Privacy-Preserving Physical-Layer-Assisted Charging Authorization Scheme for EV Dynamic Charging System

Marbin Pazos-Revilla, Ahmad Alsharif, Surya Gunukula, Terry N. Guo, Mohamed Mahmoud, *Member, IEEE*, Xuemin (Sherman) Shen, *Fellow, IEEE*

***Abstract*—Dynamic charging system will enable moving electrical vehicles (EVs) to charge their batteries through magnetic induction by charging pads (CPs) placed on a portion of the roadbed. To realize such a system, the EVs need to communicate with the various parts of the system that include a bank, a charging service provider (CSP), road side units (RSUs), and CPs. In this paper, we propose a secure and privacy-preserving physical-layer-assisted scheme for dynamic charging systems to authenticate EVs and preserve the drivers' location privacy. We develop an efficient hierarchical authentication scheme that addresses the scalability nature of the system. Efficient cryptosystems are used to authenticate the EVs to the bank, CSP, and RSUs, but our evaluations indicate that the contact time of fast moving EVs and the CPs is too short to exchange multiple messages and execute time-consuming operations. Therefore, we develop an efficient physical-layer-based authorization scheme that utilizes autocorrelation demodulation and hypothesis testing to enable the CPs to identify and charge the authorized EVs. Through extensive analysis, simulation, and practical experiments, we demonstrate that the proposed scheme is secure against the considered attacks and can achieve full anonymity of the drivers' locations, fast authentication, and high authorization rate.**

***Index Terms*—Privacy preservation; secure wireless networks; fast authentication; electric vehicles; and dynamic charging.**

I. Introduction

Electric Vehicles (EVs) can reduce the dependency on fossil fuels and promote the adoption of intermittent renewable energy sources by acting as energy storage systems to store the energy produced by the renewable energy sources [1]. Due to such potential, many automotive companies have already begun to roll out EVs from their production lines [2]. Currently, more than 23,000 public charging stations have been deployed in the US and it is expected that fast-charging stations will be built on major highways [3]. Comparing to the time needed to fill the gasoline vehicles with gas, the EVs need much longer time to charge their batteries. Dynamic charging is a promising technology that can address this issue by enabling the EVs to charge while being driven [4]. This technology can also help drivers when their EVs do not have enough power to move to the nearest charging station to charge.

In dynamic charging systems, charging pads (CPs) are placed under a portion of the roadbed and an EV's battery is charged by magnetic induction while the EV is being driven over the CPs. The evaluations given in [5] demonstrate that the efficiency of the power transfer in dynamic charging systems can reach 75%. Each charging station in the dynamic charging system has a large number of CPs extended over a long distance (several miles) to allow the EVs to acquire enough amount of power while travelling within this distance. CPs should not switch on at all times because doing so not only wastes too much energy, but also charges all EVs that are driven on the road. Instead, CPs should switch on only when the EV that needs to charge is above it. Also, they should switch on only for the authorized EVs to prevent energy theft by unauthorized EVs. In order to realize such a system, the EVs need to communicate with the various parts of the system that include a bank, a charging service provider (CSP), road side units (RSUs), and CPs, without revealing the location information of the EVs.

In this paper, we propose a privacy-preserving physical-layer-assisted scheme to authenticate the EVs and preserve the drivers' location privacy. We develop an efficient and scalable hierarchical authentication scheme. A combination of efficient cryptosystems are used to authenticate the EVs to the bank, CSP, and RSUs. However, our evaluations have demonstrated that the contact time of fast moving EVs and the CPs is too short to exchange multiple messages or execute complex schemes. Therefore, we develop an efficient physical-layer-based authorization scheme that utilizes autocorrelation demodulation and hypothesis testing to enable the CPs to identify the authorized EVs and charge them.

Our main contributions and the challenges the paper aims to address can be summarized as follows.

- We propose a novel scalable system that addresses security, location privacy, and also efficiency in EV dynamic charging system. The proposed scheme can achieve full anonymity where no entity or even colluding entities can know the drivers' locations. Comparing to the existing works, the proposed schemes in [6]–[8] do not address privacy and the CSP is trusted to know the EV's locations in [9], [10].
- In order to consider the scalability and the large geographic area of the dynamic charging system, we de-

M. Pazos-Revilla, A. Alsharif, S. Gunukula, and M. Mahmoud are with the Department of Electrical and Computer Engineering, Tennessee Tech. University, Cookeville, Tennessee, 38505, USA. E-mail: mpazos@tntech.edu, ahalsharif42@students.tntech.edu, sgunukula43@students.tntech.edu, and mmahmoud@tntech.edu

T. Guo is with Center for Manufacturing Research, Tennessee Tech University, Cookeville, TN 38505, USA. E-mail: nguo@tntech.edu

X. Shen is with Department of Electrical and Computer Engineering, University of Waterloo, Canada. E-mail: xshen@bbcr.uwaterloo.ca.

Manuscript received XXX, XX, 2017; revised XXX, XX, 2017.

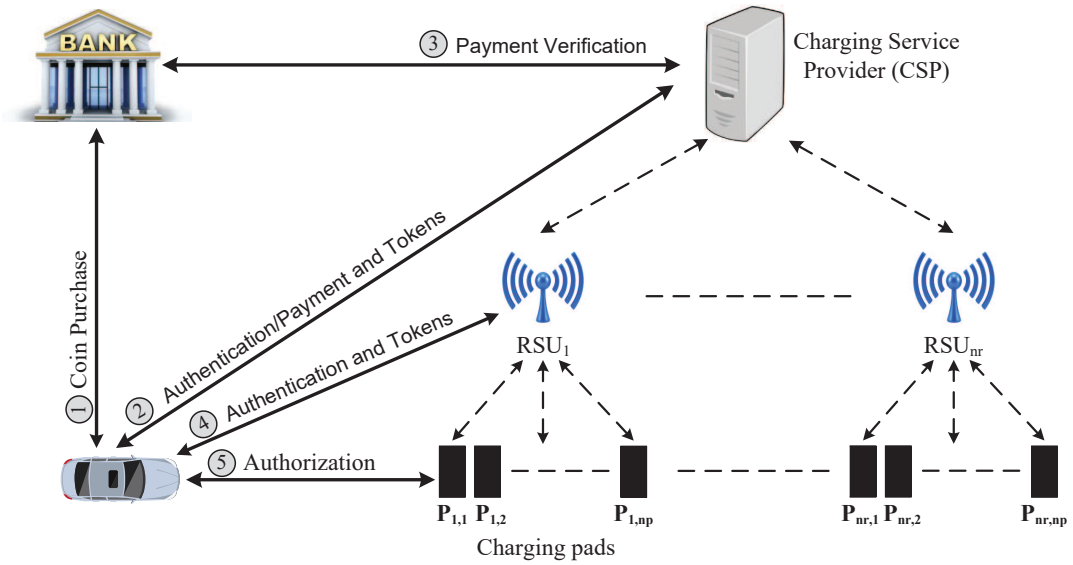


Fig. 1. The network model.

velop a hierarchical authentication approach that uses lightweight cryptosystems. The main idea is that when an EV authenticates to the CSP, the CSP sends secret keys (called tokens) shared with the RSUs to enable the EV to efficiently authenticate to the RSUs. Similarly, each RSU sends secret tokens shared with the CPs to enable the EV to efficiently authenticate to the CPs. Comparing to the proposed schemes in [9], [10] that require each CP to store all the pseudonyms and keys including the ones that may be used at other stations and CPs, the CPs and RSUs in our scheme calculate and store only the keys they use in their communications.

- Cost-effective CPs may have limited computational power, and therefore the CPs may not be able to run extensive-computation cryptosystems or exchange several messages during the short period of time available for communication between CPs and the EV. In order to address this challenge, we develop a physical-layer-based authorization scheme that is run at the physical layer and uses the shared secrets between the EVs and CPs.
- Simulations, analysis, and practical experiments are conducted to evaluate the proposed scheme. The results indicate that the scheme can preserve location privacy and is efficient and secure against the attacks listed in section II.

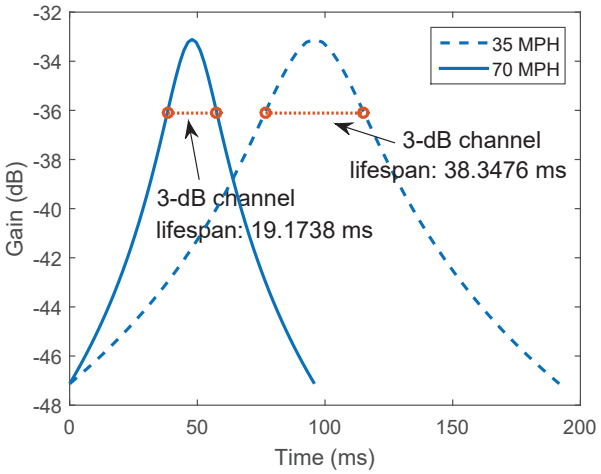
The remainder of the paper is organized as follows. The network and threat models and the main challenges/requirements are discussed in section II. Detailed description of the proposed scheme is covered in section III. The performance evaluations are discussed in section IV, while privacy and security analysis is given in section V. Finally, the related works are discussed in section VI, and conclusions are drawn in section VII.

II. Preliminaries

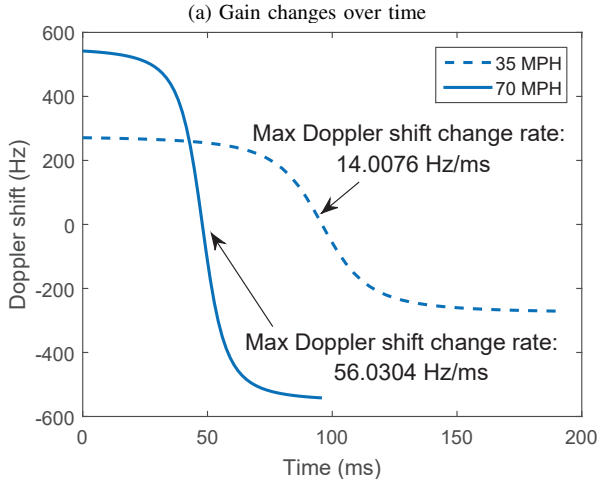
A. Network and Threat Models

As illustrated in Figure 1, the network model has a bank, a charging station, and EVs. Each charging station can be extended to several miles, and it has a CSP, RSUs, and CPs. The RSUs are access points that are deployed on the road along the charging section, whereas the CPs are the elements that charge the EVs using electromagnetic induction. Each CP can charge only one EV at a time. The EVs and CSPs can communicate with the bank, e.g., using the Internet. Each CSP can communicate with all RSUs in the charging station, and each RSU can communicate with a number of CPs. Also, EVs can communicate with CSPs and RSUs using wireless communication, whereas the communication with the CPs is achieved by using a dedicated short range wireless communication device installed at the bottom of the EVs. Each EV maintains an account in the bank and uses the account to buy anonymous coins that are used to pay for charging and anonymously authenticate the EV to the CSP. Moreover, the CPs need to authenticate the EVs to charge only the authorized EVs.

For the threat model, the proposed scheme aims to preserve drivers' location privacy and secure the payment and the authentication. For privacy, we consider a strong adversary model assuming that the attackers include the CSP, the RSUs, the CPs, the bank, EVs, and external eavesdroppers. The attackers aim to learn the drivers' locations. They also aim to link the packets sent from the same EV so that if the attacker manages to know the real identity of the EV, it can learn much location information about the driver. For the payment, we consider the attacks that aim to charge without pay or with less payment. To do that, the attackers may try to buy coins without payment, e.g., by impersonating other EVs. They may also try to forge coins and double spend valid coins. The attackers can also attack the authentication scheme to charge for free, e.g., by launching replay attacks and reusing



(a) Gain changes over time



(b) Doppler shift changes over time

Fig. 2. EV-CP channel characteristics with half-omni-directional antennas.

old authentication tokens. These attacks can be launched by external attackers and internal EVs, and the attackers can collude or work individually.

B. Challenges and Requirements

1) Security, Privacy, and Efficiency: Considering that the number of EVs is very large and their charging needs can reach over several miles of roads, the scalability of the system can make the design of the security scheme a real challenge. Furthermore, the conflicts between security and privacy also complicate the problem. To elaborate, the real identities should be used to secure the payment, but they should not be used to preserve privacy. Using certified pseudonyms to preserve privacy imposes extra overhead for issuing, renewing, and revoking certificates [9], [10]. Instead, the anonymous coins in our scheme, are designed to support efficient payment, anonymous authentication, and key establishment. Also, to address the scalability of the dynamic charging system, hierarchical authentication scheme is developed, where the EVs should first authenticate to the CSP, and then to the RSUs and CPs.

2) EV-CPs Authorization: The wireless communication channel between the EVs and the CPs is used to enable the EVs to authenticate themselves so that the CPs can only charge authorized EVs. This channel is quite unique and highly dynamic when compared to those in commonly known wireless scenarios such as cellular, WiFi, and radar applications that are not optimally designed to address short range and extremely dynamic channel between the EV's transmitter and the CP's receiver.

In order to estimate the characteristics of the EV-CP channel, we used the path loss model [11]. We considered an EV moving at an average speed of 35 and 70 mph, a distance of 12 inches between the EV and the CPs, and transmitter (at EV) and receiver (at CP) antennas with the same radiation pattern and equal gain within the half sphere. The estimated channel behaviour is shown in Figure 2, where the 3-dB channel lifespan is 38.35 ms at 35 mph and 19.17 ms at 70 mph, while the maximum doppler shift change rate is about 14 Hz/ms at 35 mph and 56.03 Hz/ms at 70 mph.

These results demonstrate that it is extremely difficult to complete carrier frequency recovery to demodulate the signal in such a short window of time, and achieve smooth handover communication transitions from one charging pad to another. This suggests that for the communication between the EVs and the CPs, *non-continuous burst communication mode with non-coherent modulation/demodulation scheme* should be considered because it shows low sensitivity to channel gain changes and requires neither channel estimation nor synchronization at carrier and symbol levels, thus reducing the requirements for signal recovery and the timing constraints for a final authorization decision. The results also indicate that it may not be possible to use extensive cryptosystem or even exchanging several messages.

III. Proposed Scheme

A. Overview

As illustrated in Figure 1, the first phase in our scheme is the purchase of anonymous coins from the bank. The coins are used for authenticating the EV to the CSP, payment, and establishing a shared symmetric key with the CSP. In this phase, an EV should use its real identity which is necessary to pay from its bank account. Coin purchase does not need to be done right before charging. Instead, EVs can purchase coins at any time and store them to be used later when charging is needed. When an EV needs to charge, it sends the anonymous coin to the CSP which contacts the bank to ensure that the coin has not been used before. The bank cannot link the coin to the EV that bought it to preserve location privacy. Then, the CSP sends secret keys (called tokens) shared with the RSUs to the EV. The EV uses these tokens to authenticate to the RSUs. Similarly, each RSU sends to the EV time-based one-time tokens (TOTs) shared with the CPs controlled by that RSU. The TOTs are secret tokens that have a short lifespan for utilization and can be used only once. The EV uses the TOTs to authenticate to the CPs to get charged. During EV-CPs authorization phase, a TOT is sent to the CP and the authorization is completely done at the physical layer. Finally, electric charge is delivered to the EV if the authorization is successful.

B. Purchasing of Coins

Each EV should contact the bank to buy coins to use when it needs to charge. In this communication, the EV should use

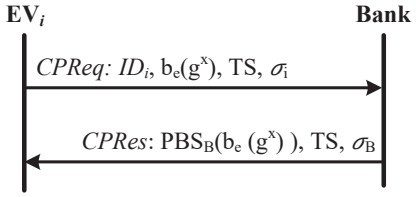


Fig. 3. Anonymous coin purchase.

its real identity so that the payment can be deducted from its bank account. Partial blind signature [12] is used to compute the coins so that when the EV uses the coins at a charging station, the bank cannot link the coin to the EV that bought it to preserve the location privacy of the EV driver.

Initially, a multiplicative cyclic group $\mathbb{G}$ of prime order p is generated by the bank, where g is the generator of $\mathbb{G}$. Figure 3 gives the exchanged messages during the coin purchase phase. When an EV$_i$ needs to buy a coin, it first selects a secret random number x and computes g^x. Then, it blinds g^x using a secret value to produce $b_e(g^x)$ and sends a *Coin Purchase Request (CPReq)* to the bank. As shown in the figure, the *CPReq* packet has the real identity of the EV (ID_i), $b_e(g^x)$, timestamp (TS), and signature (σ_i).

After receiving the *CPReq* packet, the bank first verifies the timestamp and the signature. Then, it checks the account of EV$_i$ to make sure that it has enough money to pay for the coin. The bank deducts a specific amount of money from EV$_i$'s account and uses a partial blind signature scheme to sign $b_e(g^x)$ along with the issuing date of the signature. This date will be used later to efficiently check whether the coin has been spent before. It is common that many EVs contact the bank to purchase coins every day. Thus, the issuance date of the coin cannot be used by the bank to link a coin to a buyer when the coin is used. Finally, the bank sends a *Coin Purchase Response (CPRes)* packet to EV$_i$. As shown in the figure, the packet has the partial blind signature $(PBS_B(be(g^x), date))$, TS, and a regular signature (σ_B).

After receiving the *CPRes* packet, the EV should verify the timestamp and the bank signature. Then, it unblinds the partially blind signature to obtain the bank signature on g^x and date, as follows.

$$Sig_B(g^x, date) = b_e^{-1}(PBS_B(b_e(g^x), date)) \quad (1)$$

Later, when EV$_i$ needs to charge, it can use the anonymous coin given in Equation 2 to pay and authenticate to the CSP.

$$Anonymous\ Coin = g^x, date, Sig_B(g^x, date) \quad (2)$$

We assume that each coin has a specific monetary amount and is sufficient to charge from a certain number of CPs. This coin can prove that EV$_i$ has paid and it is a legitimate member in the system because it has to compute a signature to buy the coin. Due to using blind signature, the bank cannot link the anonymous coin in Equation 2 to the real identity of the EV that purchased the coin.

C. Charging Request and Hierarchical Authentication

When EV$_i$ needs to charge from a charging station, it should contact the CSP to authenticate, pay, and establish a shared key to secure the communication between them. As shown in Figure 4, EV$_i$ sends a charging request packet that has g^x and the CSP selects a secret random value y and computes a shared key $k = g^{xy}$. Then, it sends g^y, the encryption of the concatenation of g^y and g^x using the key k ($E_k(g^x, g^y)$), and its signature (σ_C). $E_k(g^x, g^y)$ can prove to EV$_i$ that the CSP calculated the correct key. After receiving the message and verifying the CSP signature, EV$_i$ calculates the shared key ($k = g^{xy}$) using its secret x and the received g^y, and then, it uses the key to encrypt the anonymous coin and sends the ciphertext to the CSP which in turn decrypts the ciphertext and verifies the bank signature. After that, the CSP sends the coin to the bank to make sure that it has not been used before and also to deposit the payment in the CSP's account. The bank first hashes the coin's signature and searches a table that stores the hashes of used coins' signatures. The bank can use the coin's issuance date to shorten the search space. If the bank does not find the coin in the table of used coins, it adds the hash of the coin's signature to the table and informs the CSP that the coin is valid. In this case, the CSP uses the shared key with EV$_i$ to encrypt a set of secret tokens that enables EV$_i$ to authenticate to the RSUs. To reduce the communication overhead, the CSP can send only one token and EV$_i$ can use iterative hashing operations, e.g., using MD5 or SHA, to compute the rest of the token locally. Each coin should be enough to charge from a certain number of CPs. To simplify our description, we assumed that an EV spends only one coin, but it can send multiple coins to the CSP if it needs to charge from a larger number of CPs.

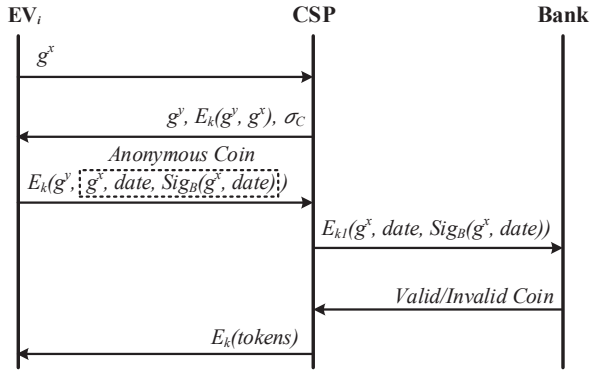


Fig. 4. Charging request.

In order to consider the scalability and the large geographic area of the dynamic charging system, we use a hierarchical authentication approach that uses lightweight cryptosystems. The idea is that the CSP should share a set of secret tokens with each RSU and each RSU should share a set of TOTs with the CPs under its control. This can be done offline, e.g., one time in each day. The EV can use the shared tokens with RSUs, received from the CSP, to authenticate to each RSU, e.g, using any challenge/response technique such as the efficient ones that use keyed hash functions [13]. This authentication is efficient because of the use of pre-shared symmetric keys (tokens) and lightweight hashing operations. After this level of authentication, the EV should receive a set of TOTs from

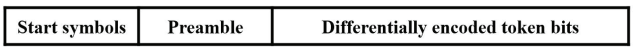


Fig. 5. TOT frame.

each RSU that are needed to authenticate the EV to the CPs controlled by the RSU. The communication overhead can be reduced if the RSU sends only one TOT and EV_i uses iterative hashing operations, e.g., using MD5 or SHA, to compute the remaining TOTs locally.

D. Physical-Layer-Based Authorization

The short contact time between the EVs and the CPs and the low computation power of the CPs necessitate developing a very fast authorization scheme. Therefore, multiple rounds of packet transmissions, computationally intensive cryptosystems, and techniques like error control and correction may be hard to use. In our scheme, since each EV shares secret TOTs with CPs, the EVs can just send the TOT shared with each CP, and the authorization verification can be done only at the physical layer. However, in order to ensure security and reliability, the communication system should be designed to ensure that the probability of receiving the TOT is very high at different weather conditions. This is because the EVs do not charge if the TOTs are not received. Also, we should ensure that the attackers cannot intercept the TOTs and use them. Based on these requirements and the results given in section II, *non-continuous burst communication mode with non-coherent modulation/demodulation technique* is recommended to be used between the EVs and the CPs. Autocorrelation demodulation (ACD) [14], also called differential transmitted reference (DTR) [15], is such a technique that meets these requirements.

We propose using ACD rather than other non-coherent schemes such as On-Off Keying because ACD does not need a threshold for demodulating the soft-bit stream. Adjusting demodulation threshold requires measuring signal and noise strengths and this threshold should be re-adjusted for every EV which is impractical to implement in our application. Along with the ACD, a supporting hypothesis testing algorithm will be used. In this manner the system can achieve a high rate of successful authorizations of EVs with valid TOTs. Moreover, multi-symbol detection can be combined with ACD to achieve a better error-rate performance [14]. Because the channel sets a very short window of time for reliable communications, it imposes the need for a design without real-time automatic gain control circuitry to adjust the gain at the receiver in response to the amplitude changes in the received signal, and instead, an amplitude normalization algorithm will be applied to each demodulated waveform via post processing.

We propose a joint authorization scheme that exploits channel diversity in frequency and time to provide high rate of successful authorizations. Consider that the EV transmitter and the CPs' receivers support N frequency tones. N consecutive TOTs shared with N successive CPs in front of the moving EV are transmitted in parallel at the same time. The EV creates a physical-layer frame consisting of a frame head, a preamble, and a payload of a differentially encoded TOT as shown in Figure 5. The frame head serves as TOT frame start indicator, and the preamble is used to find bit timing by the receiving CP before the TOT is decoded. This frame is transmitted to the CP that is equipped with a frame-head detector, and a bit-timing unit using preamble correlation. Also, each CP is equipped with N ACD receivers and maintains a pool of n TOTs shared with the RSU.

Our scheme can work with one tone $(N = 1)$ for which the corresponding communication model is shown in Figure 6, or the scheme can support N tones. To simplify our description, let's consider a system that uses two tones f_1 and f_2, i.e., $N = 2$, as illustrated in Figure 7 where the CPs are connected in series; that is, each CP (except the first and last ones) is connected to its preceding and following CP, and hard-wired connections between consecutive CPs allow fast communication between them. The joint decision function box shown in Figure 7 contains three units: equal-weight combiner, amplitude normalizer and hypothesis decision unit, where the most relevant of the three in regards of authorization is the hypothesis decision unit and Θ_k which is the decision threshold that is pre-determined for sufficiently low false and unsuccessful authorization rates.

The following steps summarize the authorization process between EV_i and CP_k.

1) The beacon transmitter of CP_k signals EV_i about the start of a new round of transmission.
2) Upon receiving a beacon signal from CP_k, EV_i transmits two TOT frames containing the TOTs $\tau_{i,k}$ and $\tau_{i,k+1}$ which are shared with CP_k and CP_{k+1}, respectively. Both TOTs are transmitted simultaneously, i.e., the TOT $\tau_{i,k}$ is transmitted on frequency tone f_1 while the TOT $\tau_{i,k+1}$ is transmitted on frequency tone f_2.
3) After receiving the TOT frames, CP_k demodulates the received TOT waveforms, i.e., the 2-tone ACD receiver at CP_k outputs two discrete-time waveforms $W_{i,k}^{(1)}$ and $W_{i,k+1}^{(2)}$ which are amplitude-varying and noisy versions of $\tau_{i,k}$ and $\tau_{i,k+1}$.
4) CP_k now has received three discrete-time waveforms; $W_{i,k}^{(1)}$ and $W_{i,k+1}^{(2)}$ received from EV_i, and $W_{i,k}^{(2)}$ received from CP_{k-1}. Equal-weight combining of the current received waveform $W_{i,k}^{(1)}$ and the previously received one $W_{i,k}^{(2)}$ is done to produce $\tilde{\tau}_{i,k}$ which can be viewed as a "soft-bit" stream of the transmitted token $\tau_{i,k}$.
5) A hypothesis decision is performed against n TOTs of the CP_k's token pool, through the following steps.
   (a) The amplitude of the estimated TOT $\tilde{\tau}_{i,k}$ is normalized to $\rho(\tilde{\tau}_{i,k})$ where $\rho(\ )$ is a function representing amplitude normalizer.
   (b) Correlations decision variables r_m are calculated by

$$r_m = \langle \rho(\tilde{\tau}_{i,k}), \tau_{m,k} \rangle,\ 1 \le m \le n \tag{3}$$

   where $\langle \rho(\tilde{\tau}_{i,k}), \tau_{m,k} \rangle$ is the inner-product operation of the estimate $\tilde{\tau}_{i,k}$ and the TOT $\tau_{m,k}$.
   (c) The hypothesis decision is to find a decision variable r_m that is greater than the threshold Θ_k, and take the largest one found as an outcome. The hypothesis decision is either $\mathcal{H}_m$ (TOT m passes authorization)

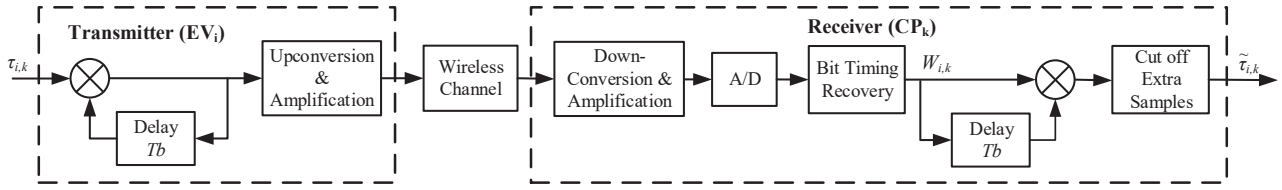


Fig. 6. Single-tone communication model.

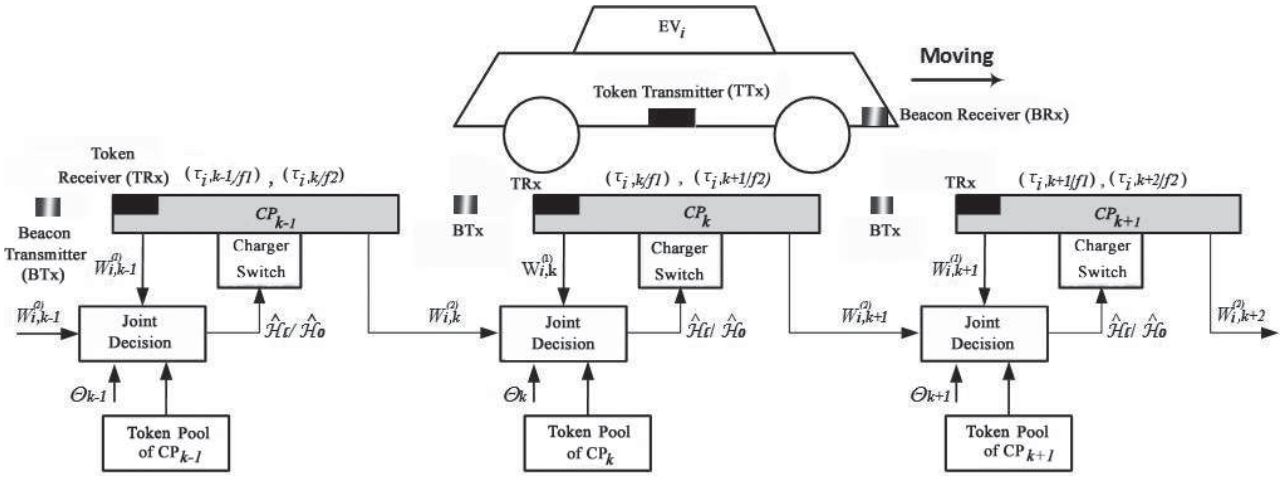


Fig. 7. Multi-tone multi-pad joint authorization process.

or $\mathcal{H}_0$ (no TOT passes authorization) and can be expressed as

$$\begin{cases} \mathcal{H}_m: & if\ r_m \geq \Theta_k,\ and\ r_m > r_{i'} \\ & \quad i' = 1, 2, \cdots, n,\ i' \neq m \\ \mathcal{H}_0: & if\ r_m < \Theta_k,\ m = \{1, 2, \cdots, n\} \end{cases} \tag{4}$$

Because of the noise embedded in the currently received $W_{l,k}^{(1)}$ and the previously received $W_{l,k}^{(2)}$ that are received at different frequencies and times, they tend to be statistically independent, thanks to the diversity in both frequency and time. In other words, *when the signal quality is occasionally bad, we can expect performance (measured in receiver operating characteristic, or ROC) improvement by combining signals received at two separate locations*. The diversity level can be continuously increased as N increases, at the cost of increased system complexity.

IV. Performance Evaluation

In this section, we present the evaluation results of our physical-layer-based authorization scheme under different conditions including EV speed, TOT transmit power, detection threshold (Θ), and environmental conditions.

A. Metrics

In our evaluations, we measure the following metrics.

1) *Authorization Success Probability (P_S).* This is the probability that the valid TOT $\tilde{\tau}_{i,k}$ sent by EV_i is matched to one of the locally stored n TOTs in CP_k. The higher P_S, the better our scheme is. We define P_S conditioned on the hypothesis decision $\mathcal{H}_i$ as follows.

$$P_S = P(r_i \geq \Theta,\ r_i > r_{i'},\ 1 \leq i' \leq n,\ i' \neq i\ |\mathcal{H}_i) \tag{5}$$

2) *Missed Authorization Probability (P_M).* This is the probability that a valid TOT $\tilde{\tau}_{i,k}$ sent by an EV does not match any of the locally stored n TOTs in a CP, i.e., all the decision variables are below the threshold Θ. The lower P_M, the better our scheme is. Obviously, the summation of P_M and P_S should always equal to one. We define P_M conditioned on $\mathcal{H}_i$ as follows.

$$P_M = P(r_{i'} < \Theta,\ 1 \leq i' \leq n\ |\mathcal{H}_i) \tag{6}$$

3) *False Authorization Probability (P_F).* This is the probability that the invalid token $\tilde{\tau}_{i,k}$ is mistakenly accepted, i.e., falsely matched to $\tau_{m,k}$ where $i \neq m$. The lower P_F, the better our scheme is. We define P_F conditioned on $\mathcal{H}_i$ as follows.

$$P_F = P\left(\bigcup_{\substack{1 \leq m \leq n \\ m \neq i}} \{r_m \geq \Theta,\ r_m > r_{i'},\ 1 \leq i' \leq n,\ i' \neq m\}\ |\mathcal{H}_i \right) \tag{7}$$

B. Experiment Setup

In our experiments, we used MATLAB to simulate our scheme. We assumed that the pad beacon and the TOT frame head can be detected at detection probability of one, and a perfect bit timing can be obtained. We also consider EV speed to be either 35 or 70 mph, and carrier frequencies between 5 GHz and 6 GHz. This range of frequencies is selected for

TABLE I
EXPERIMENT PARAMETERS AND THEIR CORRESPONDING VALUES.

Parameter	Value
Carrier frequencies	5 GHZ to 6 GHZ
Antenna beamwidth	30°
Antenna gain	3.5 dBi
Receiver noise figure	7 dB
Bit rate	1 Mbps
Pulse shaping	Root Raised Cosine with roll-off factor 0.5
TOTs pool size	100
Tx/Rx separation	1 foot

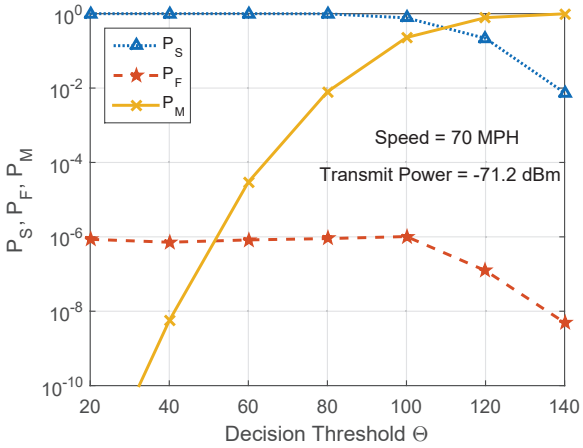


Fig. 8. The impact of the decision threshold (Θ) on P_S, P_M, and P_F at -71.2 dBm transmission power.

the following reasons. First, the spectrum in this range is less crowded compared to the lower frequency bands. Second, the values of the frequencies are not very high, so RF circuits can be relatively built easier. Finally, within this frequency range, the antennas' sizes are very small. Table I summarizes the parameter settings considered in our experiments.

The value of Θ should have a direct impact on the performance metrics, and thus it is important to select a good value for Θ. It can be observed from Figure 8 that the values of Θ between 20 and 80 should be selected to achieve high P_S while maintaining very low P_F and P_M. In this range, P_S is almost one and P_F and P_M are almost zero. Figure 8 was computed at TOT transmission power of -71.2 dBm. Similarly, a good value for Θ can be determined at any other power level.

C. Experiments' Results

The ROC curves at two power levels (-71.5 dBm and -72.5 dBm) are depicted in Figure 9. Tokens, computed using SHA-256, are used for authorization and the EV speed is 70 mph. For clarity, we have included a fine logarithmic plot (inner figure) with the linear plot (outer). From the plots, it can be observed that with power level of -72.5 dBm, the successful authorization rate, P_S, is higher than 0.9 with very low false authorization rate, P_F. Moreover, the performance of the authorization scheme significantly improves with just a slight increase in the transmitted power as seen in the plot

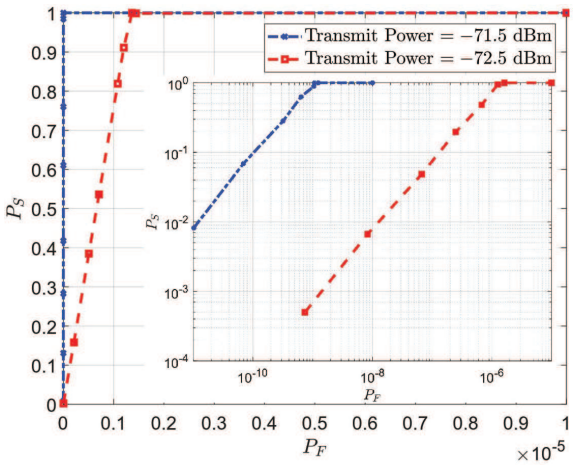


Fig. 9. ROC curves at different transmit power with SHA-256 token at 70 mph.

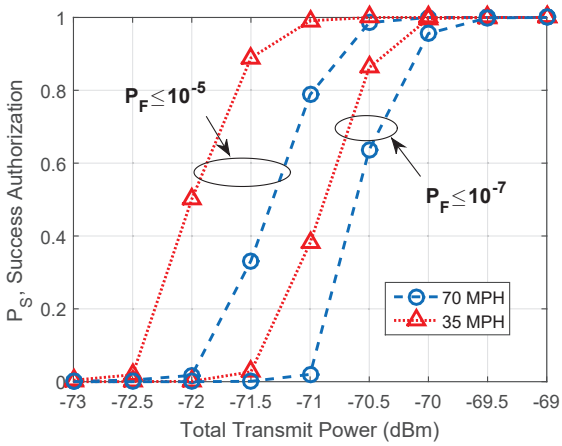


Fig. 10. P_S vs. transmit power.

of the -71.5 dBm. As shown in the inner plot, P_F values are maintained at extremely low levels, reaching the value of 10^{-11} at -71.5 dBm, which could be achieved when low ranges of values of detection threshold are used, as indicated by Figure 8.

Figure 10 gives P_S at different values of TOT transmission power, where the TOTs are computed by using SHA-1. It can be observed that perfect P_S with P_F that is no greater than 10^{-7} can be achieved if the transmit power level is above -69 dBm at a pre-selected value of θ. Also, the increase of the transmission power can reduce P_F and eliminate the reduction in P_S due to the increase in the EV speed. Based on our simulations, high level of authorization rate performance can be achieved within 2 ms using SHA-256 tokens with transmission rates of 1 Mb/sec and EV speed of 70 mph.

Since the TOTs can have different lengths when computed by different hashing algorithms, Figure 11 gives P_S versus transmit energy for MD5, SHA-1 and SHA-256 hashing algorithms. It can be observed that the longer the TOT, the more transmit energy is required to achieve the same value of P_S. Also, the transmission power and energy in Figure 11 and Figure 10 are small because the distance between the transmitter and the receiver is short.

Furthermore, to assess the robustness and reliability of our authorization scheme under various environmental conditions, practical experiments were conducted using layers of wa-

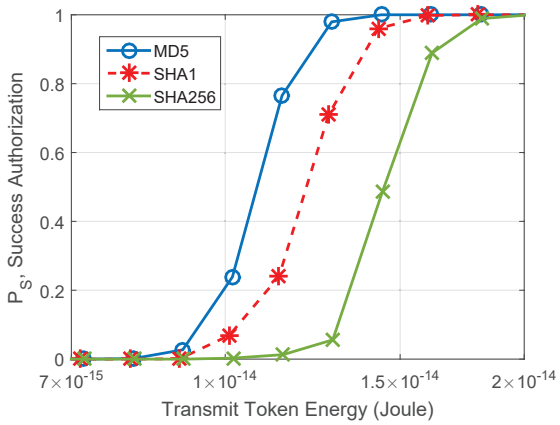


Fig. 11. P_S vs transmit TOT energy for different hashing algorithms at $P_F \leq 10^{-5}$.

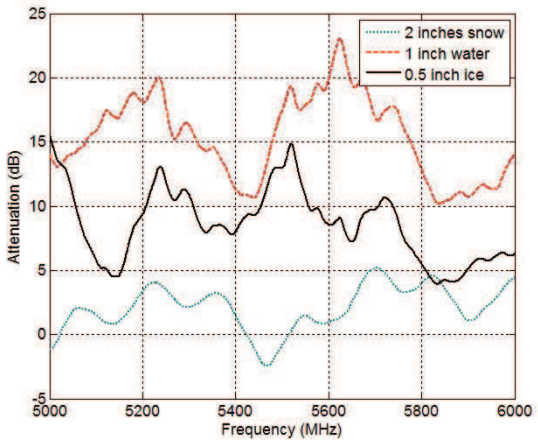


Fig. 12. Impact of environmental conditions on our scheme.

ter, snow, and ice in order to measure the attenuation in the transmitted TOTs. In our experiments, various layers of the previously mentioned materials were placed between the transmitting and receiving antennas with a surrounding RF insulating foam to prevent interference from other RF signals. Figure 12 gives the attenuation levels at different frequencies. It can be observed that the water experiences an average level of attenuation of about 15 dB and a maximum attenuation of 23 dB in the range of frequencies between 5 and 6 GHz. On the other hand, the attenuation level reaches a maximum of 5 dB using 2 inches of snow within the same range of frequencies while the maximum measured attenuation was 15 dB for the 0.5" ice layer.

To maintain the high performance of our scheme under different environmental conditions, the transmit power should be adjusted. For example, Figure 10 shows that when an EV transmits tokens at -69 dBm under clear weather conditions, P_S is almost one, but, this transmit power should be increased to overcome the attenuation due the environmental conditions. For instance, to overcome the expected worst attenuation of 23 dB due to the water layer, an EV must transmit tokens at -46 dB instead of -69 dB. Similarly, it should transmit at -64 dBm and -56 dBm to overcome the 2" snow layer attenuation and the 0.5" ice layer attenuation, respectively.

V. Security and Privacy Analysis

In this section, we analyze the security and privacy of the proposed scheme against the attacks considered in the threat model. We highlight the privacy/security features of our scheme, and provide an experimental analysis and evaluation to the potential threats caused by jamming and/or eavesdropping attacks on the physical-layer-based authorization scheme.

A. Privacy preservation

Identity Anonymity. In our scheme, the EVs use anonymous coins for payment and authentication. The coins cannot be linked to the EV that bought them due to using blind signature. To elaborate, the real identity of an EV is used only during the purchase of coins which is necessary to clear the payment. However, when a coin is sent by a CSP to the bank for double spending check, the bank cannot link the anonymous coin to an EV to preserve location privacy, assuming that each CSP has a known location. This is because the bank cannot link g^x of the coin to the blinded value $b_e(g^x)$ sent during the coin purchase phase. As a result, our scheme provides full anonymity where no one entity or even colluding entities can link a coin used by an EV to its real identity.

Coins and Charging Requests Unlinkability. Neither the bank nor the CSP can link different coins and charging requests sent by the same EV at different occasions, and thus they cannot know that they are sent from the same EV. This is because coins have one-time random numbers (x) that are not linkable and can make the coins different.

B. Security of EV communications with Bank, CSP, and RSUs

Double Spending. When an EV submits a signed coin to the CSP, the CSP sends it to the bank to make sure that the coin has not been used before. Because the bank maintains a list of used coins as mentioned in subsection III-C, our scheme can thwart double spending attacks when an EV tries to reuse a coin.

Forging Coins. In order to forge coins, the attacker should be able to compute a valid signature of the bank. This is impossible because it needs the private key of the bank.

Purchasing Coins Without Payment. When an EV purchases coins, it has to use its real identity so that the bank can make sure that it has enough money to pay for the coins. An EV cannot impersonate other EVs to obtain coins without payments because it has to compute a valid signature to authenticate itself. Also, if an attacker eavesdrops on the communications between the bank and an EV, he cannot unblind the partial blind signature to steal the coin because he does not know the blinding value that is used to blind g^x.

Keys and TOTs Reuse Attack. Attackers may try to reuse old tokens shared with RSUs and TOTs shared with CPs to charge more than once for only one payment. This is not possible in our scheme since the RSUs and CPs delete the tokens and TOTs from the list of valid tokens and TOTs once they are used. Also, the CSP and the RSUs should make sure that the tokens they share are not reused.

Charging More for Less Payment. The CSP allows EVs to charge from a number of RSUs by giving the EV secret tokens

shared with some RSUs. EV_i cannot authenticate to additional RSUs because it does not have shared tokens and thus EV_i can charge only from a defined set of RSUs based on the amount of the payment.

Authentication and Key Management. In our scheme, signatures are used to authenticate EVs to the bank and CSPs to EVs. Efficient challenge/response technique that uses keyed hashe function is used to authenticate EVs to RSUs. Also, if an EV can calculate the correct key shared with the CSP, this is a proof that the EV is the one that created g^x of the coin because the computation of the key needs the secret x. Moreover, our key management procedure can resist *Man-in-the-Middle* attack because the CSP signs its share g^y and the EV's share g^x is signed by the bank, and it is infeasible to forge these signatures.

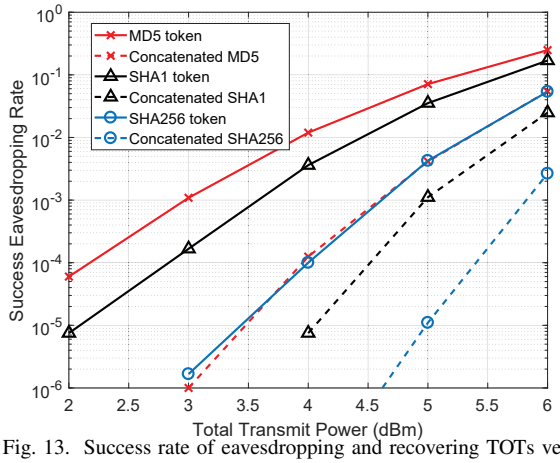


Fig. 13. Success rate of eavesdropping and recovering TOTs versus transmit power.

C. Physical-Layer-Based Authorization Scheme

Several possible attacks may be launched by attackers to attack our physical-layer-based authorization scheme. In this subsection, we discuss how our proposed scheme can resist these attacks.

Eavesdropping Attacks. If an attacker is able to capture a TOT and the TOT is not received by the CP, he can use it to charge. In our scheme, several measures have to be taken to ensure that this attack is infeasible. First, the communication system is designed so that the probability of receiving the TOTs by the CPs is very high. Second, the TOTs are valid for only short time. Third, the RF signal leakage is reduced by placing the EV-transmitter antenna on the bottom-center of the EV because the EV's body acts as an RF barrier to the signal. Fourth, the use of limited beam-width "directional" antennas imposes further limitations on signal leakage. Finally, the TOTs are transmitted using a small amount of power because the distance between the EVs and the CPs is very short.

In order to evaluate this attack, we conducted practical experiments. The probability that an attacker can successfully capture the TOTs from signal leakage was measured in the surrounding area of a car model in two different scenarios: 1) A receiving antenna was placed at 45 degrees and at a distance of 20 inches away from the car model; and 2) A receiving antenna was placed right at the edge of the car model and at different locations around the car model.

As indicated in Figure 13, an eavesdropper could possibly capture MD5 TOTs transmitted at 4 dBm with a probability of 0.01. However, referring to section IV, EVs should transmit the TOTs at -69 dBm under normal weather conditions and at -46 dBm under bad weather conditions to achieve P_S of almost one, and thus the EVs will never transmit the TOTs at the high power levels given in Figure 13. Moreover, the TOTs that have long size can further reduce the probability that it is captured. For example, MD5 TOTs with 16-byte size transmitted at 4 dBm could be successfully recovered by an eavesdropper with the probability of 0.01, while longer TOTs computed by SHA-256 with 32-byte size could be captured with the probability of 10^{-4}, when both are transmitted at the same power level. If there is a need to increase the TOT length, we can either change the hashing algorithm or concatenate the outputs of the hash function. Figure 13 shows that for the same transmit power level, the probability to successfully eavesdrop concatenated TOTs is much less than that of single TOTs. Therefore, the given results in Figure 13 confirm that it is extremely hard to eavesdrop the TOTs as long as they are transmitted at a power level less than 2 dBm.

Jamming Attacks. An attacker can launch a *narrow-band* jamming attack to jam one or some of the used carrier frequencies. To evaluate how our system can resist this attack, three cases are considered in our experiment. In the first one, the communication between the EV and the CP utilizes only one tone and the attacker jams this tone. In the second case, the attacker jams only one tone of a 2-tone EV-CP system while in the third case no jamming on the communication between the EV and CP is considered. This case is considered as a reference for fair comparisons.

Figure 14 measures P_S at different levels of transmit power for the considered cases. As shown in the figure, the single-tone scheme is affected heavily by the jamming attack when compared to non-jamming case. In order to overcome jamming in this case, the EV must increase the transmit power to 9 dBm. On the other hand, when utilizing the two-tone approach, the system just experiences a few dB reduction compared to the benchmark performance. The experiment results also indicate that the increase of the number of frequency tones used in the communication increases the scheme's robustness against jamming attacks.

In a complex attack, the attackers may try to jam the CPs to prevent them from receiving the TOTs, and simultaneously try to capture the TOT to use it. It is extremely difficult to launch this attack successfully in our scheme for several reasons. First, jamming the CPs makes the eavesdropping of the TOTs very hard because of the proximity of the CPs' receivers and the EV's transmitter, i.e., by jamming the CPs, the attacker also jams the TOT signal. Second, since the TOTs have short lifetime, the attacker should use them within a short time window.

From the simulation and experiment results presented in this section and section IV, we can conclude the following important points.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2780179, IEEE Transactions on Vehicular Technology

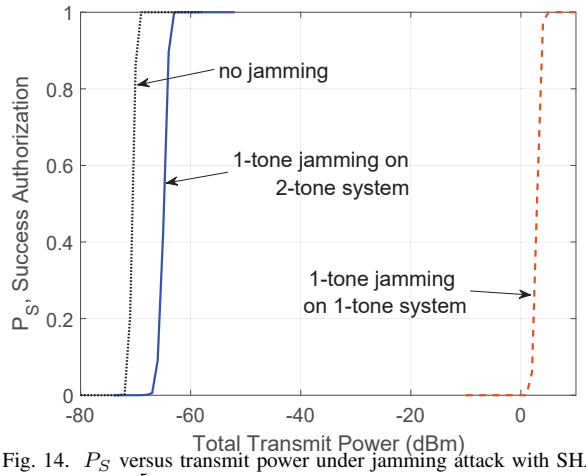


Fig. 14. P_S versus transmit power under jamming attack with SHA-1 TOTs and $P_F = 10^{-5}$.

1) Under normal environmental conditions, EVs should transmit TOTs at least at -69 dBm to ensure almost 100% of successful authorization.
2) Under different environmental conditions including snow, ice or water layer, the TOT transmit power should be increased to overcome the expected attenuation. In worst case, the transmission at -46 dBm can overcome a maximum attenuation of 23 dB.
3) Multi-tone systems are preferred over single-tone systems because of their higher resistance to jamming attacks.

VI. Related Works

Few papers in the literature have investigated the security and privacy issues of dynamic charging of EVs. In [9], [10], Li et al proposed a privacy-preserving authentication scheme for EV dynamic charging. When an EV needs to charge, it has to contact the CSP to obtain a set of pseudonyms and their corresponding symmetric keys. Then, the EV should use them to authenticate itself to every CP it encounters in its way. Comparing to our scheme, each CP needs to store only the keys it will use. Also, our scheme can provide full anonymity to EVs where the bank cannot know any location information, but in [9], the CSP (that plays the role of the bank in our scheme) can know the EV's location from the CPs that charge the EV.

In [6], Li et al. proposed an authentication scheme for EV dynamic charging. Unlike our scheme, this scheme does not address privacy issues. The scheme mainly focuses on fast handover between different RSUs. In [16], Hussain et. al. proposed authentication schemes for EV dynamic charging in which each EV should mutually authenticate to each CP and establish a symmetric session key with every CP. In this case, an EV has to exchange multiple messages with each CP, and each CP has to communicate with the CSP back and forth during the real-time authentication, which is not efficient for fast moving EVs because of the short contact time between the EVs and CPs. Also, given the large number of CPs, the interactive communications between the CPs and CSP may create a bottleneck at the CSP. In our scheme, we use a hierarchical authentication architecture which is much more scalable than the flat architecture used in [16].

Several physical-layer authentication schemes utilizing the channel impulse response were proposed in [17]–[20]. These schemes can not be applied to the dynamic charging scenario because they assume that the transmitter and the receiver are stationary to guarantee fixed channel impulse response while the channel in our scenario is highly dynamic. Also, the scheme proposed in [20] assumes the existence of prior successful authentications in order to successfully authenticate future attempts, which is difficult to use in our scheme because of the large number of EVs and CPs in the system.

In [21], Shan et. al. proposed a mutual challenge-response authentication scheme utilizing the reciprocal characteristics of the wireless fading channel between a transmitter and a receiver. However, it can not be applied in our scenario for different reasons. First, since it depends on channel reciprocity, it requires that the challenge sent by the moving EV and the response coming from the CP to be sent over the *same* channel which can not be guaranteed due to the motion of the EV. Second, this scheme requires exchanging several messages between the CPs and the EVs, which may not be efficient because of the short contact time between the CPs and fast moving EVs.

In [22], a physical-layer-assisted authentication scheme based on public key cryptography is proposed for VANETs. In the proposed scheme, each EV should have a list of anonymous public/private key pairs and anonymous certificates with pseudo identities. To use this scheme in our application, the CPs have to verify the certificates and signatures sent by the EVs, which requires the CPs to have a large computational power, i.e., the CPs are not cost effective. Furthermore, the scheme suffers from significant performance degradation at high speeds, but our scheme can achieve almost 100% successful authorization at high speed.

Various schemes have been proposed to secure and preserve privacy in different wireless networks and applications, such as [23]–[31], but these schemes cannot be used to solve the problems addressed in this paper because they are designed for different network and threat models.

VII. Conclusions and Future Work

In this paper, Cryptosystems are used to secure the EV communications to the bank, CSP and RSUs, and in order to consider the short contact time between fast moving EVs and CPs, a physical-layer-based authorization scheme has been developed to enable the CPs to only charge authorized EVs. Analysis, simulations, and practical experiments were conducted to evaluate the proposed scheme. The results indicate that the system is secure against the considered attacks, the communication and computation overheads are acceptable, and full anonymity is achieved. In addition, by selecting a good transmit power, the physical-layer-based authorization scheme can achieve high successful authorization rate under different weather conditions. Also, a good transmit power can increase the robustness of the scheme against jamming and eavesdropping attacks. In our future work, we will investigate optimally adjusting the transmit power level automatically at different environmental conditions based on the Received

Signal Strength Indicator (RSSI) levels of the beacon signal sent by the CPs.

VIII. Acknowledgment

This publication was made possible by the US National Science Foundation under the grant number 1619250. The statements made herein are solely the responsibility of the authors.

References

[1] S. M. Lukic, J. Cao, R. C. Bansal, F. Rodríguez, and A. Emadi, "Energy storage systems for automotive applications," *IEEE Transactions on Industrial Electronics*, vol. 55, no. 6, pp. 2258–2267, 2008.

[2] Tesla Motors-High Performance Electric Vehicles, "Available online: http://www.teslamotors.com."

[3] Challenges of EV charging. [Online]. Available: http://www.techrepublic.com/article/the-challenges-of-ev-charging-10-things-to-know/

[4] X. Hu, S. J. Moura, N. Murgovski, B. Egardt, and D. Cao, "Integrated optimization of battery sizing, charging, and power management in plug-in hybrid electric vehicles," *IEEE Transactions on Control Systems Technology*, vol. 24, no. 3, pp. 1036–1043, May 2016.

[5] K. Lee, Z. Pantic, and S. M. Lukic, "Reflexive field containment in dynamic inductive power transfer systems," *IEEE Transactions on Power Electronics*, vol. 29, no. 9, pp. 4592–4602, Sept 2014.

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

[7] H. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur, and A. Iyer, "Flooding-resilient broadcast authentication for VANETs," *Proc. of the 17th Annual International Conference on Mobile Computing and Networking (MobiCom '11)*, pp. 193–204, 2011.

[8] L. Reyzin and N. Reyzin, "Better than BiBa: Short one-time signatures with fast signing and verifying," *Proc. of Information Security and Privacy: 7th Australasian Conference (ACISP)*, pp. 144–153, Melbourne, Australia, July 3-5, 2002.

[9] H. Li, G. Dán, and K. Nahrstedt, "Portunes: Privacy-preserving fast authentication for dynamic electric vehicle charging," *Proc. of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Venice, Italy, 3-6 Nov. 2014.

[10] H. Li, G. Dn, and K. Nahrstedt, "Portunes+: Privacy-preserving fast authentication for dynamic electric vehicle charging," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–9, February 2016.

[11] C. Phillips, D. Sicker, and D. Grunwald, "A survey of wireless path loss prediction and coverage mapping methods," *IEEE Communications Surveys Tutorials*, vol. 15, no. 1, pp. 255–270, 2013.

[12] T. Okamoto, "Efficient blind and partially blind signatures without random oracles," in *Theory of Cryptography Conference*. Springer, 2006, pp. 80–99.

[13] S. Gunukula, A. Sherif, M. Pazos-Revilla, B. Ausby, M. Mahmoud and X. Shen, "Efficient scheme for secure and privacy-preserving electric vehicle dynamic charging system," *IEEE ICC'17, Paris, France*, May 2017.

[14] N. Guo and R. Qiu, "Improved autocorrelation demodulation receivers based on multiple-symbol detection for UWB communications," *IEEE Transactions on Wireless Communications*, vol. 5, no. 8, pp. 2026–2031, 2006.

[15] Y.-L. Chao and R. A. Scholtz, "Optimal and suboptimal receivers for ultra-wideband transmitted reference systems," in *IEEE Global Telecommunications Conference (GLOBECOM '03)*, Dec 2003.

[16] R. Hussain, D. Kim, M. Nogueira, J. Son, A. Tokuta, and H. Oh, "A new privacy-aware mutual authentication mechanism for charging-on-the-move in online electric vehicles," *Proc. of the 11th International Conference on Mobile Ad-hoc and Sensor Networks (MSN)*, pp. 108–115, Shenzhen, China, Dec. 16-18 2015.

[17] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *Proc. of the 13th annual ACM international conference on Mobile computing and networking*, 2007, pp. 111–122.

[18] J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera, "Advancing wireless link signatures for location distinction," in *Proc. of the 14th ACM international conference on Mobile computing and networking*, 2008, pp. 26–37.

[19] W. Chin, T. Le, and C. Tseng, "Authentication scheme for mobile OFDM based on security information technology of physical layer over time-variant and multipath fading channels," *Information Sciences*, vol. 321, pp. 238 – 249, 2015.

[20] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *Trans. Wireless. Comm.*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008. [Online]. Available: http://dx.doi.org/10.1109/TWC.2008.070194

[21] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "Phy-cram: Physical layer challenge-response authentication mechanism for wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1817–1827, 2013.

[22] H. Wen and P.-H. Ho, "Physical layer technique to assist authentication based on PKI for vehicular communication networks." *KSII Transactions on Internet & Information Systems*, vol. 5, no. 2, 2011.

[23] M. Mahmoud, K. Rabieh, A. Sherif, E. Oriero, M. Ismail, E. Serpedin, and K. Qaraqe, "Privacy-preserving fine-grained data retrieval scheme for mobile social networks (msns)," *IEEE Transactions on Dependable and Secure Computing (TDSC)*, In press 2017.

[24] M. Mahmoud and N. Saputro and P. Akula and K. akkaya, "Privacy-preserving power injection over a hybrid AMI/LTE smart grid network," *IEEE Internet of Things Journal*, vol. 4, no. 4, pp. 870–880, Aug 2016.

[25] K. Rabieh, M. Mahmoud, and M. Younis, "Privacy-Preserving Route Reporting Schemes for Traffic Management Systems," *IEEE Transactions on Vehicular Technology (TVT)*, vol. 66, pp. 2703–2713, March 2017.

[26] A. Sherif, K. Rabieh, M. Mahmoud, and X. Liang, "Privacy-preserving ride sharing scheme for autonomous vehicles in big data era," *IEEE Internet of Things Journal*, vol. 4, pp. 611–618, April 2017.

[27] K. Rabieh, M. Mahmoud, K. Akkaya, and S. Tonyali, "Scalable certificate revocation schemes for smart grid ami networks using bloom filters," *IEEE Transactions on Dependence and Secure Computing (TDSC)*, vol. 14, pp. 420–432, July 2017.

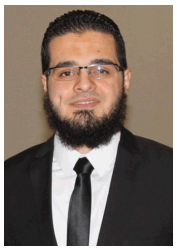
[28] Z. Haddad and A. Alsharif and A. Sherif and M. Mahmoud, "Privacy-Preserving Intra-MME Group Handover Via MRN in LTE-A Networks for Repeated Trips," *Proc. of IEEE 86th Vehicular Technology Conference (VTC2017-Fall), Toronto, Canada*, September 2017.

[29] A. Sherif, A. Alsharif, J. Moran, and M. Mahmoud, "Privacy-Preserving Ride Sharing Organization Scheme for Autonomous Vehicles in Large Cities," *Proc. of IEEE 86th Vehicular Technology Conference (VTC2017-Fall), Toronto, Canada*, September 2017.

[30] A. Alsharif, S. Tonyali, M. Mahmoud, K. Akkaya, M. Ismail, and E. Serpedin, "Performance Analysis of Certificate Renewal Scheme for AMI Networks," *Proc. of the 7th International Workshop on Computer Science and Engineering, Beijing, China*, pp. 25–27, June 2017.

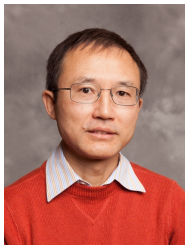
[31] H. Mohammed, S. Tonyali, K. Rabieh, M. Mahmoud, and K. Akkaya, "Efficient Privacy-Preserving Data Collection Scheme for Smart Grid AMI Networks," *Proc. of IEEE Globecom, Washington DC, USA*, December 2016.

Marbin Pazos-Revilla is currently an Electrical and Computer Engineering Ph.D. student at Tennessee Technological University under the guidance of Dr. Mohamad Mahmoud with research interests in network and communication security, cyber-physical security, intrusion detection systems, machine learning, as well as applications with Internet of Things (IoT) and embedded systems. Marbin received his M.S. in Computer Science degree from Tennessee Tech, a Bachelors degree in Information Technologies from Barry University, and carries five years of undergraduate studies in Systems Engineering and fifteen years of experience supporting LAN/WAN infrastructures.



Ahmad Alsharif is currently a graduate research assistant and working toward the PhD degree at the Center for Energy and System Research (CESR), Department of Electrical & Computer Engineering, Tennessee Tech. University, USA. He received the BSc and MSc degrees in Electrical Engineering from Benha University, EGYPT in 2009 and 2015, respectively. In 2009, he received the young innovator award from the Egyptian Industrial Modernisation Centre. His research interests include security and privacy in smart grid, vehicular Ad Hoc networks, multihop cellular wireless networks.

Surya Gunukula received his Bachelor's degree in Electronics and Communication Engineering from JNTUK, India in 2014. He is currently pursuing the Master degree in Computer Engineering from Tennessee Technological University with Network Security as his concentration. His research interests include security and privacy for Cyber-physical systems and Internet of Things (IoT).



Terry N. Guo (S'96-M'99-SM'10) received his M.S. degree in telecommunications engineering from Beijing University of Posts and Telecommunications in 1990 and Ph.D. degree in communications and electronic systems from the University of Electronic Science and Technology of China in 1997. Dr. Guo has over 20 years of academic and industrial experience in wireless communications, signal processing, radio-frequency (RF) systems and implementation aspect. His recent research interests include Internet of Things (IoT), physical-layer security, intrusion/anomaly detection, and smart manufacturing data collection and analytics.

Mohamed M. E. A. Mahmoud received PhD degree from the University of Waterloo in April 2011. After that, he was a postdoctoral fellow in Ryerson University and the Broadband Communications Research group in University of Waterloo. Currently, Dr Mahmoud is an assistant professor in the Department of Electrical and Computer Engineering, Tennessee Tech University, USA. The research interests of Dr. Mahmoud include security and privacy-preserving schemes for smart grid communication network, mobile ad hoc network, sensor network, and delay-tolerant network. Dr. Mahmoud has received two Canadian National awards; NSERC-PDF and MITACS-PDF. He also won the Best Paper Awards from IEEE International Conference on Communications (ICC'09) and IEEE Wireless Communications and Networking Conference (WCNC'16). Dr. Mahmoud is an Associate Editor in Springer journal of peer-to-peer networking and applications. He served as a technical program committee member for several IEEE conferences and as a reviewer for several IEEE journals and conferences.

Xuemin (Sherman) Shen (M97-SM02-F09) received the B.Sc.(1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. Dr. Shen is a University Professor, Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research focuses on resource management in interconnected wireless/wired networks, wireless network security, social networks, smart grid, and vehicular ad hoc and sensor networks. Dr. Shen served as the Technical Program Committee Chair/Co-Chair for IEEE Globecom16, Infocom14, IEEE VTC10 Fall, and Globecom07, the Symposia Chair for IEEE ICC10, the Tutorial Chair for IEEE VTC11 Spring and IEEE ICC08, the General Co-Chair for ACM Mobihoc15, Chinacom07 and QShine06, the Chair for IEEE Communications Society Technical Committee on Wireless Communications, and P2P Communications and Networking. He also serves/served as the Editor-in-Chief for IEEE Internet of Things Journal, IEEE Network, Peer-to-Peer Networking and Application, and IET Communications; a Founding Area Editor for IEEE Transactions on Wireless Communications; an Associate Editor for IEEE Transactions on Vehicular Technology, Computer Networks, and ACM/Wireless Networks, etc. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004, 2007, 2010, and 2014 from the University of Waterloo, the Premiers Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo, and the Joseph LoCicero Award from the IEEE Communications Society. Dr. Shen is a registered Professional Engineer of Ontario, Canada, an IEEE Fellow, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, and a Distinguished Lecturer of IEEE Vehicular Technology Society and Communications Society.