sTrade 2.0: Efficient Mutual Authentication Scheme for Energy Trading in V2G using Physically Unclonable Function

Giriraj Sharma, *Graduate Student Member, IEEE*, Amit M. Joshi, *Senior Member, IEEE*, Saraju P. Mohanty, *Senior Member, IEEE*

Abstract- This paper presents a mutual authentication scheme for vehicle-to-grid (V2G) using physical unclonable functions (PUF). Various security challenges exist during the transfer of information between entities in V2G over public channels. The proposed sTrade 2.0 security primitive allows energy trading only after secure authentication of charging station (CS) and electric vehicles (EVs) with a grid server (GS). Generally, CS are unmanned, and EVs are parked in open spaces; hence, physical security is a major challenge. PUFs are created by utilizing internal manufacturing variations that occur during the chip fabrication process. Random number generator bit self-test-arbiter PUF (RBST-APUF) has been used for experimental validation of sTrade 2.0. PUF is integrated with EV and CS; hence no need to store any secret key. Formal security verification is performed using the Random or Real (ROR) model and popular automatic verification of internet security protocol (AVISPA) simulation tool, while informal security verification uses Dolev-Yao (DY) and CK adversary model. Further, the performance evaluation result shows that our scheme uses minimum computational and communicational overheads compared with most recent schemes.

***Index Terms*—Smart Grid; Physical Unclonable Function (PUF); Vehicle to grid (V2G); Energy Trading, Security.**

I. Introduction

V2G is a promising technology that enables EVs to interact with the power grid to draw power from the electric grid and return energy from their batteries to the electric grid. This technology holds tremendous potential for smart cities, offering efficient, emission-free transportation while utilizing renewable energy sources for recharging. A key feature of V2G is its bi-directional energy flow, facilitating effective generation and distribution of electricity among consumers and prosumers [1]. V2G allows the charging of EVs during slack hours and discharge during peak hours. It lowers the grid's peak demand and gets reward points for EVs to participate in energy trading. The V2G system comprises essential components, including EVs, CS, and GS.

G. Sharma is with the Department of ECE, Malaviya National Institute of Technology, Jaipur, India 302017, Email: 2019rec9564@mnit.ac.in

A. M. Joshi is with the Department of ECE, Malaviya National Institute of Technology, Jaipur, India 302017, E-mail: amjoshi.ece@mnit.ac.in.

S. P. Mohanty is with the Department of Computer Science and Engineering, University of North Texas, USA 76207, E-mail: saraju.mohanty@unt.edu.

With the progress of information and communication technology (ICT), secure and reliable communication has become challenging in the V2G network. EVs and CS authenticate GS before the commissioning of energy trading. An adversary may steal confidential data and information like power consumption and energy patterns and may manipulate data and send false information to lead to the wrong decision by the server [2]. As EV and CS remain in an open network and communicate over public channels, the adversary may also get physical access and retrieve essential data from non-volatile memory; hence, a secure and reliable authentication protocol and hardware security are essential.

Numerous authentication protocols have been implemented for the V2G environment, employing cryptographic techniques like elliptic curve cryptography, identity-based encryption, hash functions, and PUF to ensure secure communication between entities. However, some protocols, such as [3] and [4], are unsuitable for resource-constrained devices. Most schemes either lack essential security attributes or incur large communication and computational expenses. Given these limitations in existing protocols, we propose a lightweight authentication and key agreement scheme that prioritizes entity privacy and security within the V2G network [5].

The paper's organization is as follows: Section II defines the related literature on the security of the V2G network, while section III describes the contribution of the current paper. An overview of PUF background is given in section IV. Section V explains the network and threat model of the proposed scheme. Section VI discusses the registration and different authentication phases for the V2G network. Section VII explains the security analysis of the proposed scheme. The performance comparison with state-of-the-art work is carried out in section VIII, while section IX concludes the work.

II. State of Art Work in V2G Network

A. Industrial electronics market for V2G Technology

The market growth of the V2G network was about US$ 1.77 billion in 2022. It may reach around US$ 17.43 billion with a CAGR of 48% in the next five years. The awareness of smart power generation is continuously increasing with the usage of EVs, which has fostered the application of industrial electronics in V2G [4]. Various countries' government policies have also boosted the adaptation of battery-operated vehicles over petrol and diesel vehicles. The annual sale of EVs

reported a 40% increase for 2019 and expects to grow at 18% in the next decade [6]. The V2G technology would be able to combat the challenge of peak demand in the energy sector and is likely to be adopted around the globe by 2030. The charging mechanism of batteries will be faster with the growth of the electronics industry in the coming years, which may increase the load on power grids. Hence, the role of V2G would be greater in the grid energy balance system [7].

B. Prior Work for V2G Security

Secure, efficient and reliable communication is paramount in the V2G network. The concept of V2G energy trading for the smart grid was elaborated by [14]. Later, various research schemes were proposed for V2G in smart grid [4], [13], [15]. A lightweight cryptography authentication protocol for V2G based on bilinear pairing was suggested by [15]. This scheme suffers large overheads and physical security challenges due to bilinear pairing. A lightweight and secure scheme based on PUF for the smart grid was introduced by [16]. The protocol protects the privacy of EV locations and could stop different security attacks with minimum computing overhead on the EV side. However, this scheme is unable to provide the physical security and anonymity.

The major challenge is hardware protection, where NVM stores secret keys, and intruders may steal confidential information through different attacks. To mitigate these issues, [17] suggested schemes based on reconfigurable PUF for physical security and energy theft. However, the scheme does not support the dynamic addition of EV and CS. However, [18] pointed out that the scheme [17] does not resist replay and DoS attacks.

In postquantum cryptography (PQC) standardization, Falcon and SABER are effective key encapsulation mechanisms, and a compact signature protocol was suggested by [19], [20]. A simple and flexible cryptographic protocol SABER is extremely suitable for potential attacks in the post-quantum era [21], [22]. Later, a PUFchain authenticated scheme based on PUF and blockchain was suggested by [23], which supports the physical security of devices by using a PUF. However, the scheme was unable to mitigate machine learning-based modeling attacks. PUF-based mutual authentication scheme for the smart grid was designed with a PUF-based fuzzy extractor [24]. The scheme was robust against physical attacks and the DY intruder model. Still, it is prone to temporary leakage in the CK-adversary model, and the performance of the smart meter is suboptimal.

The solution was proposed involving the usage of an ideal multi-blockchain system for EVs to address the challenge of storing charge records post-energy trading [25]. This approach introduces an annealing-based algorithm for determining server-node allocation and emphasizes the optimization of storage selection within each blockchain. A recent contribution by [26] explores enhanced security algorithms for Distributed Energy Resources based on recommendations from IEEE 1547-2018 interconnection and interoperability standards. The suggested algorithms include the Isolation Forest algorithm, trained on features derived from local current measurements. The approach incorporates physical dynamics into the data recovery algorithm, adopting a blended data-driven and physics-based strategy to enhance detection accuracy while minimizing operational costs. A PUF-based authentication scheme for the V2G network was suggested by [8]. The protocol demonstrates that it can resist physical attack. However, as the EV transmits a real ID during the authentication process, an adversary or even CS can find the location of the EV and misuse it. Later [9] claimed that their scheme did not reveal the location identity of the EVs against other connected entities. Their scheme was vulnerable to EV anonymity and high overhead, making it unsuitable for resource-constrained devices. The scheme in [10] described a PUF-based authentication scheme that provides physical security to both EV and CS with minimum overhead. This scheme does not support the scheduling feature; hence, whenever any EV needs to charge, it reaches CS without knowing the estimated time for charging and sometimes has to wait for a long time. However, the scheme supports energy trading, where EVs get reward points if they discharge during peak hours. An effective, lightweight authentication scheme for V2G using PUF was suggested by [12]. It supports the privacy and physical security of EVs. The author claimed various security features but did not suggest any formal verification or simulation of security protocol, and there was no information about computational overhead. A lightweight mutual authentication scheme based on elliptical curve cryptography and PUF for smart grid was proposed by [27]. The security was verified using the ProVerif tool and RoR model. The scheme withstands popular attacks, but it suffers from physical and modeling attacks. A mutual authentication scheme for Industrial IoT based on PUF was proposed by [28] and claims that this scheme resists modelling and physical attack. However, the scheme did not support anonymity and suffers from higher overheads. The comparative analysis of proposed scheme with related work is defined in Table I.

Several schemes suggested TPM, elliptical cryptography, hash function, and PUF-based protocol for smart grid V2G networks [29]. However, most schemes either suffer from larger overheads, physical security, or various security attacks. Hence, we proposed an RBST-APUF-based V2G mutual authentication scheme for the smart grid, which mitigates issues of limitation of the previously proposed approach.

III. Research gap and novel contribution

A. Research Gap

In PUF-based authentication, the output can change due to environmental variations, shifts in hardware device parameters, and changes in input voltage. These conditions can influence the authentication process significantly. The points below outline the research gaps that require to be addressed for reliable PUF-based V2G authentication systems :

- A PUF-based lightweight security framework where a PUF module can be integrated inside EV and CS and authenticate the nodes.
- A reliable PUF is required which supports error correction. Also, it can resist machine learning modeling and physical attacks.

TABLE I
A COMPARATIVE ANALYSIS OF DIFFERENT POPULAR SCHEMES

Works	Primitive used	Features	Vulnerabilities
Bansal, et al. 2020 [8]	PUF, Hash function	Provide hardware security	EV transmits real ID during the authentication; hence adversary can find the location of the EV and misuse it
Kaveh, et al. 2020 [9]	PUF, Hash function	Supports Identity prevention to CS but not support to EV	Does not support physical securities at EV
Sharma, et al. 2021 [10]	PUF, Hash, XOR	Support completer hardware security for EV and CS.	No computational cost analysis
Das, et al. 2022 [11]	IoT, PUF	Smart meter authentication	Unable to prevent energy theft
Jiang, et al. 2022 [12]	PUF, XOR, Hash	Supports security and privacy	No overhead analysis and simulation performed
Reddy, et al. 2023 [13]	PUF, XOR	Prevents Modeling attack	Reliability of PUF
This work (sTrade 2.0)	RBST-APUF, XOR, Hash function	Hardware security for EV and CS, Reliability of PUF, Error correction	No known security threats

- The protocol should supports location privacy. No entity like CS, EV, or adversary can trace each other's locations. The protocol should also support distributed charging-record management for EV networks during energy trading [25].
- Most schemes have large computation and communication overhead, and there is a need for a more efficient scheme.

B. Novel contribution

We introduce a V2G authentication technique achieved through the integration of PUF within EVs and CS. This integration significantly minimizes the susceptibility of the system and security threats.The conceptual model of sTrade2.0 is depicted in Fig. 1. The major contributions of the current paper are :

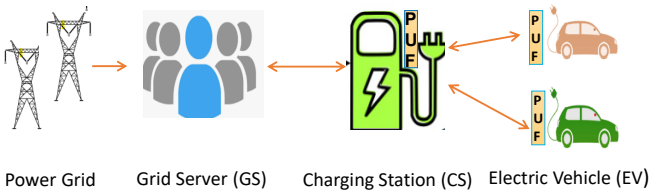

Fig. 1. Basic Overview of PUF based V2G Network

- A PUF-based lightweight hardware security framework is designed where a PUF module can be integrated inside EV and CS and can generate a unique fingerprint.
- The proposed random number generator bit self-test PUF (RBST-APUF) is reliable, and no extra hardware is required for error correction. This protocol can resist machine learning modeling and physical attack on PUF.
- The proposed protocol supports location privacy for EVs. Except for GS, no other entity like CS, EV, or adversary can trace each other's locations.
- Security verification and formal protocol analysis are demonstrated using the popular DY and CK adversary model, ROR model, and popular simulation tool AVISPA.
- sTrade2.0 is compared in terms of security, communication, and computation overhead with the existing popular scheme, demonstrating that our scheme is more efficient.

IV. PHYSICAL UNCLONABLE FUNCTION (PUF)

A PUF is a fingerprint based on the unique physical properties of the device. The PUF does not require memory to store the key. We proposed a random number generator bit self-test arbiter PUF (RBST-APUF).The proposed RBST-APUF model is shown in Fig. 2 and the block diagram is described in Fig. 3. It comprises four modules: A channelized random module, a traditional APUF, a reliability flag generator, and a self-test module. A multiplexer and a crossbar switch comprise an N-stage classical APUF. A flip flop is an arbitrator, converting analog delay into a 1/0 digital response. The self-test module is made up of two 2-2 multiplexers, two 2-1 multiplexers, and a delay module that is all connected to A1. The reliability flag generator includes XNOR.

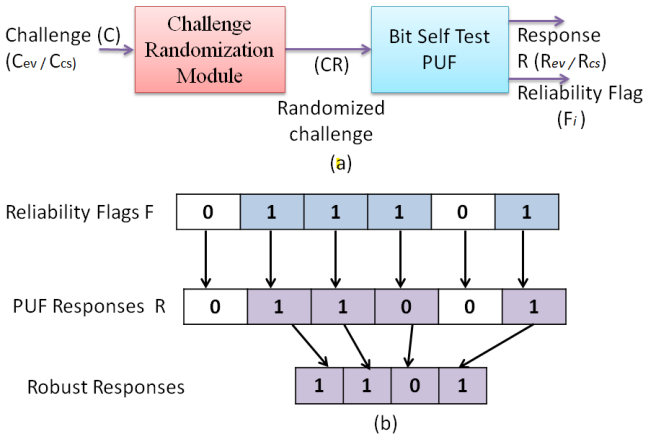

Fig. 2. RNG Bit self-test APUF (a) Model of bit self-test PUF (b) Extraction of robust response

A. *Modeling attacks and RBST-APUF:*

Recently, various machine learning-based modeling attacks successfully broke the CRP of PUF. To achieve this, the adversary collects many CRPs (C1, R1),(C2, R2)...(Cn, Rn). To prevent modeling attacks, we propose a RBST-APUF that contains a challenge randomization module (CRM). The CRM randomize the input challenge (2^l where l is randomized level) so that the adversary does not know what sub-challenges are

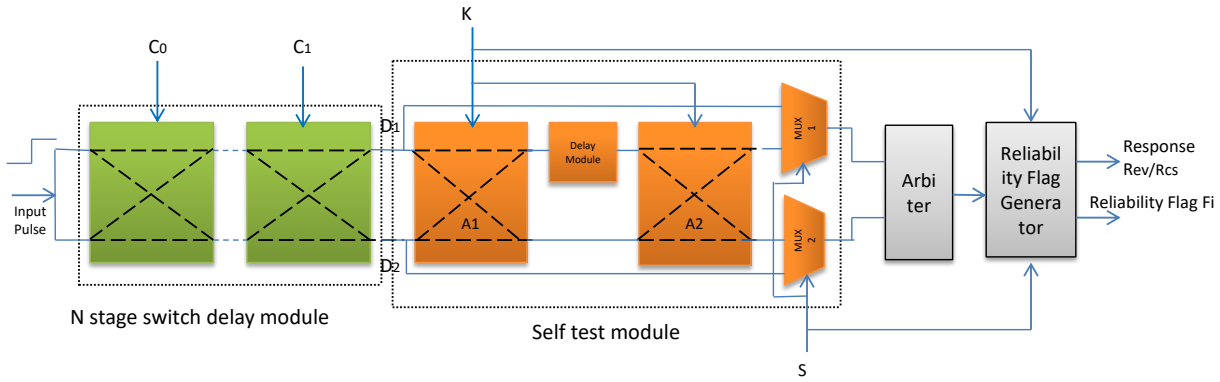

Fig. 3. Block diagram of RBST-APUF

input to the RBST-APUF to produce the perceived responses [30].

The challenge C (Ccs/Cev) is input to a proposed challenge randomization module. Taking the RBST-APUF with randomization level l=2 as an example, for response R (Rev, Rcs), the adversary knows the input challenge C but do not know the CR. There are four probability of CR: CR00, CR01, CR10, CR11.

For modeling an attack, the attacker may get the knowledge of the response, but they do not have an idea regarding the challenge, CR00, CR01, CR10, and CR11, corresponding to the response. Hence for a machine learning attack, obtaining an effective training set becomes a problem.

B. Error correction using reliability flag:

Due to environmental conditions like temperature, voltage, and aging factors, the responses of PUF are not unique for the same input. There were attempts to have error correction techniques such as fuzzy extractors, but they provided overhead of hardware complexity. To test the delay, a delay-detecting circuit is added to the traditional arbiter PUF [31]. PUFs generate output by amplifying electrical features within the same PUF, such as delay or threshold voltage. If the electrical difference generating each response can be checked automatically, the response with the greatest difference can be chosen for key generation, resulting in a more robust response. If the delay exceeds the threshold, the flag is set to 1; otherwise, it is set to 0. When a challenge (Cev or Ccs) is given as input to RBST-APUF, it generates a reliability flag (Fi) and response (Rev or Rcs) at the same time. If the flag is set to 1, the corresponding response bit is chosen; otherwise, it is discarded. As a result, we can use the reliability flag as helper data to extract or recover the keys [32].

C. Side channel attacks and countermeasure:

Side-channel attacks (SCA) represent a prevalent technique for obtaining sensitive information from the cryptographic components of a chip in the traditional realm. These security threats capitalize on weaknesses in the hardware employing rather than exploiting a weakness in the mathematical model of the algorithm [33]. The process of a side-channel attack unfolds in two stages. Initially, the physical leakage associated with every request conducted on the cryptographic application must be transformed into score vectors and probability. The complexity or noise level of the leaked data directly correlates with the difficulty of executing the SCA [34].

One form of SCA, known as differential power analysis (DFA), is a statistical attack that scrutinizes the measured power consumption derived from traces of the cryptographic algorithm's implementation. The attack traces consist of intermediate values manipulated to allow them to be expressed as a function of the secret key and a known value. To forecast power consumption, attackers often employ various models such as hamming weight or distance [22]. A comprehensive or combined attack strategy involves leveraging preprocessing techniques, with mutual information analysis and correlation power analysis being particularly effective in combination. These combined side-channel attacks demonstrate effectiveness, especially when targeting lightweight cryptography.

D. Hardware Overhead:

The hardware overhead of RBST-APUF is primarily due to the CRM as shown in Fig. 3. This module contains RNG, multiplexers, and inverters. Since RNG is commonly used, the CRM can directly use the existing RNG. Hence, the hardware overhead is mainly due to multiplexers and inverters, which are negligible [35].

V. sTRADE 2.0: SYSTEM MODEL FOR SECURITY

A. Network Model

V2G system contains three entities: EV, CS, and GS. The roles and duties of these entities are as follows:

- **Electric Vehicle**: An EV is a moving entity that reaches the nearest CS for charge or discharge. EV consists of an onboard unit (OBU) with a PUF device used during the registration and authentication. EVs have low computational resources.
- **Charging Station**: The CS is an aggregator point where various EVs connect to charge/discharge their batteries. Multiple CS may connect to GS. CS has low computational resources, while GS is highly resource-rich and storage entities.

- **Grid Server**: GS contains an extensive database and stores challenge-response pairs (CRP), the identity of EV and CS, etc. GS is considered a trusted third party that has all secret information.
  The EV does not communicate directly with the server. All participating nodes must be authenticated to achieve mutual authentication. Thus, authentication between EV and GS may be divided into two parts, i.e., mutual authentication between CS and GS and EV and CS. The GS is the only genuine authority and stores the CRP. Whenever any new EV wants to register on the network, The GS stores its CRP. For mutual authentication, GS sends challenge pairs to EV and CS. EV and CS generate a response pair using PUF and send it to the GS. The GS authenticates the CRP and allows for authentication. The proposed scheme provides secure and confidential energy trading between EVs and CS. GS receives the transaction message from CS. It should be able to verify that there is no tampering or alternation in messages.The symbols used in the proposed scheme are defined in Table II.

B. Threat Model

This paper considers the two popular adversary models, DY and CK, for security analysis. An intruder has the following capacity and can execute the following attacks.

- An adversary has the ability to manipulate insecure communication channels, allowing them to eavesdrop on, modify, alter, or block transmitted messages within the V2G network.
- An adversary can acquire secrets stored in non-volatile memory (NVM) through a side-channel attack.
- An adversary is capable of executing clone or physical attacks. The CK adversary model ensures that information leakage in one session does not compromise the security of subsequent sessions.
- The adversary cannot compromise GS as it is considered completely trustworthy.

VI. PROPOSED V2G SECURITY PROTOCOL

A. Registration Phase:

Initially, EV and CS must register with GS in the network, where registration occurs via a secure medium or offline mode. Fig. 4 depicts the proposed system model for V2G security.

1) EV Registration Phase:

Step 1: Each EV registers itself by sending its identity IDev to GS.

Step 2: After receiving identity IDev, GS generates challenge pair Cev, pseudo EV ID PIDev= (IDev$\|$Cev) and sends these towards EV.

Step 3: After receiving challenge Cev, EV generates response Rev=PUF(Cev) through PUF. Pseudo ID PIDev is stored at EV while CRPs are sent back, and GS stores these CRPs along with IDs in its database.

2) CS Registration Phase:

Step 1: Each CS registers itself by sending its identity IDcs to GS.

Step 2: GS sends challenge parameter Ccs toward GS for registration. After receiving the challenge parameter, CS generates the response Rcs =PUF(Ccs) and sends it toward GS. GS stores this CRP along with the PIDcs, and IDcs in its database.

TABLE II
LIST OF SYMBOLS

Symbols	Descriptions
h	Hash function
IDev, IDcs	ID of EV, CS
Tev, Tcs,Tgs	Time stamp EV, CS and GS
Rcs, Ccs	CS PUF CRP
$\oplus$	XOR operator
Rev, Cev	EV PUF CRP
K1,K2,K3,K4,D1,D2,D3,D4	Authentication Message
PIDev, PIDcs	Secret ID of EV and CS
SKev, SKcs	Session key of EV and CS
$\|$	Concatenation operator

B. Mutual Authentication Phase:

The mutual authentication phase has been completed in two steps.

1) CS-GS mutual authentication phase: After registration of EV and CS with GS, EV starts for charging/discharging.

Step 1: Initially, EV sends its pseudo-identity PIDev towards CS. CS calculates fresh time stamp Tcs and sends PIDcs and Tcs toward GS.

Step 2: GS checks freshness of Tcs, PIDcs in the database and calculates D1=h(Rcs$\|$Ccs$\|$PIDcs$\|$Tcs) and K1=(Ccs$\oplus$IDcs$\oplus$Tcs). After that, GS sends D1 and K1 toward CS.

Step 3: After receiving K1 the CS calculates challenge parameter Ccs=(K1$\oplus$IDcs$\oplus$Tcs) using K1 and the retrieved challenge Ccs generates Rcs=PUF(Ccs) response parameters. With the help of CRP, CS calculates $D1^*$=h(Rcs$\|$Ccs$\|$PIDcs$\|$Tcs). If D1 equals $D1^*$, it further calculates new challenge Rcs+1=PUF(Ccs+1); otherwise, it turns down the connection. Further, it calculates K2=(Rcs+1$\oplus$Rcs$\oplus$Tcs). Subsequently, it computes D2=h(Rcs+1$\|$Ccs+1$\|$PIDcs$\|$Tcs). Further, CS calculates the secret session key SKcs= kdf(Ccs+1$\|$Tcs$\|$Tgs).

Step 4: K2, D2 are transmitted toward GS. At the GS, new challenge parameters Ccs+1 and Rcs+1 are calculated. Further, $D2^*$=h(Rcs+1$\|$Ccs+1$\|$PIDcs$\|$Tcs) is calculated and is compared with received D2. If D2 is equal to $D2^*$, it is further processed, else ends the connection. Further, new PIDcs+1=PIDcs$\oplus$Ccs+1 and session key SKcs=kdf(Ccs+1$\|$Tcs$\|$Tgs) is generated for authentication. Lastly, new CRP (Ccs+1, Rcs+1) and new pseudo ID PIDcs+1 are saved in the GS database.

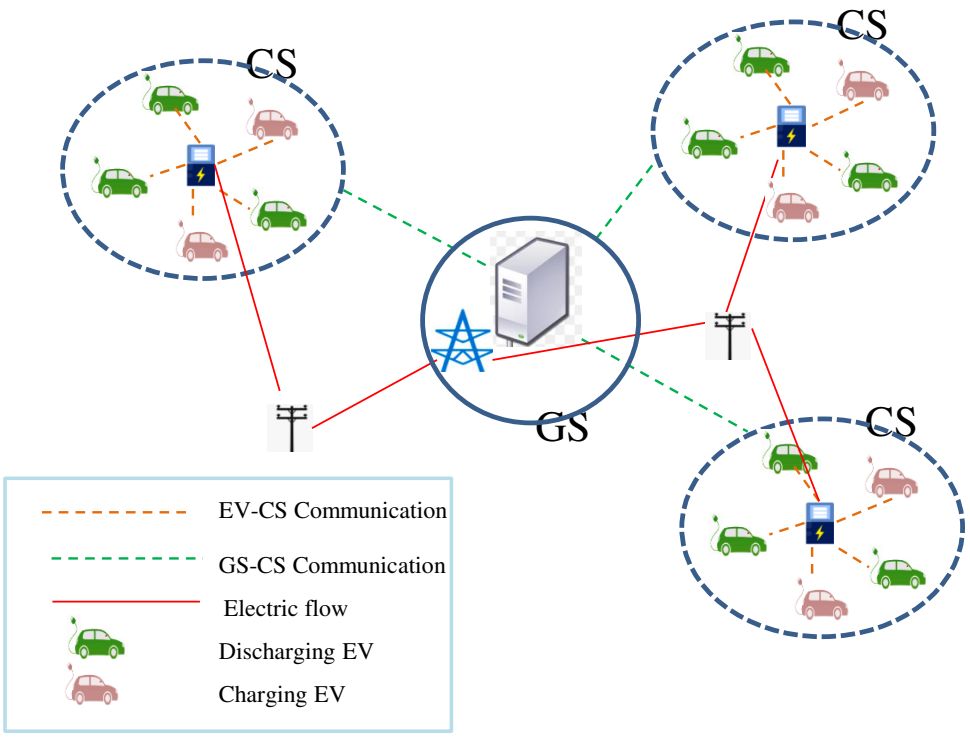

Fig. 4. System Model

2) EV-CS mutual authentication phase: After CS-GS authentication, EV-CS authentication starts.

Step 1: CS sends EV identity PIDev, Tev, towards GS.
Step 2: GS checks fresh time stamp Tev, retrieves CRP, encrypts with SKcs $(Cev, Rev)_{SKcs}$, and sends toward CS.
Step 3: CS decrypts CRP (Cev, Rev) and calculates D3=h(Rev‖Cev‖PIDev‖Tev). After it, CS sends D3 and challenges Cev towards EV.
Step 4: After receiving the challenge parameter Rev from CS, EV generates Rev=PUF(Cev) response parameters. EV calculates $D3^*$=h(Rev‖Cev‖PIDev‖Tev). If D3 equals $D3^*$, it calculates Rev+1=PUF(Cev+1); otherwise, it tears down the connection. Further it calculates K4=(Rev+1⊕Rev⊕Tev) and subsequently, it computes D4=h(Rev+1‖Cev+1‖PIDev‖Tev). Further, $D4^*$=h(Rev+1‖Cev+1‖IDev‖TSev) is calculated and compared with received D4. If D4 equals $D4^*$, it further processes; otherwise, it finishes the connection. Further, SKev=kdf(Cev+1‖Tev‖Tcs) session key is generated for authentication.
Step 5: K4, D4 transmitted toward CS. At the CS new CRP Cev+1 and Rev+1 and PIDev+1=PIDev⊕Cev+1 are calculated and transmitted toward GS after encryption E(Cev+1,Rev+1,PIDev+1)SKcs. After decryption, Cev+1, Rev+1 and PIDev+1 are saved at GS. The PIDev+1 value changes in each session as the value of Cev+1 changes.

C. Dynamic CS and EV addition Phase

A new EV or CS may join the V2G network during this phase by sending a registration request to GS. All registered EV will get information about new CS. Above discussed authentication phases are depict in Fig. 5.

VII. Security Analysis and Comparison

The formal security of the proposed protocol is assessed using the ROR oracle model and the automated security verification tool AVISPA. Additionally, informal security is analyzed by employing the DY and CK models under different attack scenarios. Table III compares diverse security aspects among various well-known schemes.

A. Formal verification using Random or Real oracle model

Formal security verification is based on the ROR model, which measures protocol security by evaluating the probability of SK cracking on the repeated game round in V2G. The proposed ROR model assumes that the adversary $\mathcal{A}$ can interact with other communicating entity B = (EV, CS, GS), here $\prod_{E_i}^{x}$,$\prod_{C_j}^{y}$, $\prod_{S_k}^{z}$ can perform the following queries:
• Send(B, M): In this query, $\mathcal{A}$ can send message M to B in V2G and receives a response from a specific entity.
• Execution(B): $\mathcal{A}$ Utilizing this query, an attacker can initiate a passive attack within the V2G system. $\prod_{E_i}^{x}$, $\prod_{C_j}^{y}$ and $\prod_{S_k}^{z}$.
• Reveal(B): $\mathcal{A}$ can get the session key SK of $\prod_{S_k}^{z}$ and $\prod_{C_j}^{y}$ by executing this query.
• Corrupt(B): If this query is executed, it will get long-term session key SK in V2G.

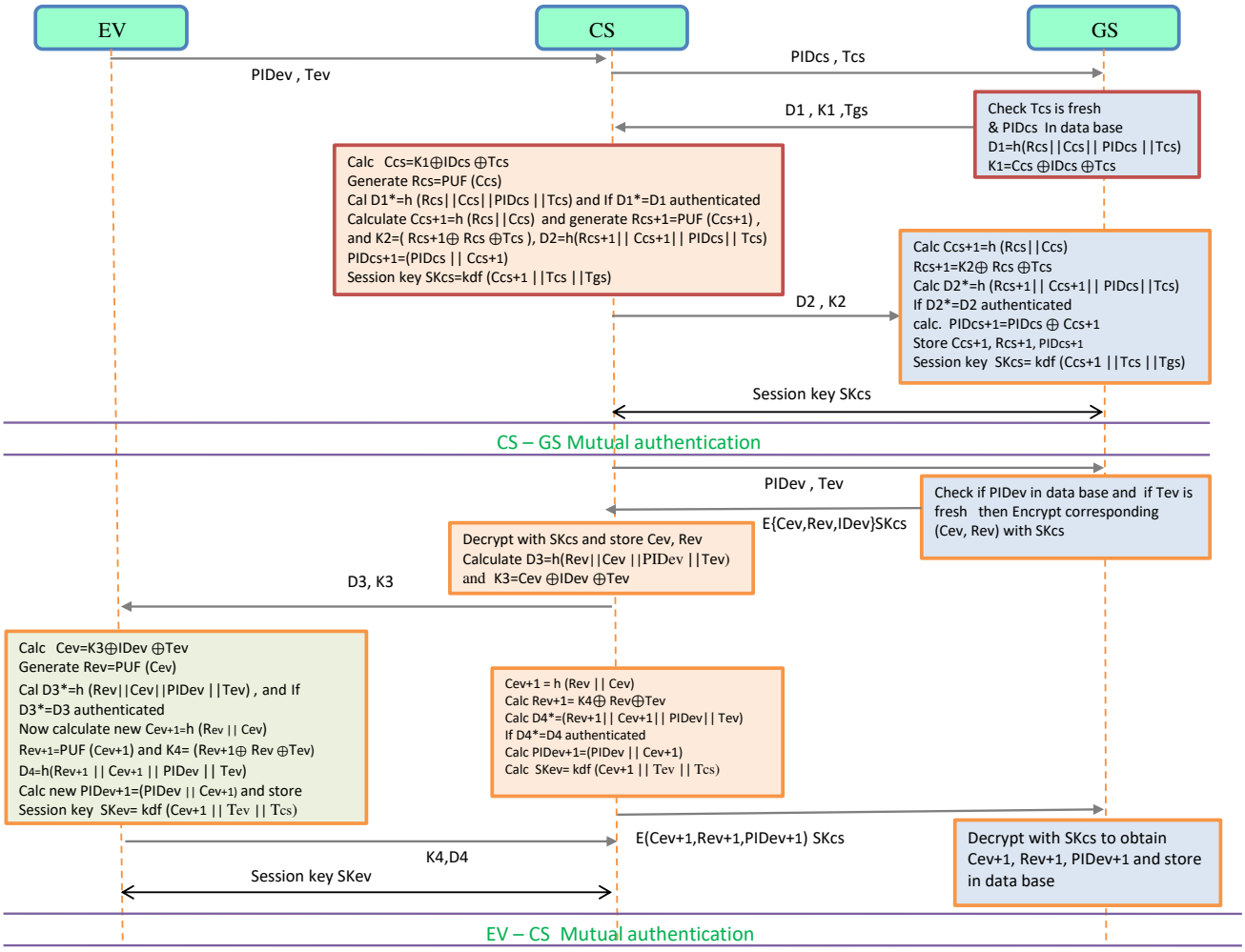

Fig. 5. Mutual Authentication

TABLE III
COMPARISON OF SECURITY FEATURES

Scheme /Attacks	MiTM attack	DOS attack	Forward secrecy	Anonymity	Replay attack	Modeling attack
Kaveh, et al. 2020 [9]	YES	YES	YES	NO	NO	NO
G.Sharma, et al. 2021 [10]	NO	YES	YES	NO	YES	NO
Jiang, et al. 2022 [12]	YES	YES	NO	YES	YES	NO
Reddy, et al. 2023 [13]	YES	YES	YES	YES	YES	YES
Our scheme(sTrade 2.0)	YES	YES	YES	YES	YES	YES

• Test(B): $\mathcal{A}$ has the capability to send a query to any participant within the V2G system, and it tosses up a coin. If C=1 $\mathcal{A}$, obtain the correct secret key. When C equals 0, a randomly chosen value with the same bit string as SK is returned..

Theorem 1: Assuming that $\mathcal{A}$ is an actively running polynomial-time adversary and conducts queries, the probability that $\mathcal{A}$ can compromise the protocol is

$$Adv_{\mathcal{P}}^{SK}(\mathcal{A}) \leq \frac{q_s}{2^{l-2}} + \frac{3q_h^2}{2^l} + 2max\{C^{'}.q_s^{'}, \frac{q_s}{2^l}\}$$

where q_s and q_h denote the number of send and hash queries respectively, l represents the number of bits, and C' is a constant.

Proof: We illustrate the proof of the theorem using seven game rounds, denoted as $G_m = \{0, 1, 2, 3, 4, 5, 6\}$. $Succ_P^{G_m}$ represents the probability of winning in different rounds of the game, and $Adv_{\mathcal{P}}^{SK}$ denotes the advantage of breaking the protocol.

• **Game$_0$** : In the first round of game G_0 does not make any query. The probability of $\mathcal{A}$ successfully cracking is:

$$Adv_{\mathcal{P}}^{SK}(\mathcal{A}) = 2\Pr\left[Succ_P^{G0}\right] - 1. \quad (1)$$

• **Game$_1$** :In this particular round, $Game_1$ performs Execute (B) operation.$\mathcal{A}$ intercepts only message D1,D2,D3,D4 are transmitted over insecure communication channel. Since the value of Ccs and Cev are unknown $\mathcal{A}$ During this round, it

cannot compute the secret session keys SKcs and SKev. Hence probability of $Game_1$ is same as $Game_0$.

$$|\Pr\left[Succ_P^{G1}\right] = \Pr\left[Succ_P^{G0}\right] \quad (2)$$

• **Game$_2$** : In this particular round, $Game_2$ performs Send (B) operation other than $Game_1$. As per Zipf's law probability of $Game_2$ is

$$|\Pr\left[Succ_P^{G2}\right] - \Pr\left[Succ_P^{G1}\right]| \leq \frac{q_s}{2^l} \quad (3)$$

• **Game$_3$** : In this particular round, $Game_3$ executes one additional Hash(B) operation and one fewer Send(B) operation. The probability of collusion occurring during the hash query simulation, as per the birthday paradox, is

$$|\Pr\left[Succ_P^{G3}\right] - \Pr\left[Succ_P^{G2}\right]| \leq \frac{q_h^2}{2^{l+1}} \quad (4)$$

• **Game$_4$** : In this game $\mathcal{A}$ uses $\prod_{S_k}^{z}$ to acquire the GS challenge Ccs or $\prod_{S_k}^{z}$ and $\prod_{C_j}^{y}$ to obtain private value used during registration. Assume that $\mathcal{A}$ acquire the GS challenge Ccs. Because A can not calculate the value of Ccs+1, it can not calculate the SK, where SKev=kdf(Cev+1||TSev||TSev). Therefore the probability of $Game_4$ is

$$|\Pr\left[Succ_P^{G4}\right] - \Pr\left[Succ_P^{G3}\right]| \leq \frac{q_s}{2^l} + \frac{q_h^2}{2^{l+1}} \quad (5)$$

• **Game$_5$** : $\mathcal{A}$ uses Corrupt (B) to capture the parameters in CS (Cev+1,Rev,TSev). Therefore the probability of $Game_5$ is

$$|\Pr\left[Succ_P^{G5}\right] - \Pr\left[Succ_P^{G4}\right]| \leq max\{C^{'}.q_s^{'}, \frac{q_s}{2^l}\} \quad (6)$$

• **Game$_6$** : In this game, $\mathcal{A}$ has the capability to guess the session keys SKcs and SKev. It is important to note that the session key remains independent of the hash oracle and other parameters. Hence the probability of $Game_6$ is

$$|\Pr\left[Succ_P^{G6}\right] - \Pr\left[Succ_P^{G5}\right]| \leq \frac{q_h^2}{2^{l+1}} \quad (7)$$

Hence the probability that $\mathcal{A}$ can guess is

$$|\Pr\left[Succ_P^{G6}\right]| = \frac{1}{2} \quad (8)$$

Based on equations (1) -(8), we got (10), which proves the theorem.

$$Adv_{\mathcal{P}}^{SK}(\mathcal{A}) \leq \frac{q_s}{2^{l-2}} + \frac{3q_h^2}{2^l} + 2max\{C^{'}.q_s^{'}, \frac{q_s}{2^l}\} \quad (10)$$

B. Formal security verification using AVISPA Tool

We formally verify the security protocol of the proposed protocol using the popular push button AVISPA simulation tool. It is a suite of applications for validating security attacks [36]. This tool uses role-based HLPSL, where the role of each entity (EV, CS, and GS) is defined. Fig. 6 depicts the EV HLPSL code. AVISPA employs two widely used backends for executing the program: OFMC (On-the-Fly Mode Checker) and Cl-AtSe (Constraint-Logic-based Attack Searcher). It uses the DY model as the intruder model.

Fig. 7 depicts the protocol simulation result, where version means suite version, summary means safe or unsafe, details

```
role role_EV
(EV:agent,CS:agent,GS:agent,H,PUF:hash_func,SKev:symmetric_key,SND,RCV:channel
(dy))
played_by EV
def=
        local
                State:nat,

TSev,TScs,Rev,Cev,D3,D33,IDev,Cevn,Revn,A4,D4,PIDev,PIDevn,Rcs,Rcsn:text,

                Kab:symmetric_key

        init
                State := 0
        transition
                1. State=0 /\ RCV(start) =|>
                        State':=1 /\ TSev':= new() /\ Cev':=new() /\
IDev':=new() /\  secret(SKev,sec_1,{EV,CS,GS}) /\ D3':=H(Rev.Cev.IDev)
/\SND(D3,Cev,TSev)
                2. State=1 /\   RCV(D3,Cev,TSev)  =|>
                        State':=2   /\ D33':=H(Rev.Cev.IDev)/\ Cevn':=H
(Rev.Cev) /\ Rev':=PUF(Cev)/\ Revn':=PUF(Cevn) /\ TSev':= new()/\ A4':=xor
(Revn,Rev,TSev) /\ TScs':= new()/\ D4':=H(Revn,Cevn,IDev,TScs) /\
PIDevn':=xor(PIDev,Rev) /\ SKev':=H(Cevn.TSev.TScs)  /\ SND(A4,D4,PIDevn)
```

Fig. 6. EV HLPSL Code

about several sessions, and protocol means your program, goal, and backend. The statistics show time consumed in different sections. The results in the protocol simulation and the intruder attacks section show that our protocol is safe against various attacks.

% OFMC % Version of 2006/02/13 SUMMARY SAFE DETAILS BOUNDED_NUMBER_OF_SESSION S PROTOCOL /home/span/span/testsuite/results /smartgrid.if GOAL as specified BACKEND OFMC COMMENTS STATISTICS parse time:0.00sec search Time:0.53sec visitedNodes:457 Nodes	SUMMARY SAFE DETAILS BOUNDED_NUMBER_OF_SESSI ONS PROTOCOL /home/span/span/testsuite/res ults/smartgrid.if GOAL as specified BACKEND CL-AtSe STATISTICS Analysed: 0 states Reachable: 0 states Translation: 0.19 seconds Computation: 0.00 seconds

Fig. 7. Simulation Result for OFMC and CL-Atse backend

C. Informal Security Analysis

This subsection conducts an analysis of various security threats using informal security analysis, a widely employed method to showcase the cryptographic protocol's capabilities. The protocol demonstrates resilience against various attacks, including replay, impersonation, and man-in-the-middle attacks.

Preposition 1:The proposed scheme can mitigate man-in-middle attacks.

Proof:- An adversary $\mathcal{A}$ may insert itself between the communication of an EV and CS or GS and gain control of the communication between them. Assume that $\mathcal{A}$ intercepts the relayed messages on the communication channel and attempts to manipulate the intermediate messages (D1, K2,

D2) or (D3, K4, D4), posing as a legitimate entity in front of the others. However, this is not possible until the $\mathcal{A}$ gets the response (Rcs or Rev) of the EV/CS. Without knowledge of Rcs, the adversary can not calculate D1 and D2. Similarly, without knowledge, Cev's adversary can not calculate D3, D4, and K4. Further, if D1, D2 is not equal to D1*, D2*(modified) authentication is terminated. Thus, the $\mathcal{A}$ cannot execute the MiTM attack under the considered situations.

Preposition 2: The proposed scheme is resilience against replay attack.

Proof:- In this attack $\mathcal{A}$ repeat the message already sent such as D3=h (Rev|| Cev|| IDev). As Tcs, Tev, and Tgs, PIDev changes in each session hence the adversary can not reuse message D3 in each session, as a new challenge message is generated.

Preposition 3: The proposed protocol ensures message integrity.

Proof:- EV and CS generate a fresh session key for each session. CS and EV produce fresh (Rev and Cev) and timestamps (TSev, TScs). The CRP verifies the integrity and authenticity of the transmitted message data.

Preposition 4: The proposed protocol can mitigate DoS attacks.

Proof:- In this type of attack, an adversary could inundate the network by sending undesired and fake packets to all protocol entities. In our proposed scheme, each entity promptly validates received packets, distinguishing them from bogus ones, and verifies the freshness of the timestamp. Both the EV and CS generate a new session key for each session. CS and EV generate fresh values (Rev and Cev) and new timestamps (TSev, TScs), effectively safeguarding against DOS attacks.

Preposition 5: The proposed protocol is resilient against backward and forward key secrecy.

Proof:- Only a legitimate EV can generate Cev+1, hence calculating fresh SKev=kdf(Cev+1|| Tev|| Tcs). Similarly, legitimate CS can generate fresh SKcs=kdf(Ccs+1|| Tgs|| Tcs). If any session key is compromised, the security design ensures that the compromise does not aid in recovering past or future session keys. Therefore, the system provides session key security against any form of attack.

VIII. Comparative Performance Assessment

In this section, we compare our protocol with other existing state-of-art schemes.

A. Computational overhead analysis

This subsection compares and analyzes the proposed scheme's computational cost with popular schemes such as [9], [10], [12], [13]. GS is a resource-rich entity and, hence, is not taken for computational cost analysis. The simulation was performed on a 32-bit operating system with intel core i5, a 2.60 GHz CPU for EV, and a 64-bit core i7, 2.60 GHz CPU with 6 GB RAM for CS. It is assumed that CS has a higher operating capacity than EV. Table IV depicts the execution time involved in different cryptographic operations like multiplication (Tm), encryption and decryption (Ted), a one-way hash (Th), MAC operation (Tmac), PUF operation (Tpuf), respectively.

TABLE IV
Execution time of different cryptographic operation

Cryptographic operation	EV Time (μs)	CS Time (μs)
Hash (Th)	39.2	11.1
HMAC (Tmac)	119.3	33.8
PUF (Tpuf)	160.7	135
Addition (Tadd)	790	216
Xor(Txor)	125.3	104.7
Random Number (Trng)	82.3	31.5
Encryption (Te)	199.6	41.8
Decryption (Td)	309	64.5
Fst (TFst)	191	39.1

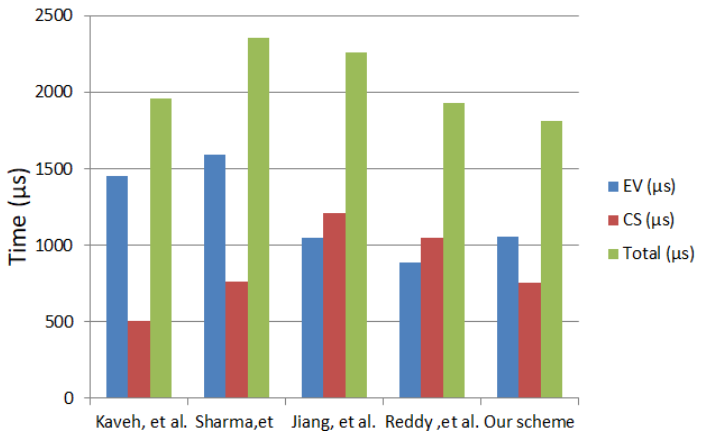

Fig. 8. Computational overhead analysis at EV and CS

Based on the above analysis, the total computational cost (8Txor+12Th+4Tpuf) involved in sTrade 2.0 is 1810.6μs. Similarly [9] uses 1960.8μs, while [10] consumes 2356.6μs and [12] uses 2259.2μs overhead. A detailed comparison is depicted in Table V and Fig. 8. The above comparison shows that the computation cost in sTrade 2.0 is the least.

B. Communicational overhead analysis

In this subsection, we have compared the communicational overhead of the proposed scheme with other popular schemes such as [9], [10], [12] and [13]. The comparisons of different schemes are based on messages transmitted and received during the authentication process. For instance, the size used in timestamp = 4byte(B), hash values =16B, pseudo-random numbers ID =8B, and key size =16B is considered. Scheme [9] consumes 360B overhead, while [10] takes 320B. Similarly [12] transmit total overhead 388B while [13] send 272B. In the proposed scheme, the overhead transmitted between EV-GS is 88B, while CS-GS is 76B. The total overhead of 164B is much less than that of other schemes. Fig. 9 depicts the detailed comparison.

C. Discussion

The paper proposes suitable authentication scheme for the V2G network. We have used PUF for hardware security, where

TABLE V
CRYPTOGRAPHER OPERATION AND COMPUTATIONAL COST

Schemes	Electric Vehicle	Charging Station	Computational Overhead Time (μs)	Communicational Overhead (Byte)
Kaveh, et al. 2020 [9]	8Th+4Tpuf+4Txor	8Th+4Txor	1960.8	360
Sharma, et al. 2021 [10]	6Th+2Tpuf+1Tadd+2Txor	6Th+2Tpuf+1Tadd+2Txor	2356.6	320
Jiang, et al. 2022 [12]	4Th+4Tpuf+2Txor	4Th+4Tpuf+6Txor	2259.2	388
Reddy, et al. 2023 [13]	8Th+2Tpuf+2Txor	8Th+4Tpuf+4Txor	1933.2	272
Our scheme	4Txor+6Th+2Tpuf	4Txor+6Th+2Tpuf	1810.6	164

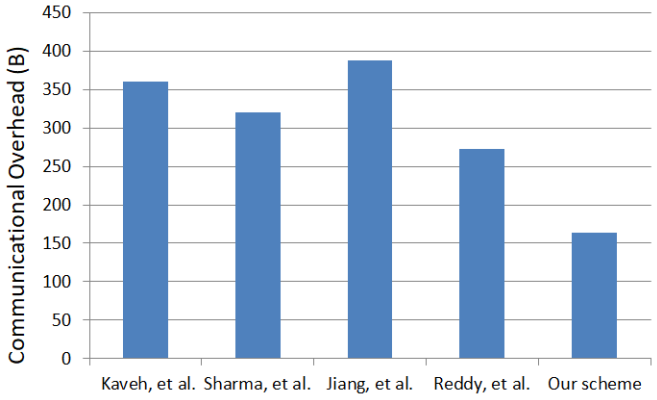

Fig. 9. Communicational overhead analysis

PUF tends to be vulnerable towards temperature variation and ageing [37]. To mitigate these challenges, we propose a RBST-APUF, which generates a flag bit to identify a weak response. Further reliability of PUF may be tested using different test beds. Further, we extend our findings from our previous research using a reliable RBST-PUF and provable security scheme ROR model, and the DY model. The obtained results are further compared with other state-of-the-art methods. Notably, our proposed model demonstrates superior performance in terms of computational overheads and robustness when compared to other related works.

Another popular simulation tool for hardware security verification is hardware-in-the-loop (HIL). It is a technique where real signals from a controller are connected to a test system in the assembled product [38].

IX. CONCLUSION

In V2G networks, electric energy consumption and data information are normally transmitted over public channels. It is revealed that most V2G authentication schemes either have a larger overhead or suffer from security requirements. Hence, we designed a lightweight authentication scheme, sTrade 2.0, based on a physical unclonable function, XOR, and hash function. In addition, the protocol's security was assessed through informal and formal analysis using the ROR model and AVISPA simulation tool. The designed protocol preserves EV location privacy and protects it from popular attacks like denial of service, MiTM, and replay attacks. Furthermore, computational and communicational overhead analysis shows that our protocol is lightweight compared to other popular schemes. The proposed RBST-APUF can withstand modelling and physical attacks, which supports error correction techniques without additional hardware. The designed protocol also supports the dynamic addition of CS and EV.

For future scope, V2V, G2V, and G2G auction-based energy trading could be proposed. The privacy issues of V2G and EV may be proposed for a more reliable V2G framework. Further, the trusted platform module (TPM) and PUF may be integrated to have the advantages of both devices for smart grid security.

REFERENCES

[1] A. Mehrabi and K. Kim, "Low-complexity charging/discharging scheduling for electric vehicles at home and common lots for smart households prosumers," *IEEE Trans. Consum. Electron.*, vol. 64, no. 3, pp. 348–355, 2018.

[2] H. Jain, M. Kumar, and A. Joshi, "Intelligent energy cyber physical systems (iECPS) for reliable smart grid against energy theft and false data injection," *Electrical Engineering*, pp. 1–16, 2021.

[3] V. C. Patil and S. Kundu, "Realizing robust, lightweight strong PUFs for securing smart grids," *IEEE Trans. Consum. Electron.*, vol. 68, no. 1, pp. 5–13, 2022.

[4] V. Hassija, V. Chamola, S. Garg, D. N. G. Krishna, G. Kaddoum, and D. N. K. Jayakody, "A blockchain-based framework for lightweight data sharing and energy trading in V2G network," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5799–5812, 2020.

[5] G. Sharma, A. M. Joshi, and S. P. Mohanty, "sTrade: blockchain based secure energy trading using vehicle-to-grid mutual authentication in smart transportation," *Sustainable Energy Technologies and Assessments*, vol. 57, p. 103296, 2023.

[6] M. Inci, M. M. Savrun, and Ö. Çelik, "Integrating electric vehicles as virtual power plants: A comprehensive review on vehicle-to-grid (V2G) concepts, interface topologies, marketing and future prospects," *Journal of Energy Storage*, vol. 55, p. 105579, 2022.

[7] G. Sharma, A. M. Joshi, and S. P. Mohanty, "Fortified-Grid 3.0: security by design for smart grid through hardware security primitives," in *2023 IEEE International Symposium on Smart Electronic Systems (iSES)*. IEEE, 2023, pp. 421–425.

[8] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani, "Lightweight mutual authentication protocol for V2G using physical unclonable function," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7234–7246, 2020.

[9] M. Kaveh, D. Martín, and M. R. Mosavi, "A lightweight authentication scheme for V2G communications: A PUF-based approach ensuring cyber/physical security and identity/location privacy," *MDPI Electronics*, vol. 9, no. 9, p. 1479, 2020.

[10] G. Sharma, A. M. Joshi, and S. P. Mohanty, "An efficient physically unclonable function based authentication scheme for V2G network," in *Proc. IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS)*, 2021, pp. 421–425.

[11] R. Das, G. Karmakar, J. Kamruzzaman, and A. Chowdhury, "Measuring trustworthiness of smart meters leveraging household energy consumption profile," *IEEE J. Emerging Sel. Top. Ind. Electron.*, vol. 3, no. 2, pp. 289–297, 2022.

[12] Z. Jiang, Z. Zhou, L. Xiong, and L. Zhou, "An efficient lightweight anonymous authentication scheme for V2G using physical unclonable function," in *Proc. IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*. IEEE, 2021, pp. 1–5.

[13] A. G. Reddy, P. R. Babu, V. Odelu, L. Wang, and S. A. Kumar, "V2G-Auth: lightweight authentication and key agreement protocol for V2G environment leveraging physically unclonable functions," *IEEE Trans. Ind. Cyber-Phys. Syst.*, 2023.

[14] W. Kempton and J. Tomić, "Vehicle-to-grid power fundamentals: Calculating capacity and net revenue," *Journal of power sources*, vol. 144, no. 1, pp. 268–279, 2005.

[15] Y.-N. Cao, Y. Wang, Y. Ding, H. Zheng, Z. Guan, and H. Wang, "A PUF-based lightweight authenticated metering data collection scheme with privacy protection in smart grid," in *Proc. IEEE Intl. Conf on Parallel Distributed Processing with Applications, Social Computing Networking (ISPA/BDCloud/SocialCom/SustainCom)*, 2021, pp. 876–883.

[16] P. Gope and B. Sikdar, "An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication," *EEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6607–6618, 2019.

[17] P. Gope, O. Millwood, and B. Sikdar, "A scalable protocol level approach to prevent machine learning attacks on physically unclonable function based authentication mechanisms for internet of medical things," *IEEE Trans. Ind. Inf.*, vol. 18, no. 3, pp. 1971–1980, 2021.

[18] C. Sabillón Antúnez, J. F. Franco, M. J. Rider, and R. Romero, "A new methodology for the optimal charging coordination of electric vehicles considering vehicle-to-grid technology," *IEEE Trans. on Sustainable Energy*, vol. 7, no. 2, pp. 596–607, 2016.

[19] A. Sarker, A. C. Canto, M. M. Kermani, and R. Azarderakhsh, "Error detection architectures for hardware/software co-design approaches of number-theoretic transform," *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, 2022.

[20] A. Sarker, M. M. Kermani, and R. Azarderakhsh, "Efficient error detection architectures for postquantum signature falcon's sampler and kem saber," *IEEE Trans. Very Large Scale Integr. VLSI Syst.*, vol. 30, no. 6, pp. 794–802, 2022.

[21] J. Yan, F. Guo, and C. Wen, "Attack detection and isolation for distributed load shedding algorithm in microgrid systems," *IEEE J. Emerging Sel. Top. Ind. Electron.*, vol. 1, no. 1, pp. 102–110, 2020.

[22] J. Kaur, A. C. Canto, M. M. Kermani, and R. Azarderakhsh, "A comprehensive survey on the implementations, attacks, and countermeasures of the current NIST lightweight cryptography standard," *arXiv preprint arXiv:2304.06222*, 2023.

[23] S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUF chain: A hardware-assisted blockchain for sustainable simultaneous device and data security in the internet of everything (IoE)," *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 8–16, 2020.

[24] M. Tahavori and F. Moazami, "Lightweight and secure PUF-based authenticated key agreement scheme for smart grid," *Peer-to-Peer Networking and Applications*, vol. 13, no. 5, pp. 1616–1628, 2020.

[25] L. P. Qian, Y. Wu, X. Xu, B. Ji, Z. Shi, and W. Jia, "Distributed charging-record management for electric vehicle networks via blockchain," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2150–2162, 2020.

[26] M. Liu, Z. Zhang, P. Ge, R. Deng, M. Sun, J. Chen, and F. Teng, "Enhancing cyber-resiliency of DER-based smartgrid: A survey," *arXiv preprint arXiv:2305.05338*, 2023.

[27] H. Ma, C. Wang, G. Xu, Q. Cao, G. Xu, and L. Duan, "Anonymous authentication protocol based on physical unclonable function and elliptic curve cryptography for smart grid," *IEEE Syst. J.*, 2023.

[28] P. K. Jena, E. Koley, and S. Ghosh, "An optimal scheme for installation of pmus and ieds to reinforce electricity market immunity against data attacks in smart grid," *IEEE J. Emerging Sel. Top. Ind. Electron.*, vol. 4, no. 2, pp. 603–613, 2022.

[29] G. Sharma, A. M. Joshi, and S. P. Mohanty, "Fortified-Grid: fortifying smart grids through the integration of the trusted platform module in Internet of Things devices," *Information, MDPI*, vol. 14, no. 9, p. 491, 2023.

[30] J. Ye, Y. Hu, and X. Li, "RPUF: physical unclonable function with randomized challenge to resist modeling attack," in *2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)*. IEEE, 2016, pp. 1–6.

[31] Z. He, W. Chen, L. Zhang, G. Chi, Q. Gao, and L. Harn, "A highly reliable arbiter PUF with improved uniqueness in FPGA implementation using bit-self-test," *IEEE Access*, vol. 8, pp. 181 751–181 762, 2020.

[32] A. Jain and A. M. Joshi, "Device authentication in IoT using reconfigurable PUF," in *Proc. 2nd IEEE Middle East and North Africa COMMunications Conference (MENACOMM)*, 2019, pp. 1–4.

[33] S. Seçkiner and S. Köse, "Combined side-channel attacks on a lightweight prince cipher implementation," in *Proc. IEEE 34th International System-on-Chip Conference (SOCC)*, 2021, pp. 260–265.

[34] S. Chowdhury, A. Covic, R. Y. Acharya, S. Dupee, F. Ganji, and D. Forte, "Physical security in the post-quantum era: A survey on side-channel analysis, random number generators, and physically unclonable functions," *J. Cryptogr. Eng.*, pp. 1–37, 2021.

[35] S. K. Agarwal and A. M. Joshi, "Device authentication with FPGA based self correcting physical unclonable function for internet of things," *Microprocessors and Microsystems*, vol. 95, p. 104717, 2022.

[36] K. Mahmood, S. Shamshad, M. Rana, A. Shafiq, S. Ahmad, M. A. Akram, and R. Amin, "PUF enable lightweight key-exchange and mutual authentication protocol for multi-server based D2D communication," *J. Inf. Secur. Appl.*, vol. 61, p. 102900, 2021.

[37] D. Das, C. Kumar, and M. Liserre, "Stabilization of smart transformer based islanded meshed hybrid microgrid during electric vehicle charging transients," *IEEE J. Emerging Sel. Top. Ind. Electron.*, vol. 4, no. 4, pp. 1255–1264, 2023.

[38] M. Liu, C. Zhao, Z. Zhang, R. Deng, P. Cheng, and J. Chen, "Converter-based moving target defense against deception attacks in dc microgrids," *IEEE Trans. on Smart Grid*, vol. 13, no. 5, pp. 3984–3996, 2021.

Giriraj sahrma (GS'00) received his BE degree in Electrical Engineering from MBM University, Jodhpur, India in 2000 and his Master's degree from Mewar University. He is a Research Scholar at the ECE department of MNIT, Jaipur. His current research interests include Smart grid ,communication and cyber-physical securities. He worked a Divisional Engineer in BSNL(A Govt of India PSU). He is the author of 4 conferences and 3 journal papers.

Amit M. Joshi (SM'21) completed his M.Tech and Ph.D. from NIT, Surat in 2009 and 2015, respectively. He is currently working as an Associate Professor at Malaviya National Institute of Technology, Jaipur (MNIT Jaipur) since July 2013. His specialisation areas are Biomedical signal processing, Smart healthcare, VLSI DSP Systems, and embedded system design. He is a senior member of IEEE and an associate member of IETE. He has also published around 125+ research articles in excellent peer-reviewed international journals/conferences and has also filed three patents. He has a total of 1624 Google Scholar citations, i10 index 46, H-index of 21. Also, he served as a Technical Programme Committee member for IEEE conferences (iSES, ICCE, ISVLSI, VDAT). He also received the honour of UGC Travel fellowship, SERB DST Travel grant award, and CSIR fellowship. Also, He has also served as a Mentor for the IEEE Engineering in Medicine and Biology Society student mentorship program

Saraju P. Mohanty (Senior Member, IEEE) received the bachelor's degree (Honors) in electrical engineering from the Orissa University of Agriculture and Technology, Bhubaneswar, in 1995, the master's degree in Systems Science and Automation from the Indian Institute of Science, Bengaluru, in 1999, and the Ph.D. degree in Computer Science and Engineering from the University of South Florida, Tampa, in 2003. He is a Professor with the University of North Texas. His research is in "Smart Electronic Systems" which has been funded by National Science Foundations (NSF), Semiconductor Research Corporation (SRC), U.S. Air Force, IUSSTF, and Mission Innovation. He has authored 500 research articles, 5 books, and invented 10 granted/pending patents. His Google Scholar h-index is 56 and i10-index is 239 with 13,000 citations. He is a recipient of 18 best paper awards, Fulbright Specialist Award in 2021, IEEE Consumer Electronics Society Outstanding Service Award in 2020, the IEEE-CS-TCVLSI Distinguished Leadership Award in 2018, and the PROSE Award for Best Textbook in Physical Sciences and Mathematics category in 2016. He has delivered 24 keynotes and served on 14 panels at various International Conferences. He has been the Editor-in-Chief of the IEEE Consumer Electronics Magazine during 2016-2021 and currently serves on the editorial board of 8 journals/transactions. He has mentored 3 post-doctoral researchers, and supervised 15 Ph.D. dissertations, 26 M.S. theses, and 20 undergraduate projects.