mathbf{R}\ N_O}{M \triangleleft S_{k2} \ \mathbf{R}\ N_O}}{M \mid\equiv \#(N_O)}}{M \mid\equiv V \overset{N_O}{\leftrightarrow} M}$$

(c) Proof for: “**M** is convinced that N_O is a valid shared key between **V** and **M**”.

$$\dfrac{\dfrac{M \mid\equiv V \overset{K''}{\leftrightarrow} M \wedge M \mid\equiv V^c \triangleleft\| S_{k2} \wedge M \overset{K''}{\mid\!\sim} S_{k2}}{M \mid\equiv \{V,M\}^c \triangleleft\| S_{k2}} \wedge M \mid\equiv \#(S_{k2})}{M \mid\equiv V \overset{S_{k2}}{\leftrightarrow} M}$$

(d) Proof for: “**M** is convinced that S_{k2} is a valid shared key between **V** and **M**”.

$$\dfrac{\dfrac{\dfrac{\dfrac{M \mid\equiv \#(S_{k2}) \wedge \dfrac{M \mid\equiv V \overset{K''}{\leftrightarrow} M \wedge M \overset{K''}{\triangleleft} S_{k2}}{M \mid\equiv V \overset{K''}{\mid\!\sim} S_{k2}}}{M \mid\equiv V \mid\equiv V \overset{K''}{\leftrightarrow} M} \wedge M \mid\equiv V \mid\equiv \{M\}^c \triangleleft\| K^{\#} \wedge \dfrac{M \mid\equiv V \overset{K''}{\leftrightarrow} M \wedge M \overset{K''}{\triangleleft} K^{\#}}{M \mid\equiv V \overset{K''}{\mid\!\sim} K^{\#}}}{M \mid\equiv V \mid\equiv \{V,M\}^c \triangleleft\| K^{\#}} \wedge M \mid\equiv sup(V)}{M \mid\equiv \{V,M\}^c \triangleleft\| K^{\#}} \wedge \dfrac{M \mid\equiv \#(S_{k2}) \wedge \dfrac{M \overset{K''}{\triangleleft} S_{k2} \ \mathbf{R}\ K^{\#}}{M \triangleleft S_{k2} \ \mathbf{R}\ K^{\#}}}{M \mid\equiv \#(K^{\#})}}{M \mid\equiv V \overset{K^{\#}}{\leftrightarrow} M}$$

(e) Proof for: “**M** is convinced that $K^{\#}$ is a valid shared key between **V** and **M**”.

$$\dfrac{\dfrac{V \mid\equiv V \overset{K''}{\leftrightarrow} M \wedge V \mid\equiv M^c \triangleleft\| K^{\#} \wedge V \overset{K''}{\mid\!\sim} K^{\#}}{V \mid\equiv \{V,M\}^c \triangleleft\| K^{\#}} \wedge V \mid\equiv \#(K^{\#})}{V \mid\equiv V \overset{K^{\#}}{\leftrightarrow} M}$$

(f) Proof for: “**V** is convinced that $K^{\#}$ is a valid shared key between **V** and **M**”.

Fig. 5: Proof for authentication between EV and aggregator

TABLE II: Comparison of Security Features

Features	[16]	[17]	[18]	[20]	[21]	[22]	[29]	SUKA
Mutual Authentication	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Identity Protection	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Message Integrity	Yes	Yes	No	No	Yes	Yes	Yes	Yes
Man-In-The-Middle Attack	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Impersonation Attack	Yes	No	No	No	Yes	Yes	Yes	Yes
Replay Attack	Yes	Yes	No	No	Yes	Yes	Yes	Yes
Session Key Security	Yes	Yes	No	Yes	No	Yes	Yes	Yes
Physical Security	No	No	No	No	No	No	No	Yes
Formal Security Proof	Yes	No	No	No	Yes	No	No	Yes

TABLE III: Comparison of computation overhead

Operations	[17]	[18]	[16]	SUKA
Cryptographic Operations ($\oplus, +,$ scalar multiplication and exponent)	81	36	37	33
Pairing	19	-	-	-
Encryption/Decryption	-	2	-	2
Hash (H)	6	9	16	-
MAC/HMAC	7	4	-	8
PUF	-	-	-	2

an EV wants to authenticate with the grid server: one session key between the aggregator and grid server, and another one between EV and aggregator. We showed that SUKA has MA, identity protection, message Integrity, physical security, session key security along with protection against various attacks such as MITM attack, replay attacks and impersonation attacks. Moreover, it uses simple computations, which makes it very efficient and fast. Hence, we argue that the proposed protocol, SUKA, is a very viable solution for upcoming V2G systems.

References

[1] B. K. Sovacool and R. F. Hirsh, “Beyond batteries: An examination of the benefits and barriers to plug-in hybrid electric vehicles (phevs) and a vehicle-to-grid (v2g) transition,” *Energy Policy*, vol. 37, no. 3, pp. 1095–1103, 2009.

[2] C. D. White and K. M. Zhang, “Using vehicle-to-grid technology for frequency regulation and peak-load reduction,” *Journal of Power Sources*, vol. 196, no. 8, pp. 3972–3980, 2011.

[3] H. Liu, Z. Hu, Y. Song, and J. Lin, “Decentralized vehicle-to-grid control for primary frequency regulation considering charging demands,” *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3480–3489, 2013.

[4] H. Lund and W. Kempton, “Integration of renewable energy into the transport and electricity sectors through v2g,” *Energy policy*, vol. 36, no. 9, pp. 3578–3587, 2008.

[5] L. Gelazanskas and K. A. Gamage, “Demand side management in smart grid: A review and proposals for future direction,” *Sustainable Cities and Society*, vol. 11, pp. 22–30, 2014.

[6] 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 Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2340–2351, 2015.

[7] A. Abdallah and X. Shen, “Lightweight Security and Privacy-Preserving Scheme for V2G Connection,” in *2015 IEEE Global Communications Conference (GLOBECOM)*. IEEE, dec 2015, pp. 1–7. [Online]. Available: http://ieeexplore.ieee.org/document/7417592/

[8] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, “Design and Implementation of PUF-Based ”Unclonable” RFID ICs for Anti-Counterfeiting and Security Applications,” in *2008 IEEE International Conference on RFID*. IEEE, apr 2008, pp. 58–64. [Online]. Available: https://ieeexplore.ieee.org/document/4519377/

[9] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, “Brand and IP protection with physical unclonable functions,” in *2008 IEEE International Symposium on Circuits and Systems*. IEEE, may 2008, pp. 3186–3189. [Online]. Available: http://ieeexplore.ieee.org/document/4542135/

[10] W. Kempton and J. T. Tomic, “Vehicle-to-grid power fundamentals: Calculating capacity and net revenue,” *Journal of Power Sources*, vol. 144, pp. 268–279, 2005. [Online]. Available: http://www.udel.edu/V2G.

[11] Sekyung Han, Soohee Han, and K. Sezaki, “Development of an Optimal Vehicle-to-Grid Aggregator for Frequency Regulation,” *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 65–72, jun 2010. [Online]. Available: http://ieeexplore.ieee.org/document/5446440/

[12] F. Kennel, D. Gorges, and S. Liu, “Energy management for smart grids with electric vehicles based on hierarchical MPC,” *IEEE Transactions on Industrial Informatics*, vol. 9, no. 3, pp. 1528–1537, 2013.

[13] 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. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0301421509003978

[14] B. K. Sovacool and R. F. Hirsh, “Beyond batteries: An examination of the benefits and barriers to plug-in hybrid electric vehicles (PHEVs) and a vehicle-to-

grid (V2G) transition," 2008. [Online]. Available: www.elsevier.com/locate/enpol

[15] L. Pieltain Fernández, T. Gómez San Román, R. Cossent, C. Mateo Domingo, and P. Frías, "Assessment of the impact of plug-in electric vehicles on distribution networks," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 206–213, 2011.

[16] N. Saxena, S. Grijalva, V. Chukwuka, and A. V. Vasilakos, "Network Security and Privacy Challenges in Smart Vehicle-to-Grid," *IEEE Wireless Communications*, vol. 24, no. 4, pp. 88–98, 2017.

[17] 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 Transactions on Smart Grid*, vol. 2, no. 4, pp. 697–706, dec 2011. [Online]. Available: http://ieeexplore.ieee.org/document/5771586/

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

[19] H.-R. Tseng, "A secure and privacy-preserving communication protocol for V2G networks," in *2012 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, apr 2012, pp. 2706–2711. [Online]. Available: http://ieeexplore.ieee.org/document/6214259/

[20] H. Liu, H. Ning, Y. Zhang, Q. Xiong, and L. T. Yang, "Role-dependent privacy preservation for secure v2g networks in the smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, pp. 208–220, feb 2014.

[21] J. L. Tsai and N. W. Lo, "Secure Anonymous Key Distribution Scheme for Smart Grid," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 906–914, mar 2016.

[22] A. Abdallah and X. Shen, "Lightweight Authentication and Privacy-Preserving Scheme for V2G Connections," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2615–2629, 2017.

[23] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably Secure Authenticated Key Agreement Scheme for Smart Grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1900–1910, may 2018.

[24] 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 of Things Journal*, vol. 5, no. 4, pp. 2526–2536, aug 2018.

[25] H. Guo, Y. Wu, F. Bao, H. Chen, and M. Ma, "UBAPV2G: A unique batch authentication protocol for vehicle-to-grid communications," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 707–714, 2011.

[26] H. Liu, H. Ning, Y. Zhang, and M. Guizani, "Battery status-aware authentication scheme for V2G networks in smart grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 99–110, 2013.

[27] J. Chen, Y. Zhang, and W. Su, "An anonymous authentication scheme for plug-in electric vehicles joining to charging/discharging station in vehicle-to-Grid (V2G) networks," *China Communications*, vol. 12, no. 3, pp. 9–19, 2015.

[28] N. Saxena and B. J. Choi, "Authentication Scheme for Flexible Charging and Discharging of Mobile Vehicles in the V2G Networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1438–1452, jul 2016.

[29] M. Tao, K. Ota, M. Dong, and Z. Qian, "AccessAuth: Capacity-aware security access authentication in federated-IoT-enabled V2G networks," *J. Parallel Distrib. Comput.*, vol. 118, pp. 107–117, 2018. [Online]. Available: https://doi.org/10.1016/j.jpdc.2017.09.004

[30] P. Gope and B. Sikdar, "Lightweight and Privacy-Friendly Spatial Data Aggregation for Secure Power Supply and Demand Management in Smart Grids," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1554–1566, jun 2019.

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

[32] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and U. Ruhrmair, "The Bistable Ring PUF: A new architecture for strong Physical Unclonable Functions," in *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*. IEEE, jun 2011, pp. 134–141. [Online]. Available: http://ieeexplore.ieee.org/document/5955011/

[33] C. Boyd and W. Mao, "On a Limitation of BAN Logic," in *Advances in Cryptology EUROCRYPT '93*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1993, pp. 240–247. [Online]. Available: http://link.springer.com/10.1007/3-540-48285-7{_}20

[34] W. Mao and C. Boyd, "Towards formal analysis of security protocols," in *[1993] Proceedings Computer Security Foundations Workshop VI*. IEEE Comput. Soc. Press, pp. 147–158. [Online]. Available: http://ieeexplore.ieee.org/document/246631/

[35] S. Sutar, A. Raha, and V. Raghunathan, "Memory-based combination pufs for device authentication in embedded systems," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 4, no. 4, pp. 793–810, 2018.