RAMA: Real-Time Automobile Mutual Authentication Protocol Using PUF

Gaurang Bansal[1], Naren[1], Vinay Chamola[1]
[1]Department of Electrical and Electronics Engineering, BITS Pilani, Pilani Campus, India
Email: h20140128@pilani.bits-pilani.ac.in (Gaurang Bansal), f2015547@pilani.bits-pilani.ac.in (Naren),
vinay.chamola@pilani.bits-pilani.ac.in(Vinay Chamola)

***Abstract*—The batteries of electric vehicles enable the functionality of V2G networks. The purpose of V2G is to handle the trading of energy for electric vehicles powered by batteries as well as the power grid. This is essential to make more efficient use of the energy of the grid. The electrical energy stored in the EV batteries can function as a power source for the grid and other energy-deficient EVs. The energy stored in the batteries of the EVs could be used to pump power into the grid when the load on the grid is too heavy. Despite its wide-ranging applications, the privacy and safety of intelligent grids continue to be a severe problem. Any protocol designed for V2G applications must be safe, lightweight, and safeguard the car owner's privacy. As individuals usually do not guard EVs and charging stations, physical security is also a must. To address these issues, we are proposing a Real-time Automotive Mutual Authentication protocol for V2G devices based on Physical Unclonable Functions (PUF). PUFs are used by the proposed protocol to obtain a two-step mutual authentication (MA) between an EV and the Grid Server. It is lightweight, safe, and preserves privacy.**

I. Introduction

Global demand for electricity is projected to surge to 82% by 2030. Power grids are therefore aimed at reducing the number of auxiliary generators needed. They use demand-response methods to decrease energy usage and boost effectiveness [1]. Although these methods have a number of advantages, safety and privacy problems stay major weaknesses [2]. During the exchange of electricity between a car and a service provider, a lot of data is passed. However, an opponent could compromise this information flow by manipulating it or ultimately capturing it. This could lead to unjust or oppressive trades in energy between the two sides. In addition, the victim's data (which could be recorded) can be used in criminal operations and directed advertisements. The computing systems used in V2G are cheap, tiny, and affordable [3]. The EVs are very often parked in easily accessible locations. This allows an attacker to capture V2G units from such cars without being noticed. Hence, making V2G units safe against physical invasions is essential. An intruder, for example, could obtain and launch numerous exploits with the secret keys present on the unit. Physical Unclonable Functions (PUFs) have surfaced as a lucrative approach for defense against physical attacks. PUFs eliminate the need to hold confidential keys in the storage of the units and operate on challenging-response combinations. A PUF's challenge-response system captures the intrinsic variability of the IC fabrication process [4]. Its response depends on both the input and the chip's physical microstructure [5]. The physical randomness induced by the variations in the manufacturing process helps to make each PUF unique, i.e., it is impossible to create two identical copies.

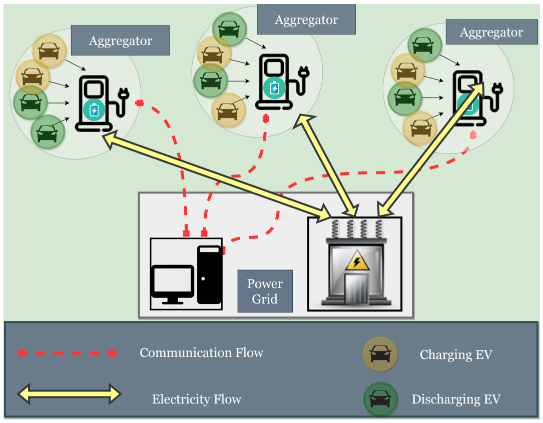


Fig. 1: System model

An aggregator in V2G schemes is really acharging stationthat functions as a middleman between the EVs and the electricity grid. In such scenarios, secure communication necessitates authentication between the EVs and the aggregator, and between aggregator and the grid, as well as between the EVs and the grid. Using a two-stage process, the presented Real-time Automobile Mutual Authentication(RAMA) protocol achieves the above-described authentications. Using Pseudo IDs (PIDs), the vehicle's identification is obscured to safeguard the identifiers and location of the car owner. In RAMA, there are two distinct session keys, one between the aggregator and the grid, and the other between the EV and the aggregator. These session keys are characteristic of the PUFs installed on the aggregator and the EV. This guarantees communication secrecy and eliminates the need to retain any secret keys in the EVs and aggregator's memory. The proposed protocol implements fast cryptographic operations, ensuring that it is energy-efficient and lightweight. There is also a limited set of message passes, resulting in reduced overhead.

The rest of this document is arranged as follows. The related work in V2G techniques is discussed in Section II. Section III discusses a preliminary background to PUFs. Section IV details the network model and the notations used in this document. The MA protocol (RAMA) is discussed in Section V. We evaluate and contrast the performance of our protocol with state-of-the-art protocols in Section VI and finally conclude the document in Section VII

II. Related Work

The idea of V2G was first proposed in 2004 by Kempton and Tomic [6]. The structure of a V2G network must have been well defined, and the effect of V2G on the power grid must be examined before protocols for V2G systems could be established. The writers of [7] carried out this research. The most important components of a V2G protocol are a secure connection, privacy and computational efficiency [8]. The existing literature of [9, 10, 11, 12] has offered substantial recognition to the preservation of privacy in V2G systems. Yang *et al* presented a protocol P^2 in [9] to achieve privacy for each EV along with a rewarding arrangement that is vital to the practical application of V2G. Liu *et al* Describe their proposal, $AP3A$, which can determine whether an EV is at home or visiting the network [10]. Instead of exposing individual battery level, $AP3A$ transmits the aggregated energy status of cars associated to an aggregator, thereby ensuring privacy to each EV. Liu *et al* [12], [13] present a scheme to identify the various roles played by an EV, i.e., either as a customer, storage or generator. Their $ROPS$ scheme addresses specific privacy concerns for each role. Tsai and Lo accomplish MA and protection of identity through the use of a secret key supplied by a third party affiliate [14]. This allows the smart meters to authenticate rapidly with the vendor. [15],[16] suggest a computationally less expensive privacy protection system. They identify the specific problem, which is of EV authentication in the V2G scheme. The energy grid, therefore, assumes the duty of maintaining the communication's confidentiality and integrity. They accomplish less overhead by decreasing the number of messages communicated. Based on the Canett-Krawczyk adversary model of smart grids, [17] have come up with a safe authenticated Key Agreement scheme. Shen *et al* suggest a key agreement procedure for privacy protection for V2G networks [18]. They guarantee security via a session key and ensure privacy via a self-synchronization technique. In [19, 20],[21], security in environments were presented. Saxena and Choi described an authentication strategy for large V2G systems in which vehicles travel as visitors from their local V2G network to many other V2G networks [23]. They propose a strategy of MA that helps to protect against attacks on key and data along with protection towards impersonation attacks. Tao *and al* [24], suggest $AccessAuth$, a capacity-aware protocol, taking into account the capacity constraints of each EV, V2G network, and provides admission control based on the mobility of EVs. Their authentication model is high-level, and the procedure is rooted in the trust which established beforehand among the V2G network domains to guarantee that sessions are conducted only by approved nodes. To suggest a lightweight MA protocol, Gope and Sikdar [25] used hash functions which are irreversible and of non-collision type. Fouda *et al* [26], presented a light-weight message authentication system. Smart meters of different levels achieve MA between one another in the smart grid, following which a shared session key is created. With this shared session key and a hashed authentication code component, they accomplish light-weight message authentication. Moghadam et al. present a secure and lightweight communication protocol for smart grids based on hashing and private key to ensure strength of security and key agreement simultaneously [27].

While this scheme has been described for use in smart grid systems, it can be applied to V2G networks also. Although there are several privacy-conserving, light-weight, MA and key formation protocols for V2G applications, neither of them include all the desired privacy and security characteristics. It is observed that if a scheme offers complete security, either it requires equipment that would be resource-intensive or it involves sophisticated computations.

III. Preliminary Background

A PUF is based on a unique physical property of a device. It is similar to and as unique as the biometrics of a human. The distinguishing attribute of a PUF is that it relies on a physical basis, making it impossible to reproduce a PUF using cryptographic primitives. Additionally, the term "physical unclonable" indicates that it is computationally infeasible or difficult to produce a physically identical PUF [28]. By using PUFs in an interconnected system such as IoT or V2G systems, every single device can have its own unique "fingerprint" which cannot be cloned or reproduced. A PUF behaves like a mathematical function whose input (challenge) and output (response) are both in the form of a string of bits. A PUF function can be represented as:

$$K = PUF(C) \tag{1}$$

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

All PUFs behave in the following manner with respect to their input C and output K:

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

IV. Network Model

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

The server on the power grid starts with a set of challenge-response pairs, (C, K), for each EV. The grid server acquires this initial set (C, K) at the time of initialization. To deploy a new vehicle on the roads, initialization involves the initial set (C, K) to be sent to the power grid server using a secure channel. This initialization can be done using a timed one-time password algorithm (TOTP) [29] and an operator using a password. After this exchange, the vehicle can function on its own without needing any operator or secure channel. The grid server stores the actual identity ID_V, and the (C, K) pair for each vehicle, while the vehicle itself does not store anything. Later, this ID_V is replaced with pseudo-identities in further exchanges.

TABLE I: Notations

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

V. Proposed Mutual Authentication Protocol

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

- Aggregator and grid.
- Vehicle and aggregator.

Both these stages are similar, therefore we present only the second stage, i.e., MA between a vehicle and the aggregator.

A. Mutual Authentication between Vehicle and Aggregator

We begin stating that the first stage of the RAMA protocol is complete and a session key S_k is established between the aggregator and the grid. This is shown as a red box in Figure 2. Now, we present the second stage, i.e., for authentication between a vehicle and an aggregator.

1) The aggregator sends an encrypted message $Msg_{M2G} = E([ID_V, N_V], S_k)$ containing the ID of the vehicle ID_V, and its nonce N_V encrypted with S_k to the grid server.
2) The grid server decrypts this message using S_k and obtains ID_V and nonce N_V. It checks within its memory if ID_V exists and whether nonce N_V is fresh. If either of the conditions fails, the authentication request by the vehicle is terminated. Using ID_V, the grid server finds the corresponding set of challenge-response pairs (C'', K'') from its memory:

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

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

$$D_1 = N_V \oplus F(K''_0, N_A)$$
$$D_2 = N_A \oplus F(K''_1, D_1)$$
$$D_i = D_{i-2} \oplus F(K''_{i-1}, D_{i-1}), \;\; 3 \leq i < m$$
$$D_m = D_{m-2} \oplus F(K''_{m-1}, D_{m-1})$$
$$D = (D_m || D_{m-1}) \oplus K''_m)$$
$$P = m \oplus K''_0.$$

3) The aggregator sends C'', D, P and the MAC to the EV. Within the MAC, the first parameter verifies the identity of the vehicle. Data integrity is ensured by the second and third parameters. Freshness of the source (aggregator in this case) is identified by N_A which is the last parameter.
4) On receiving the message from the aggregator, the vehicle generates the key K'' by using its PUF for the newly received challenge C'' as given in (1). Then, it calculates m as shown below:

$$m = P \oplus K''_0. \tag{2}$$

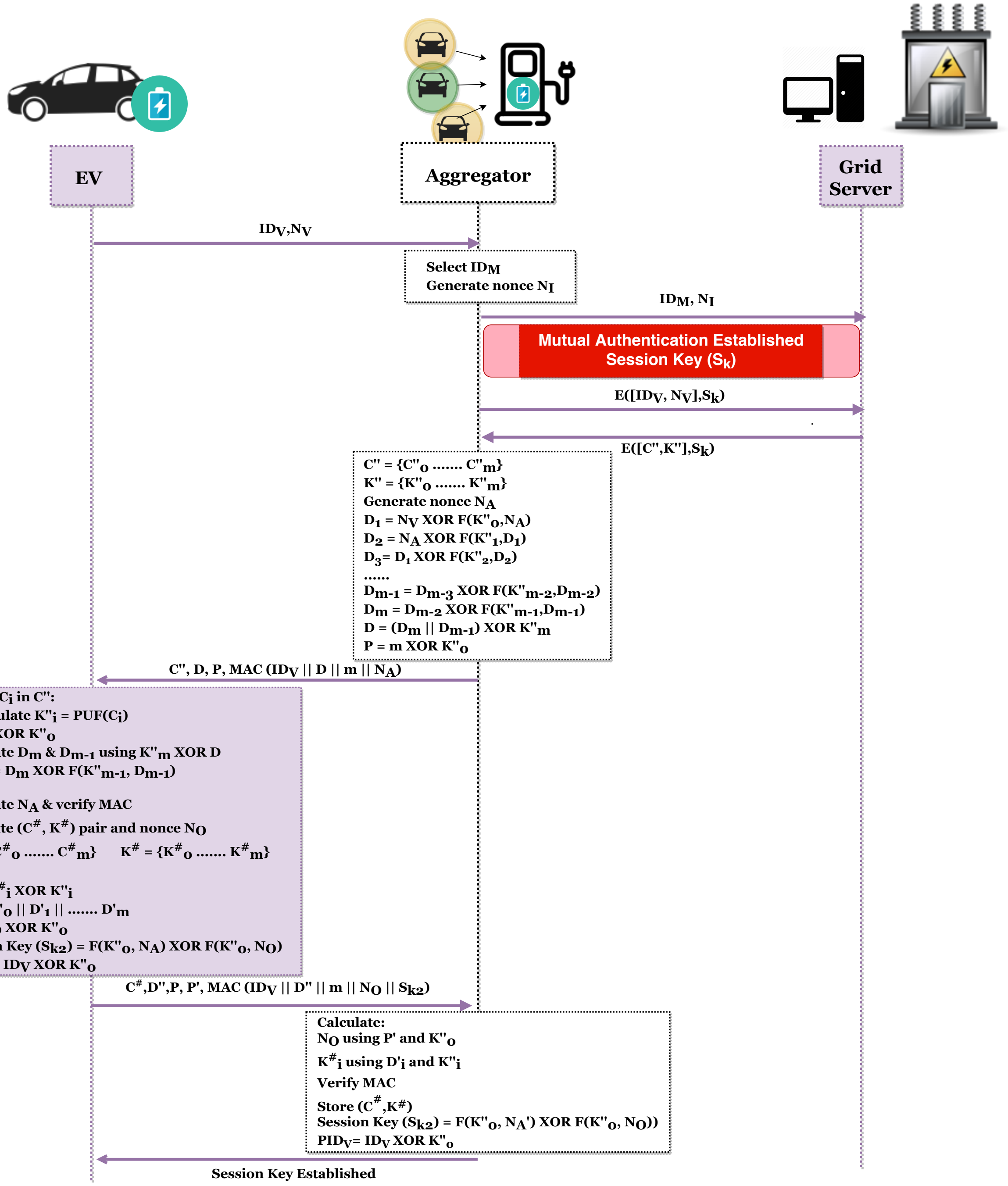
Using m and K, it finds N_A as shown:

$$D_m || D_{m-1} = K''_m \oplus D$$
$$D_{i-2} = D_i \oplus F(K''_{i-1}, D_{i-1})$$
$$N_A = D_2 \oplus F(K''_1, M_1)$$
$$N_V = D_1 \oplus F(K''_0, N_A).$$

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

$$C^{\#} = (C^{\#}_0, C^{\#}_1, C^{\#}_2, \cdots, C^{\#}_m)$$
$$K^{\#} = (K^{\#}_0, K^{\#}_1, K^{\#}_2, \cdots, K^{\#}_m).$$

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



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

Fig. 2: Mutual authentication between electric vehicle and the aggregator.

follows:

$$D'_i = K^\#_i \oplus K''_i$$
$$D'' = D'_0||D'_1||.....||D'_m$$
$$P' = N_O \oplus K''_0$$
$$S_{k2} = F(K''_0, N_A) \oplus F(K''_0, N_O)).$$

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

$$PID_V = ID_V \oplus K''_0. \tag{3}$$

This ensures identity protection because an adversary will not be able to figure out whether a previous transaction belonged to the same EV or not. ID_V then sends $C^\#$, D'', P, P' and MAC. This time the MAC includes a fifth parameter which is the session key S_{k2}. This ensures that both EV and aggregator have the same session key.

6) On receiving the message from the vehicle, the aggregator calculates N_O using P and K''_0:

$$N_O = P' \oplus K''_0. \tag{4}$$

Then, it calculates $K^\#_i$ using D'_i and K''_i:

$$K^\#_i = D'_i \oplus K''_i. \tag{5}$$

The new set of challenge-response pairs $(C^\#, K^\#)$ is

TABLE II: Comparison of Security Features

Features	[22]	[9]	[10]	[12]	[14]	[30]	[24]	RAMA
Mutual Authentication	✓	✓	✓	✓	✓	✗	✓	✓
Identity Protection	✓	✓	✓	✓	✗	✓	✓	✓
Message Integrity	✓	✓	✗	✗	✓	✓	✓	✓
Man-In-The-Middle Attack	✓	✓	✗	✓	✓	✓	✓	✓
Impersonation Attack	✓	✗	✗	✗	✓	✓	✓	✓
Replay Attack	✓	✓	✗	✗	✓	✓	✓	✓
Session Key Security	✓	✓	✗	✓	✗	✓	✓	✓
Physical Security	✗	✗	✗	✗	✗	✗	✗	✓

stored in its memory. Then it calculates the session key S_{k2} as shown below and verifies the MAC:

$$S_{k2} = F(K_0'', N_A) \oplus F(K_0'', N_O). \tag{6}$$

The pseudonym or pseudo-ID PID_V is calculated as:

$$PID_V = ID_V \oplus K_0'' \tag{7}$$

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

VI. Comparison and Analysis

A. Security Goals And Protection Against Various Attacks

A comparison of the security features of our protocol with a different state of the art protocols currently in use in V2G systems is presented in Table II. "✓" indicates that the protocol possesses a feature or is secure against an attack. "✗" indicates that the protocol lacks a feature or is insecure against an attack. All the mentioned protocols provide MA except [30]. Without MA, a participating entity can neither verify if it is sending a message to a trusted entity, nor can it verify if the message it received is from a trusted entity. With MA, both the sending and receiving parties can be sure of each other's authenticity. Identity protection is not provided by the protocol in [14]. Consequently, an attacker may easily figure out the real identity of the EV by looking at the usage data. The protocols in [10] and [12] do not provide message integrity. Our protocol uses MAC to ensure this. All the entities (EVs, aggregators and grid server) can easily detect any tampering in the messages they receive. The protocol in [10] is vulnerable to man-in-the-middle attacks. An adversary may insert itself between the communication of an EV and the aggregator, or between the aggregator and the grid server and gain control of the communication between them. The protocols in [9], [10] and [12] are vulnerable against impersonation attacks. The protocols in [10] and [12] are not secure against replay attacks. The protocols in [10] and [14] do not provide session key security. Physical security is provided only by the proposed protocol (RAMA). The attacker that captures an EV device must not be able to gather any secrets. As also mentioned in Section I, almost all authentication protocols proposed in the literature require that the EVs store at least one secret in their memory, if not more. Such storing of secrets on any device renders the protocols vulnerable to physical attacks. The MA protocol proposed in this paper has two features which make it resistant to any physical attacks: (i) EVs and aggregators need not store any secrets in their memory; (ii) there is a secure communication between the EV's microcontroller and its PUF since they are both on the same chip. Thus, even though an attacker may physically capture the device, it would be impossible for them to extract any secrets. Therefore, RAMA is resilient against physical attacks.

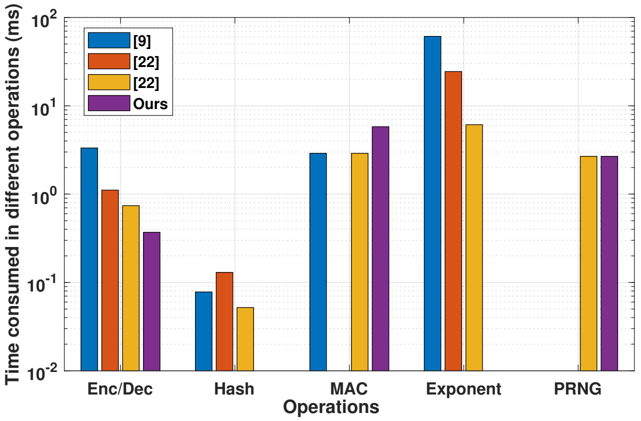


Fig. 3: Performance comparison of the proposed protocol with state-of-the-art schemes

B. Computational Performance

Here we compare the performance of our protocol with the protocols of [9], [22] and [10]. Fig. 3 shows the comparison of our protocol with the schemes mentioned above in terms of time consumed in various cryptographic operations such as Encryption/Decryption, Hash, MAC, Exponent and Pseudo Random Number Generation (PRNG). The simulations were run in Python 2.7 language on a 2016 MacBook Air with Core i5-5200U and 8GB DDR3 RAM. The protocols of [9], [22] and [10] respectively consume 64.2, 25.4 and 33.1 ms while our protocol consumes only 6.3 ms in these cryptographic operations. Thus, the proposed protocol is much faster than current state-of-the-art schemes.

VII. Conclusion

This paper proposed MA protocols for the two stages or steps which arise in a V2G system: (i) For MA between the aggregator and the grid server, and (ii) for MA between EV and aggregator. The proposed protocol (RAMA) uses a challenge-response architecture, which is enabled by PUFs. This gives our proposed protocol the advantage of not having to store any secret information in EVs and aggregators. Secrets are stored only in the grid server. Only one set of challenge-response pairs is stored in the server for every EV. Two session keys are established when an EV wants to authenticate with the grid server: one session key between the aggregator and the grid server, and another one between the EV and the aggregator. We showed that RAMA achieves MA, identity protection, message integrity, physical security, and session key security along with protection against various attacks such as MITM attacks, replay attacks and impersonation attacks. Moreover, it uses simple computations, which makes it very efficient and fast. Hence, the proposed protocol is a viable solution for upcoming V2G systems. Future extensions of this work based on techniques explained in [31, 32, 33, 34, 35, 36] can explore integration of the proposed scheme with blockchain to strengthen security provisioning.

References

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

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

[3] A. Abdallah and X. Shen, "Lightweight Security and Privacy-Preserving Scheme for V2G Connection," in *2015 IEEE Global Communications Conference (GLOBECOM)*. IEEE, dec, pp. 1–7.

[4] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications," in *2008 IEEE International Conference on RFID*. IEEE, apr, pp. 58–64.

[5] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "Brand and IP protection with physical unclonable functions," in *2008 IEEE International Symposium on Circuits and Systems*. IEEE, may, pp. 3186–3189.

[6] W. Kempton and J. T. Tomic, "Vehicle-to-grid power fundamentals: Calculating capacity and net revenue," *Journal of Power Sources*, pp. 268–279.

[7] Sekyung Han, Soohee Han, and K. Sezaki, "Development of an Optimal Vehicle-to-Grid Aggregator for Frequency Regulation," *IEEE Transactions on Smart Grid*, no. 1, pp. 65–72, jun.

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

[9] Z. Yang, S. Yu, W. Lou, and C. Liu, "P^{2}: Privacy-Preserving Communication and Precise Reward Architecture for V2G Networks in Smart Grid," *IEEE Transactions on Smart Grid*, no. 4, pp. 697–706, dec.

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

[11] H.-R. Tseng, "A secure and privacy-preserving communication protocol for V2G networks," in *2012 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, apr, pp. 2706–2711.

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

[13] T. Alladi, V. Chamola, B. Sikdar, and K.-K. R. Choo, "Consumer iot: Security vulnerability case studies and solutions," *IEEE Consum. Electron*, vol. 9, pp. 6–14, 2019.

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

[15] V. Hassija, G. Bansal, V. Chamola, V. Saxena, and B. Sikdar, "Blockcom: A blockchain based commerce model for smart communities using auction mechanism," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2019, pp. 1–6.

[16] G. Bansal, A. Dua, G. S. Aujla, M. Singh, and N. Kumar, "Smartchain: A smart and scalable blockchain consortium for smart grid systems," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2019, pp. 1–6.

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

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

[19] G. Bansal, V. Hasija, V. Chamola, N. Kumar, and M. Guizani, "Smart stock exchange market: A secure predictive decentralised model," in *2019 IEEE Global Communications Conference: Communications Software, Services and Multimedia Apps (Globecom2019 CSSMA)*, Waikoloa, USA, Dec. 2019.

[20] G. Bansal and A. Bhatia, "A fast, secure and distributed consensus mechanism for energy trading among vehicles using hashgraph," in *2020 International Conference on Information Networking (ICOIN) (ICOIN 2020)*, Barcelona, Spain, Jan. 2020.

[21] S. Kumar, G. Bansal, and V. Shekhawat, "A machine learning approach for traffic flow provisioning in software defined networks," in *2020 International Conference on Information Networking (ICOIN) (ICOIN 2020)*, Barcelona, Spain, Jan. 2020.

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

[23] T. Alladi, V. Chamola, J. J. Rodrigues, and S. A. Kozlov, "Blockchain in smart grids: A review on different use cases," *Sensors*, vol. 19, no. 22, p. 4862, 2019.

[24] M. Tao, K. Ota, M. Dong, and Z. Qian, "AccessAuth: Capacity-aware security access authentication in federated-IoT-enabled V2G networks," *J. Parallel Distrib. Comput.*, pp. 107–117.

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

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

[27] M. Moghadam, M. Nikooghadam, A. Mohajerzadeh, and B. Movali, "A lightweight key management protocol for secure communication in smart grids," *Electric Power Systems Research*, no. August 2019, p. 106024.

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

[29] D. MRaihi, S. Machani, M. Pei, and J. Rydell, "Rfc 6238-totp: Time-based one-time password algorithm," *Internet Requests for Comments*, 2011.

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

[31] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[32] V. Hassija, V. Saxena, and V. Chamola, "A mobile data offloading framework based on a combination of blockchain and virtual voting," *Software: Practice and Experience*, Dec. 2019.

[33] T. Alladi, V. Chamola, R. Parizi, and K. K. R. Choo, "Blockchain applications for industry 4.0 and industrial iot: A review," *IEEE Access*, Nov. 2019.

[34] A. Miglani, N. Kumar, V. Chamola, and S. Zeadally, "Blockchain for internet of energy management: A review, solutions and challenges," *Computer Communications*, Dec. 2019.

[35] V. Hassija, V. Chamola, S. Garg, N. Dara, G. Kaddoum, and N. Jayakody, "A blockchain-based framework for lightweight data sharing and energy trading in v2g network," *IEEE Trans. on Vehicular Technology*, Dec. 2019.

[36] V. Hassija, V. Saxena, and V. Chamola, "Scheduling drone charging for multi-drone network based on consensus time-stamp and game theory," *Computer Communications*, vol. 149, pp. 51–61, 2020.