Privacy-aware Authentication Scheme for Electric Vehicle In-motion Wireless Charging

Khaled Hamouid

LaSTIC Research Laboratory
University of Batna 2
Batna, Algeria
k.hamouid@univ-batna2.dz

Kamel Adi

Computer Security Research Laboratory
Department of Computer Science and Engineering
University Of Quebec in Outaouais
Quebec, Canada
kamel.adi@uqo.ca

***Abstract*—In-motion wireless charging services have emerged for the development of Electric Vehicles (EVs) industry. Fast authentication and privacy awareness are the major concerns in this promising technology. This paper proposes FLPA, a fast and anonymous authentication scheme for EVs charging on the move, which preserves the identity and location privacy of EVs during the recharging process. In order to deal with EV's high mobility and constrained resources of charging pads, FLPA provides lightweight and fast EVs authentication to charging pads while ensuring secure and fair-billing based on authenticated pairwise keys and coin chains. Through a performance analysis, we demonstrate our scheme's advantage compared to current solutions.**

***Index Terms*—electric vehicle, wireless charging, dynamic charging, privacy, anonymity, authentication, verifiable encryption, billing**

I. Introduction

An Electric Vehicle (EV) is a new generation vehicle propelled by an electric motor, using electrical energy stored in batteries instead of fossil fuel. Recently, EV's industry has become crucial in future transportation systems as it contributes in fuel consumption saving and pollution reduction. However, EVs may have shorter cruising range compared to gasoline vehicles which necessitates EVs to visit a recharging station very frequently. In-motion wireless charging, or dynamic charging [1], is a promising technology for the development of EVs industry. By installing wireless charging pads under the roadbed, EVs may charge their batteries through magnetic induction while on the move.

A support for cyber-infrastructure and security protocols is a pre-requisite for EV dynamic charging systems. In particular, authentication and proper billing are the major concerns. Indeed, the Charging Service Provider (CSP) needs to verify the authenticity of in-motion EV and its payment credentials before allowing it to use the charging infrastructure. The latter, which is mainly consisting of a large number of charging pads, must also be able to authenticate the incoming EVs to only charge the authorized EV and to bill the right customer. At the same time, this communication between the different parties should not leak privacy-sensitive information of EV users which could be maliciously exploited, such as generating movement profiles and unauthorized tracking.

Unfortunately, conventional authentication and billing methods are not suitable for dynamic charging systems due to several factors, such as EV's high mobility, highly frequent authentications, resource constrained charging pads and privacy requirement. Indeed, the contact time between the EV and charging pads is very short, especially if the EV is moving at high speed. Besides, the number of pads along the road leds to high frequent authentications. The authentication protocols must therefore be fast and lightweight. On the other hand, the EV's privacy, with regard to its location and identity should be preserved when the EVs are frequently using the dynamic charging service while on the move.

Although many research efforts aim to tackle these issues, protocols that meet privacy-aware, lightweight authentication and fair-billing requirements are still lacking. In some works [2], efficiency is improved by reducing exchanged messages to support fast authentication, while the privacy is not considered. In [3], [4], the CSP is trusted to know the EV's identity and location. In other works [5]–[7], authentication protocols take privacy as primary concern, while they require excessive messages exchange during the re-charging process which is less likely to ensure fast and lightweight authentication. In [8], recharging tokens cannot be linked to EV, and hence they could be used by impersonator EVs or may be double spent.

In this paper, we propose FLPA, a fast and privacy-aware authentication scheme for EV dynamic charging. Based on the verifiable encryption [9], authenticated-pairwise-keys [10] and coin hash chain [11], FLPA meets the following appealing features: 1) Anonymous EV authentication to the CSP and charging infrastructure using verifiable pseudonyms instead of real identities, which provides identity and location privacy of EV users, 2) Lightweight and fast authentication between EV and charging pads without involving CSP, and which requires only one message exchange and simple verification of a hash chain, 3) FLPA achieves fair-billing and prevents selfish EVs form double spending the same charging coin. 4) Conditional anonymity where EV can be traced back by only a Trusted Authority (TA) for revocation and other security purposes.

The evaluation results show that FLPA achieves better performances compared to similar existing solutions.

In the remainder of this paper, we first present the under-

lying system model as well as the details of the proposed solution in section II. Then, we present the evaluation results in section III. Finally, we conclude the paper in section IV.

II. Proposed scheme

A. System model and overview

As illustrated in Fig. 1, in our system model, we consider a *bank* (or broker), *CSP*, *charging pads (CPs)*, *road side units (RSUs)* and *EVs*. The *CSP* is responsible for deploying the charging infrastructure that mainly consists of a number of *CPs* installed under the roadbed many kilometers along. The *CPs* are used for wireless *EV*'s battery charging through magnetic induction. They can communicate with *EVs* and *CSP* through *RSUs* or directly using fast wireless communication technology (e.g. WiMax, 4G).

In the proposed scheme, the EV authentication is achieved in two phases where EV first authenticates to the CSP and then to CPs. In the first phase, FLPA suggests a strong anonymous authentication based on pseudonym's authenticity verification. Due to EV's high mobility and constrained resources of charging pads, FLPA uses, in the second phase, a fast and lightweight authentication mechanism based on Authenticated-Key-Agreement protocol [10] and hash chains. As a result, FLPA reduces the exchanged messages between the EV and CPs to a single message and the computation overhead to a symmetric decryption and simple hash chain verification.

The block diagram in Fig. 2 illustrates the proposed scheme. The first phase is the EV pseudonyms issuing by a Registration Trusted Authority (RTA), which may be for instance the issuing authority of the vehicle registration document. Then, the EV should authenticate to the bank to request an authorization to the CSP redemption for a specified amount. If the authentication succeeds, the bank sends back to EV a signed Payment Authorization Token (PAT) for the specified CSP.

When an EV needs to charge, it first sends a request including its PAT to the CSP. The latter authenticates anonymously the EV by verifying its pseudonym using the *pseudonym verification protocol*, and then it verifies the provided PAT. If the anonymous EV and its PAT are valid, the CSP sends back to EV a charging *coin chain* along with a customer secret key. This key is used by EV to establish efficiently *an authenticated pairwise key* with any charging pad. Each coin corresponds to a power charging unit, and their number in the chain depends on the amount value specified in the PAT.

When the EV arrives to the electric re-charging lane, it starts authentication process with the first charging pad by sending the first coin of the chain encrypted with the corresponding pairwise key. Coins are used in increasing order during the charging process. For each validated coin, the EV receives one power charging unit, and the coin gets saved by all the pads to prevent double spending. Note that, pads do not need to save all coins but only the last used coin. It is easy to detect double spending by only verifying the hash chain root and the last saved coin. In the final phase, the last coin with the associated EV pseudonym is sent to the CSP for billing and redemption, when the EV sends a termination notice or when the coin chain timeout is reached which means that the EV will no longer send other coins from this same coin chain. At the billing and redemption phase, the CSP sends to the bank the EV's PAT and the amount owed computed from the last coin sent by the pads.

It is important to note that, during all the dynamic charging and billing process, FLPA ensures that no one including CSP and charging infrastructure could identify the EV from either the PAT, coin chains or any other exchanged messages. In addition, as the PAT and coin chain are cryptographically bound to the associated pseudonym, no one should be able to use them other than the real holder of the corresponding pseudonym.

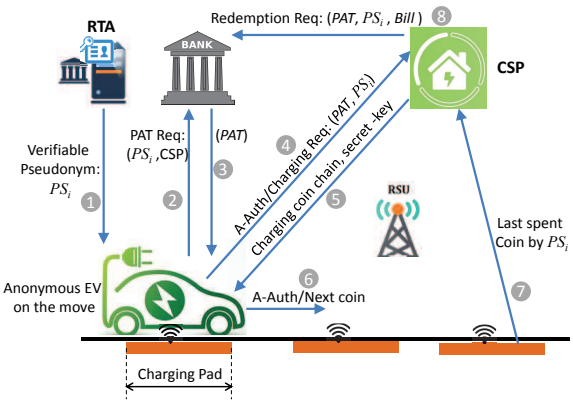

Fig. 1. FLPA architecture model (A-Auth: Anonymous authentication, PAT: Payment Authorization Token, RTA: Registration Trusted Authority)

B. Verifiable Pseudonyms Pre-distribution

To achieve EV privacy during authentication and charging process, we propose a pseudonym-based anonymity scheme based on the Camenisch's verifiable encryption method [9]. We assume an RTA to be responsible for managing the anonymity and the revocation of EVs. The RTA generates for each registered EV i a *verifiable pseudonym* PS_i. The RTA uses three private/public keys pairs $\{(x_1, Y_1), (x_2, Y_2), (a, A)\}$, where $x_1, x_2, a \in_R \mathbb{Z}_q$ (for prime q), $Y_i = g_i^{x_i}$ $(i = 1, 2)$, $A = g_2^a$, and g_1, g_2, g are generators of cyclic groups G_1, G_2, G respectively. A pseudonym PS_i is generated as a composite of two cryptographic functions. First, the real identity (ID_i) of EV i is signed by the RTA's secret-key x_2 based on Schnorr's scheme [12]. This produces a signature denoted PS_i', which is then encrypted by the RTA's public-key (Y_1) based on the verifiable encryption algorithm.

In this light, the pseudonym generation protocol for a given EV i is as follows:

- **Registration**
  - i generates a random secret $r_i \in \mathbb{Z}_q$, and computes $u_i = g_1^{r_i}$.
  - i transmits a pseudonym request, that includes its identity (ID_i) as well as the pseudonym's verification public parameters $(u_i, Y_1^{r_i})$, to the RTA.

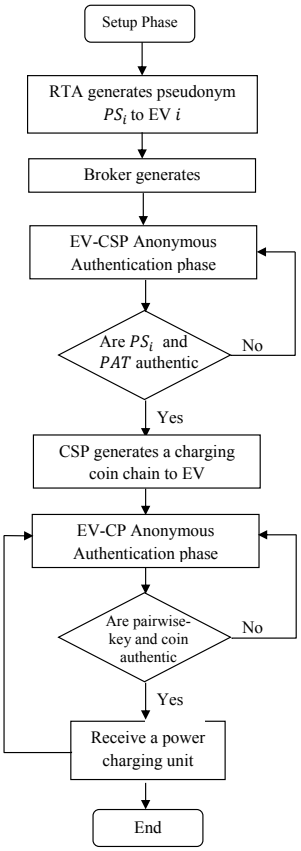

Fig. 2. Block diagram of proposed scheme

– The RTA verifies the validity of public parameter u_i as:

$$u_i^{x_1} =^? Y_1^{r_i} \tag{1}$$

- **Identity signature**
  - The RTA computes the following signature on ID_i:

$$PS_i' = x_2.H(ID_i||A) + a \tag{2}$$

- **Verifiable encryption of identity signature (PS_i')**
  - The RTA produces the verifiable pseudonym of EV i as follows:

$$PS_i = enc(PS_i')_{Y_1} = g_2^{PS_i'}.u_i^{x_1} = g_2^{PS_i'}.Y_1^{r_i} \tag{3}$$

The generated pseudonym meets the following properties : *Verifiability (Authenticity), Unforgeability, Unlikability* and *Traceability*.

Authenticity verification of generated pseudonyms is performed using our adapted version of the Camenisch's Proof of Knowledge protocol (PoK). Given the RTA's public parameters (Y_1, Y_2, A), our protocol, shown in Fig. 3, shows how a given EV i holding a pseudonym (PS_i, u_i) can prove to any other party (verifier) that its pseudonym is a valid RTA's signature of its identity, without, however, revealing it.

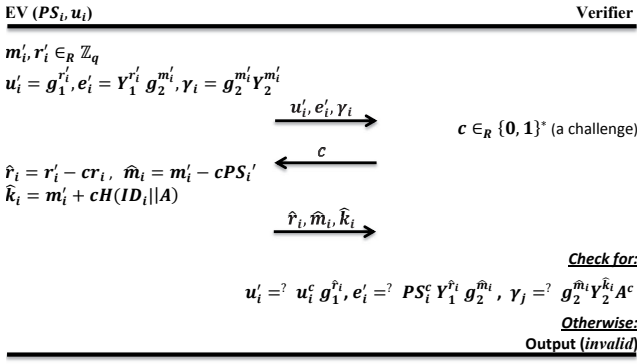

Fig. 3. PoK-based pseudonym's authenticity verification protocol

C. Payment authorization phase

When an EV needs to charge, it should connect to a bank (or a broker), which we denote as B, to request for a *Payment Authorization Token (PAT)* to a specified CSP x for a given amount M. Assuming that the bank has a private/public key pair (sk_B, pk_B).

As shown Fig. 4, when B receives the PAT Request (PATReq), that includes the EV's pseudonym PS_i, valid bank account details (acc_i), payment amount M, the CSP CSP_x, a session secret key k and a timestamp (T_B), it first verifies the authenticity of PS_i by executing the PoK protocol shown in Fig. 3. Then, B produces a PAT as a signature using its private-key $PAT = Sig_{sk_B}(PS_i, CSP_x, M, T_B)$ and sends it back to EV encrypted with the session key k. The token is then temporarily saved by B to prevent double redemption. As we can see, the token is linked to the pseudonym so that when it is used at the CSP, it provides no information about EV's real ID. In addition, the issued token is secure against reply and impersonation attacks, because our PoK protocol ensures that no one other than the real holder could prove the authenticity of the specified pseudonym and hence to validate the token.

D. Anonymous authentication and recharging permission

1) Anonymous authentication and token validation: In the first authentication phase, the EV authenticates anonymously to the CSP and validates its token (PAT) to obtain a recharging permission. In this phase, FLPA suggests a strong authentication mainly relying on the pseudonym verification based on a challenge-response proof of knowledge protocol.

In this regard, as shown in Fig. 5, the EV sends to the CSP a charging request $CReq$ that includes the PAT, the charging parameters cpm (e.g. battery type, level, etc.) and a secret session key k used to secure the communication from the CSP to EV, all encrypted with the CSP public-key sk_x. The anonymous authentication is based on the pseudonym verification where the EV should prove to the CSP that it is the holder of the pseudonym contained in the token without revealing

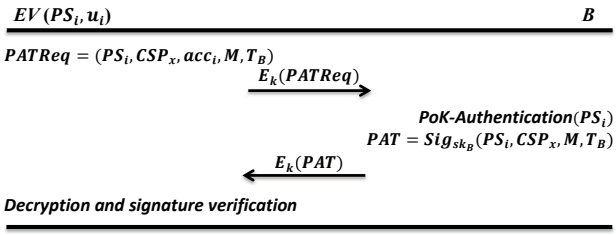

Fig. 4. PAT issuing

its real ID attributes. Therefore, the CSP authenticates the EV pseudonym by executing the *PoK verification protocol*, and then validates the token by verifying the token issuer signature $(Sig_{sk_B}(PS_i, CSP_x, M, T_B))$.

2) Recharging permission: If the authentication of EV succeeds, the CSP should generate the credentials necessary for the next authentication phase between EV and CPs. In that respect, the CSP first generates a recharging coin chain $C = (c_0, c_1, ..., c_N)$ of length N where $c_0 = H^N(c_N)$ is the root of the chain, and $H(.)$ is a private one-way hash function. Note that, the CSP generates the coin chain in reverse order by randomly picking the last coin c_N, and then computing $c_i = H(c_{i+1})$ for $i = 0, ..., N-1$. Each coin c_i is worth exactly one recharging unit, and their number N depends on the authorized amount M specified in the TAP. It may be determined from a function $f(M) = N$.

After coin chain generation, the CSP generates the pairwise-key parameters that will be used for authentication between EV and the CPs during the charging process phase.

Indeed, to allow fast and lightweight authentication between the EV and the charging pads, FLPA uses an authenticated pairwise-key scheme based on [10]. Under this bilinear pairing-based scheme, the EV uses an ephemeral customer secret-key s_i, generated by the CSP, to establish an authenticated pairwise-key with each of the charging pads. In this regard, the CSP uses a master private-key $s \in Z_q$, a master public-key $(P, P_x = sP \in \mathbb{G}_1)$ where P is a generator of $\mathbb{G}_1$, and public hash functions (H_1, H_2). Suppose that the CSP controls m charging pads denoted $CP_x = \{p_1, p_2, ..., p_m\}$. Each CP p_i is pre-loaded with a master secret-key $s_{p_i} = sQ_{p_i}$, where $Q_{p_i} = H_1(ID_{p_i})$, and a secondary random secret value $a_{p_i} \in Z_q$ where the associated public value is computed as $T_{p_i} = a_{p_i}P$.

The ephemeral customer secret-key of the EV is generated as $s_i = sQ_i$, where $Q_i = H_1(PS_i||TS_x)$ and TS_x is the timestamp associated to the current recharging session. This means that, EV could use s_i only for one recharging session.

As it is shown in Fig. 5, the CSP produces a charging permission *CPer* that includes the coin chain C, the signed root of the chain rt, the ephemeral customer secret-key s_i, the public values of CPs $(T_{p_1}, ..., T_{p_m})$ and the timestamp TS_x, all signed with sk_x and encrypted with the EV's session key k extracted previously from the PAT.

Note that, before providing a recharging permission, the CSP should check that provided token is not included in a Spent Token List (STL) stored locally, in order to prevent token double spending by selfish EVs. That said, each validated PAT is temporarily saved in the STL until billing.

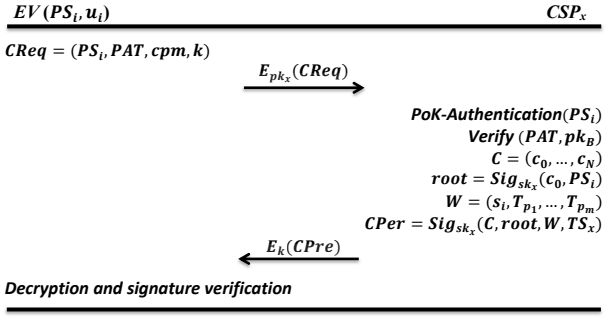

Fig. 5. Anonymous authentication and recharging permission

E. EV Charging process

In this phase, the EV authenticates to each of the CPs in the recharging lane to receive power charging from them, by using the credentials provided by the CSP. In this second authentication phase, FLPA uses a fast and lightweight authentication mechanism based on authenticated pairwise-key establishment and coin chains. In this regard, the EV successively reveals each coin of the chain, in increasing order starting from c_1, to the next CPs where each coin is worth one charging unit.

More precisely, as shown in Fig. 6, the EV sends to next CP p_j a single message including the next unspent coin c_l $(l \in [1, N])$ and the signed root rt along with a public value $T_i = a_i P$ where $a_i \in Z_q$ is a random secret value. The message is encrypted with the corresponding authenticated-pairwise key K_{i,p_j} that EV would have precomputed as:

$$K_{i,p_j} = H_2(a_i T_{p_j} || \hat{e}(s_i, T_{p_j}) \hat{e}(Q_{p_j}, a_i P_x)) \quad (4)$$

Similarly, the CP p_j computes its authenticated-pairwise key $K_{p_j,i}$ as:

$$K_{p_j,i} = H_2(a_{p_j} T_i || \hat{e}(s_{p_j}, T_i) \hat{e}(Q_i, a_{p_j} P_x)) \quad (5)$$

Where $Q_i = H_1(PS_i||TS_x)$ and TS_x is the timestamp extracted from signed root rt. Note that, by including the timestamp in computing Q_i, this ensures that EV cannot use

the current customer secret-key to achieve authentication in further charging sessions.

If the CP p_j is able to decrypt the received message with $K_{p_j,i}$, the EV is implicitly authenticated, because the suggested pairwise-key scheme ensures that no one other than the real holder of PS_i should be able to compute K_{i,p_j} used in encrypting the message. Then p_j transmits one power charging to EV, if the coin c_l is valid, that is if $H^l(c_l) = c_0$ and T_x is valid.

To prevent selfish EV from double spending of charging coins, each pad $p_j \in CP_x$ $(j = 1, ..., m)$ should save temporarily a Spent Coin Record $SCR = (PS_i||c_0||c_l)$ for each EV, where c_l is the last spent coin. Therefore, a double spending for a certain provided coin c_t is detected, if there exists a number n $(0 < n < l)$ where $H^n(c_l) = c_t$.

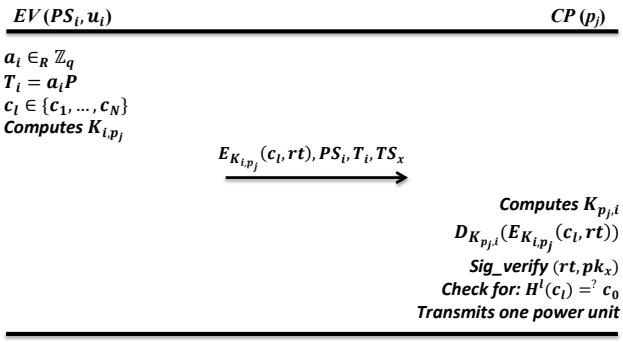

Fig. 6. EV charging phase

F. Billing and redemption

FLPA ensures fair billing, which means that the CSP bills the right customers for the received charging service, even if the EVs are charging anonymously.

Once the charging process is completed, the CPs transmit the billing information to the CSP for billing and redemption purposes. More precisely, billing is performed when the EV sends a termination notice to CPs, or when the coin chain timeout is reached, meaning that the EV could no longer send other coins from current coin chain. In that respect, the CPs send back to the CSP the last recorded SRC. Assuming that $SCR = (PS_i||c_0||c_l)$, the amount owed M' is computed by applying a function on the last spent coin included in the SRC as $M' = \pi(c_l)$.

At this stage, the CSP sends a redemption request to the bank including the EV's PAT along with billing information:

$$CSP \longrightarrow B: \quad E_{pk_B}(PS_i, CSP_x, Sig_{sk_x}(CSP_x, PS_i, PAT, M'))$$

III. Performance Analysis

In this section, we present the evaluation results of the proposed scheme based on MATLAB simulation. In this analysis, we compare our scheme to similar works, namely PBF [5] and Portunes [3], which we choose based on their relevance and significance. In our experiments, we consider the *communication/computation overhead* and the *authenticated charging efficiency* as evaluation metrics. We measure these metrics by focusing on the authentication phase between the EV and CPs during charging process, as it is the most important phase that has a direct impact on the charging efficiency in dynamic charging systems.

As simulation parameters, we use the standard 802.11p with 10 MHz channel bandwidth and 3-Mbps data transmission rate for wireless communication between EVs, RSUs, pads, and CSP. EVs are moving over the charging section at varied speeds ranging from 20 to 110 Km/h. The charging section consists of $m = 100$ pads which are 2m long and spaced by different random distances ranging from 1m to 10m. The transmission range is set to 100m.

A. Communication and computation overheads

As the EVs are charging while on the move, which means that the contact time between EV and CP is very short, it is important that the underlying authentication mechanism reduces the computation and communication overheads.

Communication overhead is measured as the amount of exchanged messages during EV-Pads authentication process. Table I shows that FLPA reduces the exchanged messages to a single message from EV to CP, which is more efficient compared to PBF and Portunes. On the other hand, the incurred computation load is measured in terms of the cryptographic operations necessary for the authentication between EV and CPs during the charging process. As we can see in Table I, our scheme is more computationally-efficient than PBF and Portunes. This is because our scheme achieves both authentication and privacy using lightweight cryptographic operations such as hashing and authenticated pairwise keys. In addition, most of authentication credentials are pre-computed by the EV before entering to the re-charging section.

It should be noted that, the optimization of communication and computation load will result in reducing the authentication delay, which is a major constraint for efficient EV dynamic charging system. Indeed, the delay includes the time taken by the EV and CPs to perform underlying cryptographic primitives (e.g. signature, verification, encryption, generation, etc.), the delay due to channel access and data transmission, backbone network delay, etc.

TABLE I
COMMUNICATION AND COMPUTATION OVERHEAD (H: HASHING, P: PAIRING, E/D: SYMMETRIC ENCRYPTION/DECRYPTION, V: SIG VERIFICATION, E_a/D_a: ASYMMETRIC ENCRYPTION/DECRYPTION, S: SIGNATURE)

	FLPA	**PBF**	**Portunes**
EV-Pad Auth computational cost	2H+2P +E+D+V	2H+2E_a +2D_a+3E+3D	2E+2D+2S +2V
EV-Pad communication cost	1 MSG	9 MSG	3 MSG

B. Authenticated charging efficiency

Since an EV should authenticate to the next CP before it can be charged, it is important to ensure a high successful authentication ratio for the range of EV speeds of interest in order to enhance the charging efficiency. Therefore, we measure the *Charging Efficiency Ratio (CER)* as the ratio of the number of successful EV-pad-authentications to the total number of CPs in the charging section. Many factors may have an impact on the successful EV-pad-authentication such as the distance between the EV and next pad as well as the EV's speed. Indeed, in order for an EV to authenticate successfully to the next pad, the time required for authentication, essentially due to messages exchange and cryptographic operations, must be less than the contact time between the EV and next CP. The contact time is equivalent to the travel time at the current speed of the EV.

Fig. 7 shows that the proposed scheme FLPA ensures better CER compared to BPF and Portunes for different EV's speeds varied from 20 to 110 (Km/h). As we can see, the increase of velocity does not deteriorate the charging efficiency within a charging section under FLPA, unlike other schemes where CER degrades from velocity=40 (Km/h).

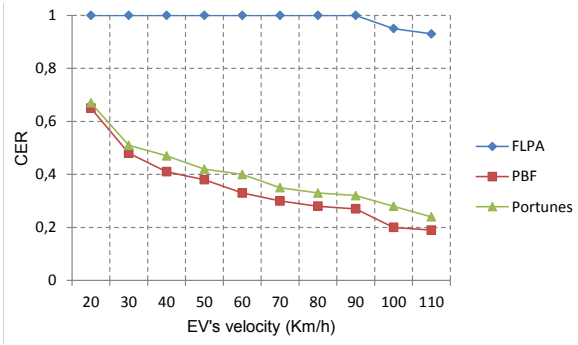

Fig. 7. Authenticated re-charging efficiency ratio

In order to study the impact of the charging section structure on the CER, we measured the Required Minimal Inter-Pads Distance (RMIPD) to have CER=100% for different velocity values. As it is shown in Fig. 8, our scheme requires only RMIPD=$1m$ even if the EV is moving at high speed, compared to PBF and Portunes which require both of them a large RMIPD for a high EV's speed. This also means that these schemes require a long electric re-charging lane. For instance, for 100 pads of $1m$ each, and EVs moving at 70 (Km/h), PBF and Portunes require approximately $2,8$ (Km) long charging lane, while our scheme require only $200m$ long charging lane.

IV. Conclusion

We have proposed in this paper an efficient privacy-aware authentication scheme for EV's dynamic charging. The proposed solution offers a twofold advantage: ensuring privacy of EV during power re-charging process and reducing the communication and computation load which guarantees fast and lightweight authentication. The suggested authentication mechanism allows EVs on the move to authenticate themselves to the CSP and charging pads while they still be anonymous, hence thwarting location tracking and profiling attacks. The evaluation results show the reliability and suitability to dynamic charging systems of our scheme.

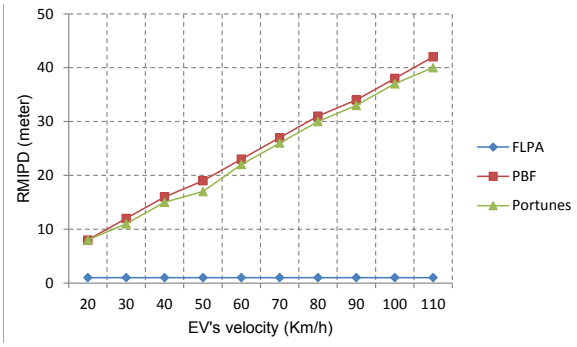

Fig. 8. Required Minimal Inter-Pads Distance (RMIPD)

References

[1] F. Musavi, M. Edington, and W. Eberle, "Wireless power transfer: A survey of ev battery charging technologies," in *2012 IEEE Energy Conversion Congress and Exposition (ECCE)*, Sep. 2012, pp. 1804–1810.

[2] H. Li, G. Dán, and K. Nahrstedt, "Proactive key dissemination-based fast authentication for in-motion inductive EV charging," in *2015 IEEE International Conference on Communications, ICC 2015, London, United Kingdom, June 8-12, 2015*, 2015, pp. 795–801.

[3] H. Li, G. Dan, and K. Nahrstedt, "Portunes+: Privacy-preserving fast authentication for dynamic electric vehicle charging," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2305–2313, 2017.

[4] K. Rabieh and A. F. Aydogan, "A fair and privacy-preserving reservation scheme for charging electric vehicles," in *2019 International Symposium on Networks, Computers and Communications, ISNCC 2019, Istanbul, Turkey, June 18-20, 2019*, 2019, pp. 1–6.

[5] R. Hussain, J. Son, D. Kim, M. Nogueira, H. Oh, A. O. Tokuta, and J. Seo, "PBF: A new privacy-aware billing framework for online electric vehicles with bidirectional auditability," *Wireless Communications and Mobile Computing*, vol. 2017, 2017.

[6] S. Gunukula, A. B. T. Sherif, M. Pazos-Revilla, B. Ausby, M. M. E. A. Mahmoud, and X. S. Shen, "Efficient scheme for secure and privacy-preserving electric vehicle dynamic charging system," in *IEEE International Conference on Communications, ICC 2017, Paris, France, May 21-25, 2017*, 2017, pp. 1–6.

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

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

[9] J. Camenisch and V. Shoup, "Practical verifiable encryption and decryption of discrete logarithms," in *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, 2003, pp. 126–144.

[10] N. P. Smart, "An identity based authenticated key agreement protocol based on the weil pairing," *IACR Cryptology ePrint Archive*, vol. 2001, p. 111, 2001.

[11] R. L. Rivest and A. Shamir, "Payword and micromint: Two simple micropayment schemes," in *Security Protocols, International Workshop, Cambridge, United Kingdom, April 10-12, 1996, Proceedings*, 1996, pp. 69–87.

[12] C.-P. Schnorr, “Efficient identification and signatures for smart cards,” in *Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology*. Springer-Verlag, 1990, pp. 239–252.