

A. Alshaeri and M. Younis, "A Blockchain-based Energy Trading Scheme for Dynamic Charging of Electric Vehicles," *2021 IEEE Global Communications Conference (GLOBECOM)*, 2021, pp. 01-06, doi: 10.1109/GLOBECOM46510.2021.9685296.

<https://doi.org/10.1109/GLOBECOM46510.2021.9685296>

© 2021 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Access to this work was provided by the University of Maryland, Baltimore County (UMBC) ScholarWorks@UMBC digital repository on the Maryland Shared Open Access (MD-SOAR) platform.

Please provide feedback

Please support the ScholarWorks@UMBC repository by emailing scholarworks-group@umbc.edu and telling us what having access to this work means to you and why it's important to you. Thank you.

A Blockchain-based Energy Trading Scheme for Dynamic Charging of Electric Vehicles

Abdulaziz Alshaeri and Mohamed Younis
Department of Computer Science and Electrical Engineering
University of Maryland, Baltimore County
Baltimore, USA
zo40379, younis@umbc.edu

Abstract—Dynamic charging is a promising technology for Electric Vehicles (EVs) since it allows EVs to replenish its energy supply while on the move. The popular technology for such dynamic recharging utilizes magnetic induction by placing a large number of special charging pads on the roads that EVs pass over while traveling. Unlike the traditional stationary systems, dynamic charging introduces several challenges in how to handle billing, conduct EV authentication, and sustain privacy. The main issue is attributed to the high motion speed of EVs which allows a very short contact time between the resource constrained charging pads and the EVs. Therefore, we propose a lightweight and fast authentication protocol for EV-to-charging-pads; the protocol is incorporated in an energy trading scheme for the dynamic charging of EVs that is based on blockchain technology. We utilize Physically Unclonable Function (PUF) in the creation of a charging ticket in order to prevent double-spending of the ticket without incurring additional overhead. Furthermore, we leverage pseudonyms to preserve the privacy of EVs. Our analysis demonstrates that the proposed protocol is secure and allows a charging pad to authenticate EV in less than 13 μ sec.

Keywords—Electric Vehicles (EVs), Dynamic Charging, Energy Trading, Authentication, PUFs, Blockchain

I. INTRODUCTION

Electric Vehicles (EVs) have emerged as an effective means for transportation that can save our planet by reducing pollution attributed to vehicles' emissions. In the US, a single EV produces annually an average of 3,774 pounds of CO₂ equivalent compared to 11,435 pounds produced by the conventional gasoline-operated vehicle [1]. Furthermore, the average cost to fuel a vehicle with a regular-grade gasoline in the US is \$2.85 while the cost of an electric eGallon is \$1.16 [2]. Therefore, EVs have gained an increasing popularity. Charging of EVs have become more convenient either using any of the thousands deployed charger stations or even at home. However, the hours-long time needed to fully charge an EV battery causes inconvenience for vehicle owners. As a result, dynamic charging has emerged as a promising technology that can avoid the need of getting a vehicle off-service to replenish energy supply.

To charge an EV during motion logistically requires infrastructure support. One of the popular techniques for dynamic contactless charging of EVs is by exploiting magnetic induction [3], where an EV harvests energy by roaming over a large number of charging pads that are placed on roadways. The charging pads communicate with EVs through Dedicated Short Range Communication (DSRC) links. In order to fulfill the energy demand of an EV, a large number of charging pads have

to be placed over a long distance where each pad will contribute a portion of the desired energy to the EV.

Dynamic EV charging introduces several challenges that ought to be thoroughly addressed. First, a charging pad needs to only charge authorized EVs; this is intuitive for billing purposes. Second, the charging pad controllers have constrained computation and communication resources; hence, it is critical to ensure that a charging pad communicates with and handles only a single EV at a time. Furthermore, an EV will pass over a charging pad at a high speed; thus, the contact time between EV and charging pad will be very short. Therefore, authentication of the EV by the charging pad has to be immediate in order to dedicate most of the contact time for the charging service. Furthermore, it is crucial to sustain the privacy of EV owners who utilize the charging service. Specifically, the location privacy of the EVs have to be preserved. That is, each time an EV gets charged by a charging pad, its location is exposed and can be exploited to infer private information about the EV's driver such as travel path, visited places, driving habits, etc. Lastly, with such dynamic and contactless charging service, it is necessary to have a robust billing and payment system that ensures integrity and traceability.

After reviewing dynamic charging schemes in the literature, the presented schemes lack a transparent energy trading system. They either offer a charging service from only a single service provider or lack transparency on how not to favor one charging provider over the other. This paper opts to fill the gap and presents an efficient energy trading scheme that considers the characteristics and challenges of dynamic EV charging. Our proposed scheme offers a transparent bidding and payment for the charging service through a blockchain network, where smart-contracts are leveraged to instrument the business logic for the energy trading. Instead of linking charging requests with the real identities of EVs, pseudonyms are adopted in order to preserve the privacy of the EV owners. Moreover, a fast and efficient authentication protocol is proposed which offers an instant authentication of EVs by charging pads. Such an authentication protocol employs Physical Unclonable Functions (PUFs) [4], and lightweight cryptography and hashing operations in order to achieve a fast authentication of EVs that are to be served by charging pads. The contribution of the paper can be summarized as follows:

- Develop a transparent, scalable and decentralized energy trading scheme for dynamic charging of EVs, where Charging Service Providers (CSPs) submit their bids (offers)

to EVs and the best offer is selected while maintaining fairness and integrity.

- Utilize PUFs to create unclonable charging tickets to confront double-spending of a ticket.
- Devise a fast and lightweight protocol for authenticating EVs that suits the resource-constrained charging pads.
- Verify the security of our scheme using the AVISPA [5].

The rest of the paper is organized as follows. The system components and network model are discussed in Section II; this section also provides a background on PUFs. Section III presents the authentication protocol used by charging pads to verify the authenticity of EVs. It also covers the security analysis of such an authentication protocol. The performance evaluation results are provided in Section IV. The related work is discussed in Section V. Finally, the paper is concluded in Section VI.

II. SYSTEM MODEL AND APPROACH OVERVIEW

In this section, a background on PUFs is provided. This covers the concept of PUF, its types, and uses in the security of hardware. Then, the system's assumptions are highlighted. This is followed by presenting the system components, network model, and the main phases involved in our scheme.

A. Physically Unclonable Functions

PUFs have been widely exploited in the literature for the authentication and key generation for the resource-constrained IoT devices [6][7]. In essence, they have been deemed as an effective approach for fingerprinting resource constrained devices; such a fingerprint is to be used for authentication and secret key storage [4]. The design principle of PUFs is founded in the process variation during manufacturing Integrated Circuits (ICs), which is experienced even for fabricating the same IC. For instance, the difference in the gate delay that is attributed to the innate manufacturing variability of a chip is the basis for the design of an Arbiter PUF that captures such delay variation on latched values. This is referred to as a silicon biometric. The key advantage of PUFs is that they enable the

derivation of secret keys without storing them in a device memory, which is quite advantageous since an adversary cannot uncover the secret through intrusion or side-channel analysis.

Conceptually, PUF is defined as $R = f(C)$ such that a distinctive response R is generated when a unique per-device function $f(\cdot)$ is queried using a stream of bit pattern, referred to as a challenge C . The strength of PUF is derived from the fact that the function $f(\cdot)$ is neither known, nor can be cloned due to the unpredictable variations during the manufacturing of the device. Thus, the challenge-response pair (CRP) constitutes the validation of the authenticity of the device. PUF is generally classified into weak and strong, based on the challenge length, N , which determines the possible combinations of the challenge-response pairs CRPs generated by the PUF. Weak PUF has a few CRPs and is utilized in storage/generation of secret keys [8], while strong PUF provides large N and is more suited for authentication [9]. The latter is assumed in our work.

B. System Architecture

Before we explain our proposed energy trading scheme, we highlight the following assumptions:

- Each EV has a unique identification number (EV ID) such as the Vehicle Identification Number (VIN) that is assigned to every motor vehicle during manufacture.
- A PUF is embedded in the design of each charging pad. Each EV will also include a PUF that will be leveraged in preserving its privacy.
- We assume that the PUF response is sufficiently stable. In [10], various constructions of error correction schemes are discussed to mitigate the circuit-level noise.
- Special roadway, or traffic lanes, are populated with charging pads. These pads are stacked in a row and operates autonomously. Each pad has its own controller that determine activation and deactivation of wireless energy emission. A pad is equipped with radio transceivers to communicate wirelessly with the EV and road-side units.
- Every charging service provider securely stores a set of challenge-response pairs (CRPs) for every charging pad. These CRPs could be provided at the time of system setup or incrementally collected by the road-side units during low traffic periods, e.g., very late night.
- The internal communication between every charging service provider and its associated (owned) road-side units and charging pads is assumed to be secure.
- The clock of charging pads is synchronized with the road-side units, e.g., by applying the mechanism such as [11].

Fig. 1 depicts the architecture and entities of our energy trading system. The involved components are defined as follows:

- *Charging Service Provider (CSP)*: this is a company that provides dynamic charging service for EVs by investing in the infrastructure needed for the dynamic charging.
- *Charging pad*: it is a special pad that is placed on the roadway that utilizes electromagnetic induction to emit energy and charge EVs that pass over. In order to increase efficiency and reduce energy wastage, a charging pad should switch on only when an authorized EV enters its zone and stay off otherwise.

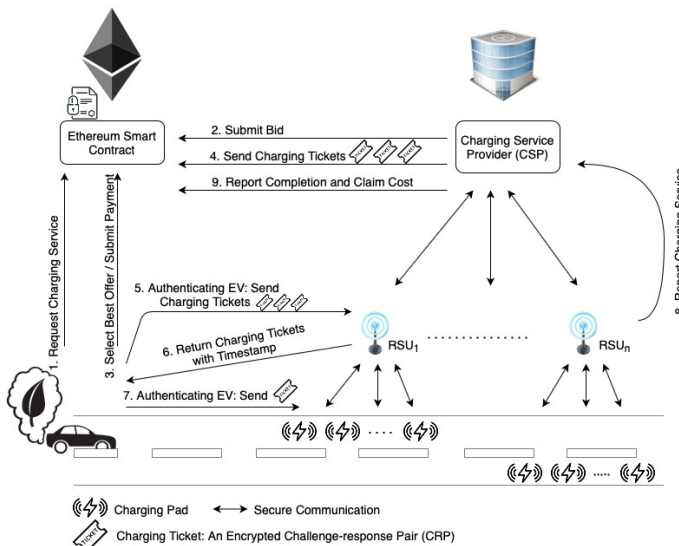


Fig. 1: Illustrating the architecture of the proposed trading system for dynamic energy charging of electrical vehicles

- **Road-side Unit (RSU):** it is a computing and communication platform that controls and manages a set of charging pads. RSU is connected securely to the CSP and a set of charging pads. Each RSU is responsible for storing a set of CRPs for the PUF of each charging pad under its control. These CRPs can be generated at pad installation time or collected in small patches during low traffic hours, i.e., late night.
- **Electric Vehicle (EV):** a vehicle that is powered by electricity instead of the traditional fossil fuel. An EV has an embedded PUF that will be leveraged in generating pseudonyms.
- **Blockchain:** it is a secure distributed ledger that is responsible for handling all the energy trading transactions. We opt for consortium blockchain as being permissioned (private) while managed by different organizations. System users can act as either EV owner or CSP. Furthermore, the blockchain network will handle peer-to-peer payment through currency exchange between system users. We consider Ethereum, which is a popular open-source blockchain platform, and its smart-contracts for managing the energy trading system. The business logic for the energy trading will be programmed in a smart-contract that will be executed by the Ethereum network.

C. System's Operation Phases

In our scheme, the process of charging an EV is divided into three phases: bidding, tickets purchase, and charging and billing. These phases are defined as follows:

Bidding phase: As shown in Fig. 2, this phase starts when an EV publishes a charging request to the blockchain network. Each charging request must include a fresh pseudonym, trip route, and charging parameters such as battery and coil type and desired charging rate. We utilize pseudonym to preserve the privacy, i.e., location, of the EV owner by hiding its real identity. A fresh pseudonym, P , is calculated as: $P = \text{hash}(C, R, ID)$. In other words, to generate a fresh pseudonym, P , an EV has to obtain a new CRP which is composed of a pair of a challenge, C , and its corresponding PUF response, R . Then, the EV appends the vehicle ID to the created CRP . This will serve as an input to a hash function. We opt for utilizing SHA-256 hash function which employs a robust cryptographic algorithm. Although the probability is very low for the PUF responses of distinct EVs for the same challenge pattern to be similar, our scheme does not take any chance and appends the vehicle's ID to the CRP before applying the hash function in order to guarantee pseudonym uniqueness. An EV's PUF is used for pseudonyms generation and is not involved in the charging coordination process.

Interested CSPs, i.e., those who have a charging service that covers the EV travelled route, will send their bids to the blockchain. The smart-contract, which will be acting as an auctioneer, determines the optimal bid, notifies the corresponding parties, the EV and the winner's CSP, and establishes a purchase agreement. An auction mechanism for the energy trading between EV and energy providers that can be adopted in our system is discussed in details in [12].

Charging Tickets Purchase: After the optimal bid is picked, a purchase agreement is established and the corresponding parties are notified. The EV then initiates a payment transaction, which covers the fees for the charging service, to

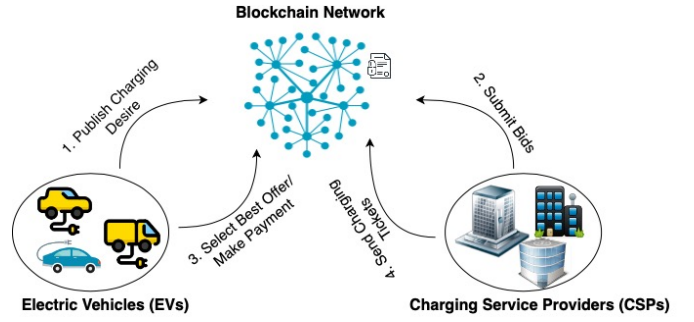


Fig. 2: Highlighting the steps in the bidding phase of dynamic EV charging

the smart-contract; the latter will notify the CSP and hold the payment until the charging service completion is reported. After being notified of the initiated payment, the CSP submits encrypted charging tickets to the smart-contract which will forward them to the corresponding EV. A charging ticket, T , is generated as follows: $T = \{CRP_{i,j}, P\}_k$. Basically, each charging ticket is composed of the EV's pseudonym, P , that is linked to the charging request and $CRP_{i,j}$, which is one of the stored challenge response pairs for charging pad i , on the controlling RSU j . Then, this ticket is encrypted using a secret key, k , which was securely shared with RSUs and charging pads beforehand. We opt for utilizing a symmetric encryption as being a lightweight, e.g., using a block cipher such as AES or a LFSR-based stream cipher like Espresso. The required number of charging tickets, N , to fulfill a charging request is calculated as: $N = d/e$, where d denotes the demanded amount of energy and e denotes the energy that can be provided by a single charging pad within the contact time between the charging pad and EV.

Charging and Billing: After purchasing the needed charging tickets from a CSP, the EV uses a single ticket for charging pad. The charging ticket proves the ownership, i.e., that the EV has paid the service fee. If the provided charging ticket is valid and the ownership is verified, the charging of the EV begins by transferring energy wirelessly to the EV battery. The billing occurs when the charging pad reports the ticket to the CSP through the RSU. After the charging tickets are reported, the CSP claims the associated fees from the smart-contract.

III. AUTHENTICATION PROTOCOL AND SECURITY ANALYSIS

This section discusses our proposed authentication protocol and analyzes its security and privacy properties. We also show the result of verifying our protocol using the AVISPA tool.

A. Authenticating EV by Charging Pad

Given the numerous vehicles on the road and the business aspect, a charging pad ought to authenticate the EV and ensure that it is indeed authorized for receiving the service. Since the contact time will be limited, the authentication protocol has to be fast. An EV will be in motion at high speed, e.g., 100 km/h; and the contact time between charging pad and EV can last up to tens of milliseconds [13]. Therefore, most of the time that EV spends passing over the charging pad should be dedicated to energy scavenging. In fact, roaming through many charging pads at high speed makes the invocation of the authentication

process quite frequent, consequently rapid verification of the authenticity of the EV and the provided charging ticket is a must in order to avoid overlapped service among vehicles. In addition, the pad is often equipped with just a microcontroller and limited storage, and hence the authentication process should be computationally lightweight.

We have designed our authentication protocol with the aforementioned requirements and constraints in mind. Our approach employs efficient and lightweight authentication primitives such as PUF and symmetric encryption to allow each charging pad to rapidly authenticate EV with a minimal possible overhead. In our protocol, each charging pad can verify the information provided by an EV with zero knowledge and no communication with neighboring pads in order to reduce storage and communication overhead. Fig. 3 depicts the steps. The protocol specifications are as follows:

1. EV sends the set of charging tickets, $\xi = \{T_1, \dots, T_n\}$, to the RSU through the message, M_1 , to present itself.
2. RSU decrypts each charging ticket, $T_y = \{CRP_{i,j}, P\}_k$, using the secret key, k , that is shared with the CSP, and looks up the pseudonym, P , in the list, L , of upcoming clients. This list is regularly updated by the CSP after ticket purchase.
3. IF $P \in L$, the RSU calculates expiration times, τ_1, \dots, τ_n , for each ticket $T \in \xi$. The time estimation is based on the EV speed and GPS coordinates while considering the possible traffic delays such that the ticket expires after 30 seconds of passing the designated charging pad. The charging tickets will be updated to include the expiration time, encrypted with k , and sent back to the EV through the message, M_2 .
4. EV sends a message, M , that contains, P' , a copy of its pseudonym, P , that was linked with the charging request and a single charging ticket, $T_y = \{CRP_{i,j}, P, \tau_y\}_k$, to each encountered charging pad based on the received order of the charging tickets. We note that the EV does not know k and cannot change T_y .
5. When a charging pad, i , receives M , it decrypts the charging ticket, T_y , using the key, k , shared with it by the CSP. Then, τ_y will be compared with the current time. If the ticket has not expired, the charging pad, i , applies C , included in T_y to its PUF to generate R' , $R' = f(C)$.
6. The charging pad, i , compares the PUF response, R' , with the response, R , available in T_y . If both responses match, i.e., $R' = R$, and the copy of the pseudonym, P' , included in M , is identical to the one in the ticket, P , this implies that the EV has provided a valid charging ticket, T_y , and is indeed authorized to receive the charging service.

If the sixth step results in a successful authentication, the charging pad, i , will switch on and start emitting energy to charge the EV battery through electromagnetic induction. These authentication steps will occur with each encountered charging pad until all purchased tickets are consumed. Each of the pads that participate will report to the CSP by sending the charging ticket, T_y , corresponding to the served EV. Such a report will in effect get relayed to the CSP through the RSU. Then, the CSP will issue a transaction to the smart-contract to claim the payment. The smart-contract will release the hold on the pending payment and send a notification to the EV.

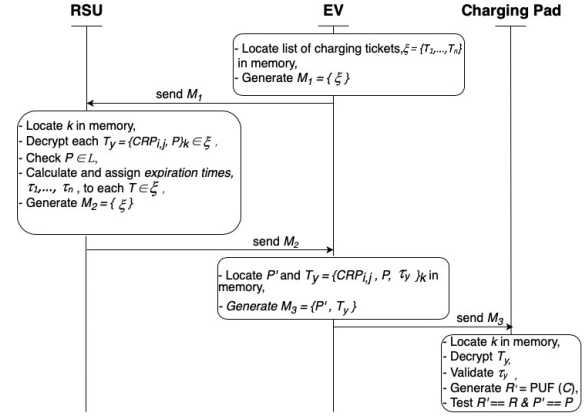


Fig. 3: Description of the protocol for EV authentication by a charging pad.

B. Privacy Preservation

Identity Anonymity. In our proposed scheme, we leverage pseudonyms in order to hide the real identity of EVs. That is, each charging request is not linked with the real identity of the requestor EV; instead, it is linked with a pseudonym. A unique pseudonym is generated by each EV for each charging request. As explained earlier in Section II, we utilize a one-way hash function, e.g., SHA-256, to create pseudonyms. Moreover, the pseudonym is a function of CRP of the embedded PUF of the specific EV; given the large CRP space, i.e., number of combinations of distinct challenge bit streams, and the fact that the response for the used challenge is not known to anyone other than the specific EV, the probability of associating a pseudonym with another EV is extremely small. Thus, charging requests cannot be exploited to trace and map to the real identity of the requestors. Furthermore, for each service for a particular EV, distinct tickets are presented by the EV to charging pads. These tickets cannot reveal the real identity of the EV since each charging ticket contains the EV's single-use pseudonym. Therefore, the privacy of EV location is preserved even when served by the same CSP and charging pads, several times.

Charging Request and Ticket Linkability. In our scheme, each single charging ticket is linked to a charging request that has to be made by an authorized EV for utilizing the system. Such linkability is achieved by sending the requests to a permissioned blockchain network. Moreover, each charging request is linked to a unique single-use pseudonym that cannot be cloned by a different EV due to the use of the EV's unique fingerprint. Therefore, if a valid charging ticket is presented to a charging pad by an EV that is not the real owner of the ticket, the authentication of the EV will not succeed. This is due to the inability of a malicious EV: (i) to reveal the real pseudonym, P , contained in the charging ticket since the ticket is encrypted, or (ii) to regenerate the pseudonym since it does not know the CRP of the EV that has been used in determining P . Thus, the condition $P' = P$ (Step 6 in the protocol) cannot be satisfied, and the verification of the ownership of the ticket will fail.

C. Attacks against Payment

Double Spending: Based on the characteristics of PUFs, a unique fingerprint is generated by each device due to the

variations in IC manufacturing. If an EV tries to double spend a ticket by presenting it again to another charging pad, the verification of the ticket will fail since the possibility of producing a similar PUF response by another charging pad is quite low. Attempts to reuse of charging tickets can only be made when the EV turns around for and presents the ticket again to the corresponding charging pad. However, such a scenario will fail since the ticket has an expiration time that is carefully calculated by the RSU based on the proximity of the EV to the pad during the first usage of the ticket. This approach prevents successful attempts for ticket reuse while not incurring storage overhead, i.e., revocation list, at the pad. We note that a replay attack is ruled out since the range of the communication between the EV and charging pad is very small; any adjacent EV will not practically intercept the ticket during transmission and has enough time to reach the pad before the ticket expires. Furthermore, another EV moving through the adjacent lane cannot be served since a charging pad only serves a single lane.

Purchasing Charging Tickets without Pay: In order for an EV to receive charging tickets from the CSP in our proposed energy trading scheme, the CSP has to be notified by the smart-contract to indicate receiving payment from the EV. This can only occur when the EV has initiated the payment to the smart-contract covering the charges enclosed in the purchase agreement. The smart-contract is a trusted entity in the system.

D. Protocol Validation Results

In order to validate our EV authentication protocol, we have utilized AVISPA [5], which has become a popular tool for validating the security properties of communication protocols. First, the protocol has been described into High-Level Protocol Specification Language (HLPSL) and its intended security properties have been specified. Then, the tool translates the protocol into an intermediate format so it can be then analyzed by the OFMC symbolic model checker and the Constraint-Logic-based Attack Searcher (CL-AtSe) of the AVISPA tool.

Our protocol is applied by each charging pad for each received ticket to ensure that the EV is an authorized vehicle and paid the fees for the intended charging service. A valid charging ticket is issued by CSP, includes a response similar to the one will be generated by PUF of the charging pad, and contains a pseudonym identical to the one presented by the EV. When describing this protocol in HLPSL, we have specified the following three security goals that ought to be satisfied in order for a charging pad to serve the EV.

- i. The CRP, enclosed in the charging ticket has to be kept secret between CSP and the charging pad since it is the critical factor in verifying the ticket validity and implicitly assessing the presenter authenticity, i.e., the EV. If the CRP is breached, it can be exploited by an adversary to deceive the charging pad as being an authorized EV.
- ii. The charging ticket has to be encrypted and cannot be revealed by an intruder in order to ensure integrity.
- iii. This goal is a unilateral authentication in which the charging pad authenticates the CSP based on the received response, R , in the ticket. That is, when the charging pad generates a similar response, R' , to the one in the ticket, R , it can be

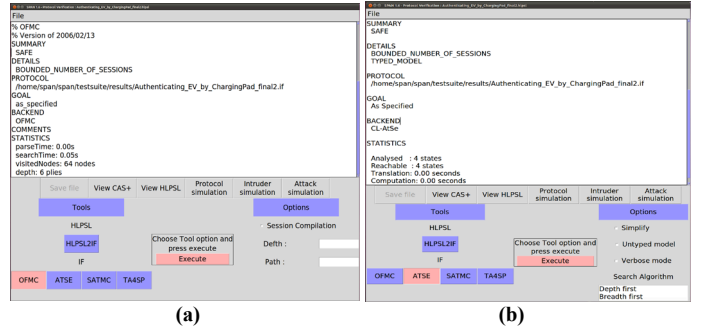


Fig. 4: The result of verifying the authentication protocol using (a) OFMC and (b) CL-AtSe backends

assured that CRP has been included in the ticket by the corresponding CSP since it maintains a list of CRPs for the charging pad and no entity will be able to clone an identical CRP other than the generating charging pad.

Figures 4(a) and 4(b), respectively, depict the result of applying the OFMC and CL-AtSe backend analyzers in AVISPA. Both backend analyzers deem our protocol to be safe and all security goals are satisfied and no vulnerability is found.

IV. PERFORMANCE EVALUATION

We have evaluated the communication and computation overhead of our proposed scheme. The former is assessed in terms of the packet size. Each generated pseudonym will be 256 bits (32 bytes) which is the size of the SHA-256 message digest. The size of a charging ticket is 36 bytes which grows to 48 bytes after being encrypted using AES symmetric encryption. We use a 128-bit (16 bytes) AES secret key in order to limit the required storage for charging pads. Meanwhile, the computation overhead measures the time it takes to form particular packets.

We have utilized the popular Crypto++ 8.5.0 library [14] to measure the runtime of the cryptographic operations used in our scheme. The measurements are made on a 2.8 GHz Dual-Core Intel Core i7 processor. Based on such setup, it takes an EV an average of $13 \mu sec$ to hash inputs using SHA-256 in order to create a fresh pseudonym. A CSP has to perform a single symmetric encryption in order to create a ticket. This takes an average of $83.8 \mu sec$ to perform AES symmetric encryption using the CBC mode. A charging pad has to perform a single symmetric decryption and to query its PUF in order to verify the authenticity of the ticket/EV. The observed average runtime for AES decryption is $12 \mu sec$. Given its simple design and hardware implementation, the time to generate a PUF response is in the order of nanoseconds, and is hence capped to $1 \mu sec$. Thus, it takes each charging pad less than $13 \mu sec$ to authenticate an EV. We note that such time can vary based on the hardware design, processing capabilities of charging pads, as well as the encryption algorithm. For example, supporting AES at the hardware level can diminish the authentication time massively, e.g., by a factor of 200.

V. RELATED WORKS

Unlike static charging of EVs, security and privacy are issues in the dynamic EV charging. In [15] scheme is proposed for charging pads to authenticate EVs without a trusted third party.

In their scheme, an EV purchases a ticket from a charging company, which signs the data provided by the EV using blind signature mechanism. A charging management center (CMC) generates a chain of keys for the EV using a hash function. To get authenticated, the EV presents a single key from the chain to each encountered charging pad. This scheme relies on the use of a revocation list since CMC and charging pads have to check whether the received ticket or key is on the revocation list. However, managing such a list imposes unwarranted overhead. Moreover, the received key by a charging pad has to be hashed a number of times which extends the computation time.

In order to preserve EV privacy, Gunukula et al. [16] adopt anonymous coins that have to be purchased from a trusted financial institution by the EV owner. Coins are provided to a CSP as a proof of payment. After verifying the validity of the coins with the issuing bank, the CSP provides tokens to EV that will be used to create shared secret keys for the authentication of the EV to RSUs. The RSU provides another token to the EV to be used for creating secret keys to be presented to charging pads for the EV authentication. A hierarchical authentication is adopted where EV authenticates itself to CSP, RSUs, and charging pads sequentially. We believe that anonymous coins do not adequately prove the legitimacy of an EV since coins can be stolen and used by another EV.

Portunes+ [13] utilizes pseudonyms to preserve EV privacy and symmetric encryption and spatiotemporal EV location for authenticating an EV to charging pads. In this scheme, a set of pseudonyms with corresponding set of keys are created by a CSP and disseminated to charging pads through pad owners during low traffic times. An EV sends its charging parameters to the CSP, which in turns generates and sends a pseudonym with corresponding set of keys to the EV. The EV has to present the pseudonym and one of keys to each encountered charging pad for authentication. For billing, the charging pads report the service fees to their owner which issues an invoice to the CSP which in turn bills the EV. Since Portunes+ assumes the trustworthiness of CSP, pad owners, and charging pads, fee overclaiming seems to be hard to detect.

Baza et al. [17] have proposed a privacy-preserving energy trading scheme for EVs and charging stations based on blockchain. This scheme adopts the use of untraceable digital coins that are offered by a trusted financial institution and have to be purchased in advance by EVs. When charging stations submit their bids to the blockchain, each interested EV selects the best bid and reserves a particular timeslot for a charging point. Digital coins are used to cover the charging service. However, this energy trading scheme is designed for static charging of EVs where they stop by charging points in parking lots. Obviously such a scheme does not suit dynamic charging since it requires each EV to reserve a timeslot, i.e. 30 mins, to charge its battery which is not practical when EVs charge while moving. Furthermore, EV authentication protocols for static systems cannot be adopted in dynamic charging due to the incredibly small contact time between EVs and charging pads.

VI. CONCLUSION

We have presented an energy trading scheme for dynamic EV charging. Our scheme leverages blockchain and smart-contracts technology to provide secure, transparent, and decentralized energy trading between charging service providers and EVs. Moreover, our scheme considers the characteristics of the dynamic charging infrastructure such as having a large number of resource-constrained charging pads and a very short contact time between EVs and charging pads. Additionally, dynamic charging puts the privacy of EVs at risk since by charging from certain pads, the location privacy of EVs can be violated. To meet the requirements, our scheme employs PUF and lightweight cryptography. PUFs have been utilized in our scheme to create unique pseudonyms for EV and generate unclonable and tamper-resistant charging tickets that enable fast validity verification and prevent double-spending. Our scheme enables EV authentication in a fast and efficient manner and its robustness is validated using AVISPA.

REFERENCES

- [1] "Emissions from Hybrid and Plug-In Electric Vehicles," afdc.energy.gov/vehicles/electric_emissions.html. [4-5-2021].
- [2] "eGallon," Energy.gov. www.energy.gov/maps/egallon. [4-May-2021].
- [3] H. H. Wu, A. Gilchrist, K. Sealy, P. Israelsen and J. Muhs, "A review on inductive charging for electric vehicles," *Proc. IEEE International Electric Machines & Drives Conference (IEMDC)*, 2011, pp. 143-147.
- [4] C. Herder, M. Yu, F. Koushanfar and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126-1141, Aug. 2014.
- [5] The AVISPA Project. <http://www.avispa-project.org/>. [09-May-2021].
- [6] U. Chatterjee et al., "Building PUF Based Authentication and Key Exchange Protocol for IoT without Explicit CRPs in Verifier Database," *IEEE Trans. on Dependable and Secure Comp.*, 16(3), pp. 424-437, 2019.
- [7] M. Aman, K. C. Chua, and B. Sikdar, "Mutual authentication in IoT systems using physical unclonable functions," *IEEE Internet of Things Journal*, Vol. 4, No. 5, pp. 1327-1340, Oct. 2017.
- [8] U. Chatterjee, R. S. Chakraborty, and D. Mukhopadhyay, "A PUF-based Secure Communication Protocol for IoT," *ACM Trans. Embed. Comput. Systems*, 16(3), pp. 67:1-67:25, Apr. 2017.
- [9] M. Aman, M. H. Basheer and B. Sikdar, "Data Provenance for IoT with Light Weight Authentication and Privacy Preservation," *IEEE Internet of Things Journal*, 6(6), pp. 10441-10457, Dec. 2019.
- [10] J. Delvaux, D. Gu, D. Schellekens and I. Verbauwhede, "Helper Data Algorithms for PUF-Based Key Generation: Overview and Analysis," *IEEE Trans. on Comp.-Aided Des. of IC & Sys.*, 34(6), pp. 889-902, 2015.
- [11] E. Mallada, Xiaoqiao Meng, M. Hack, L. Zhang and A. Tang, "Skewless network clock synchronization," *Proc of 21st IEEE International Conference on Network Protocols (ICNP)*, 2013, pp. 1-10.
- [12] N. Lasla, M. Al-Ammari, M. Abdallah and M. Younis, "Blockchain Based Trading Platform for Electric Vehicle Charging in Smart Cities," *IEEE Open J. of Intelligent Transportation Sys.*, vol. 1, pp. 80-92, 2020.
- [13] H. Li, G. Dán and K. Nahrstedt, "Portunes+: Privacy-Preserving Fast Authentication for Dynamic Electric Vehicle Charging," *IEEE Transactions on Smart Grid*, 8(5), pp. 2305-2313, Sept. 2017.
- [14] "Crypto++® Library 8.5," Crypto++ Library 8.5 | Free C++ Class Library of Cryptographic Schemes. <https://www.cryptopp.com/>. [10-May-2021].
- [15] K. Rabieh and M. Wei, "Efficient and privacy-aware authentication scheme for EVs pre-paid wireless charging services," *Proc. IEEE International Conference on Communications (ICC)*, Paris, France, 2017.
- [16] S. Gunukula, et al., "Efficient scheme for secure and privacy-preserving electric vehicle dynamic charging system," *Proc. IEEE International Conference on Communications (ICC)*, Paris, France, 2017.
- [17] M. Baza, R. Amer, A. Rasheed, G. Srivastava, M. Mahmoud and W. Alasmary, "A Blockchain-Based Energy Trading Scheme for Electric Vehicles," *Proc. IEEE Consumer Comm. & Net. Conf. (CCNC)*, 2021.