Cyber-Physical Device Authentication for Smart Grid Electric Vehicle Ecosystem

Aldar C-F. Chan, *Senior Member, IEEE*, Jianying Zhou

***Abstract*—Entity authentication and related key management is an active research topic in smart grid security. But existing works seem to have overlooked the significance that the smart grid is a cyber-physical system, which entails more considerations in the integration of its cyber and physical domains. Ignoring this could possibly undermine security since the effects of cyber authorization in the smart grid are usually extended into the physical domain. The substitution attack, a kind of the man-in-the-middle attack, has been demonstrated using this gap. This paper proposes a two-factor cyber-physical device authentication protocol to defend against coordinated cyber-physical attacks in the smart grid. The idea is to combine a novel contextual factor based on physical connectivity in the power grid with the conventional authentication factor in the challenge-response protocol, widely used in cybersecurity. The resulting protocol provides assurance on not only the digital identity of a device, but also the device's controllability in the physical domain. While the design is for the electric vehicle ecosystem, the framework could be readily extended to other smart grid subsystems.**

***Index Terms*—smart grid, multi-factor authentication, coordinated cyber-physical attacks, challenge-response, IEC 61851.**

I. Introduction

Entity authentication corroborates the identity of an entity, be it a person or a device, as it accesses certain resources requiring authorization. This primitive has been widely studied in authenticated key exchange and/or multi-factor authentication [2], [3], [6], [13], [14], [22]–[24], [29]. Entity authentication in the smart grid is also a significant research problem [5], [9]–[11], [15], [21], [29], especially for the electric vehicle (EV) ecosystem. A report published by Gartner [28] states that an EV as a roaming appliance has to be identified and located whenever it is connected to the power grid. Besides, device identity assurance of EVs is also identified as a key theme of the standardization of ISO/IEC 15118 [26]. However, there are salient features in smart grid communication, making entity authentication still challenging.

First, the envisioned smart grid will ultimately facilitate fully automated management of energy devices and systems without human intervention, meaning that device authentication would be the primary form of authentication. Machine-to-machine (M2M) communication — possibly the most common mode of smart grid communication in the future — poses a particular challenge for existing entity authentication protocols [2], [3], [6], [13], [14], [23], which are not designed to support unattended operations. A strong protection of the private key is necessary to achieve a strong assurance of digital identities in an unattended, fully automated environment. Some form of a trusted computing base (TCB) is inevitable, which is a widely accepted assumption in entity authentication and key management for the smart grid [5], [9]–[11], [15], [21], [29].

Second, all the existing protocols [5], [9]–[11], [15], [21], [29], including those with a TCB, provide security assurance up to within the cyber domain only, overlooking the significance that the smart grid is a cyber-physical system in nature. This indeed undermines smart grid security and has serious implications to typical smart grid applications such as demand response and vehicle-to-grid (V2G) [7]. The study of coordinated cyber-physical attacks is also regarded as an area of high priority in the widely cited NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0 [17]. Paverd and Martin [21] proposes a hardware security architecture to provide a trusted computing platform for device authentication in the smart grid, but does not consider coordinated cyber-physical attacks. This paper addresses both.

In the smart grid, most of the cyber commands sent over the *cyber* communication path are effected as certain operations in the *physical* power path, like closing a relay [17]. That is, a device successfully authenticated in the *cyber* domain is actually granted authorization to act freely in the *physical* domain. Consequently, the power grid reliability may be at risk if entity authentication provides little assurance that a cyber-authenticated device will be responsive to cyber commands and act accordingly to effect changes in the physical network.

Chan and Zhou [7] actually shows, using the EV ecosystem as an example, that an EV passing the typical challenge-response authentication using a TCB (which is deemed as secure in any cybersecurity standards) may not be the device which is physically connected to the power grid. Rather, it could be a malicious load connecting to the power grid, risking the reliability of the power grid. For instance, the malicious load could be irresponsive to the demand-response commands requesting the EV to curtail its power consumption when there is a shortfall of power supply — circuit breakers are ineffective in this case because a potential gap of 74A exists (according to IEC61851) before the circuit breakers are triggered, whereas, typical households draw at most 30A. Such an attack also has serious repercussions in other smart grid applications: undermining V2G when battery profiling is used [26], and eroding utility's revenue in flat-rate charging subscription plan.

This paper proposes a new two-factor cyber-physical authentication protocol for the smart grid EV ecosystem using a novel contextual factor, namely, physical connectivity of the charging cable. It is basically a challenge-response protocol

Aldar C-F. Chan is with Hong Kong Applied Science and Technology Research Institute. Email: aldar@graduate.hku.hk.

Jianying Zhou is with Institute for Infocomm Research, A*STAR.

This work is supported by Energy Market Authority (EMA), Singapore.

with two challenges — one sent over the standard cyber path (cyber challenge) and the other sent over the charging cable of the EV (physical challenge). The authentication protocol also provides an effective means to test the controllability of the EV charging load while verifiying the EV's digital identity. *This is the first design of cyber-physical authentication for the smart grid in the literature.* A proof-of-concept design and implementation is given with experimentation.

The contribution is two-fold. First, a novel cyber-physical device authentication protocol for electric vehicles is presented, with a number of desirable properties: unlike IEC 15118 [26], it requires no modification on the EV, thus readily deployable; besides, the protocol provides a strong binding between the cyber and physical parts of an EV, assuring that the EV passing the authentication knows the needed secret in the tamper resistant device or TCB and is physically connected to the specified point of the power grid; in addition, it also provides a means to verify the controllability of the EV in the physical domain. It should be emphasized that, while the protocol is specifically designed for the EV ecosystem, the two-factor cyber-physical authentication framework could be widely applicable in the smart grid to secure switchgears, trippers, etc.. The key is to find a relevant contextual factor. Second, a hardware mechanism for binding an onboard unit (OBU) and an EV is proposed, which also finds application in other scenarios such as vehicular telemetry and location-based electronic road pricing. The basic idea is that once the device is deployed in an EV, unplugging it would disable its CAN (Controller Area Network) bus interface, therefore rendering it unusable for another EV. Hence, transferring an OBU from one EV to another would not bypass the authentication.

The paper is organized as follows. Section II briefly explains the substitution attack; for details, [7] should be consulted. The proposed cyber-physical device authentication and its prototype implementation are given in Section III and IV respectively. Section V and VI discuss the security of the protocol and the experimental results. Related work is discussed in Section VII, followed by a conclusion in Section VIII.

II. Substitution Attack

The substitution attack [7], a coordinated cyber-physical attack, can be viewed as a special type of the man-in-the-middle (MitM) attack. The following discussion assumes that each EV is installed with an onboard unit called the Intelligent Electronics Device (IED). The IED, with tamper resistant storage of a secret key, serves as a token to assure the identity of an EV.[1] Nobody besides the grid operator has access to the secret key. It is also assumed that a conventional challenge-response protocol [1] based on the stored secret of the IED is used for EV device authentication. In the desirable situation, an EV without a valid registration or credential — for instance, a stolen EV — should be denied from connecting to the power grid. However, when device authentication is conducted over a wireless channel, a car-thief using the substitution attack as shown in Figure 1 can still charge a stolen EV, even though its registration and certificate have been revoked (as possibly initiated by its original owner). The car-thief can use the IED of another EV with a valid certificate and registration to run the challenge-response authentication protocol over the wireless link, while plugging in the stolen EV to the charging station. Since the keys and certificates of IED' in the second EV are still valid, they will pass the device authentication test. If the car-thief's billing account also has sufficient fund, then a charging session would start to charge the stolen EV, rather than the second EV. Charging of a stolen EV would go undetected in this way, which might have serious repercussions, such as irresponsive loads in demand response. Depending on the wireless channel in use, cooperation from the second EV is not necessary. Linking or binding a user's identity with his EV's identity may not work either since the second EV could be owned by the car-thief who has a valid user identity linked to the EV's identity. Instead, it causes inconvenience to EV owners. For the same reason, the requirement to tap a smart card at the charging station for verification would not work either.

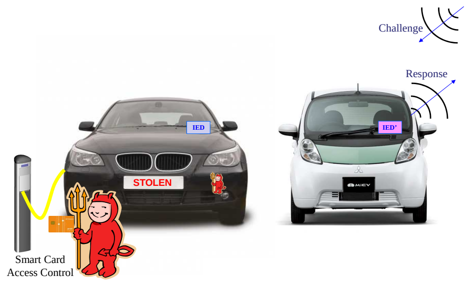


Fig. 1. Substitution Attack against EV Device Authentication

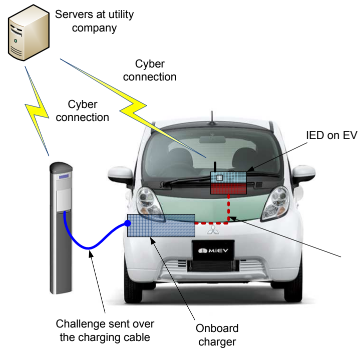

Servers at utility company
Cyber connection
Cyber connection
IED on EV
Challenge sent over the charging cable
Onboard charger

Fig. 2. The Communication Setting for Cyber-Physical Device Authentication

Other similar attacks include moving an IED from a valid EV to an illegitimate EV, and transferring the cable to an illegitimate EV after the authentication is passed by a valid EV. All these have been addressed in this paper (Section IV-B).

III. Cyber-Physical Device Authentication

A. Communication Settings

Figure 2 depicts the communication setting for the cyber-physical device authentication protocol. The IED onboard of the EV and the charging station have direct communication with the utility's backend server. The communication link between the IED and the charging station is merely a logical link. The server can be seen as the verifier for the EV identity

[1] In IEC15118 [26], the secret key is pre-installed in the EV itself, say, in one of its Electronics Control Units (ECUs).

and instructs the charging station to grant access to the EV. That is, a direct communication channel between the IED and the charging station is not necessary. The IED is connected to the CAN bus of the EV, through the OBD-II diagnosis port commonly adopted in nearly all automobiles. The charging cable is assumed to follow the SAE J1772 standard, adopted in all EV models for level 2 charging. That is, the charging cable has a control pilot pin using IEC 61851 signaling.

B. Security Assumptions

The main security assumption of the proposed protocol is tamper resistance of the IED which is a common assumption in the smart grid literature. As argued by [21], this assumption is inevitable to support fully automated M2M smart grid communication. As a corollary to such an assumption, we can assume that it is hard for an attacker to modify the IED's firmware without being detected. Remote code attestation may also be regularly used to check the code integrity of the IED.

C. Protocol Design of Cyber-Physical Device Authentication

The cyber-physical authentication protocol aims to corroborate the following: 1) the IED onboard of the EV stores the secret key corresponding to the digital identity of a valid EV; 2) the EV is physically connected to the claimed charging station. The proposed protocol is a typical challenge-response protocol, except that part of the challenge can only be received through a designated physical medium — the charging cable. Details of how to embed the second challenge in the signaling of the charging cable are given in Section IV-A.

A conventional challenge-response protocol involves two parties — a prover and a verifier. The purpose of the protocol is for the verifier to check whether the prover knows a particular secret, which is usually a cryptographic key. The verifier sends the prover a random bit string as a challenge, and in response, the prover computes a result using its private key and the challenge. Then the verifier could verify the result to see whether the prover really knows the private key in question. In this paper, the most generalized form of response computation, namely, a pseudorandom function $PRF_K(\cdot)$ — with a secret key K — is used. It should be noted that the PRF could be instantiated by any common primitives including decryption, digital signatures and Message Authentication Code (MAC). HMAC [12] is used to instantiate the PRF in the prototype implementation (Section IV) in this paper.

In the cyber-physical authentication, there are two parts of a challenge, namely, a cyber challenge C_{cyber} and a physical challenge $C_{physical}$. C_{cyber} is received over the wireless channel, and $C_{physical}$ over the charging cable. But both challenges originate from the server. The response is then computed as:

$$r = PRF_K(C_{cyber}||C_{physical}),$$

where K is the secret key stored inside the IED or a session key derived from it, depending on the actual implementation. The server (knowing K) can verify the response's correctness.

This protocol is a two-factor authentication scheme: while the secret key K shared between the server and the IED is one factor ('what-you-know'), the physical challenge $C_{physical}$ is another ('where-you-are' or 'what-you-have'). $C_{physical}$ is a novel factor which combines its numerical value and the dedicated channel for its delivery (the charging cable and its signaling). The underlying security guarantees of these two factors are based on very different means. While the first factor is a conventional one, the second one is *contextual*, similar to the notion of [2]. In addition, the contextual factor provides an assurance that the EV is actually physically connected to the charging station, and the digital information it provides to the server truly reflects the situation of the physical domain.

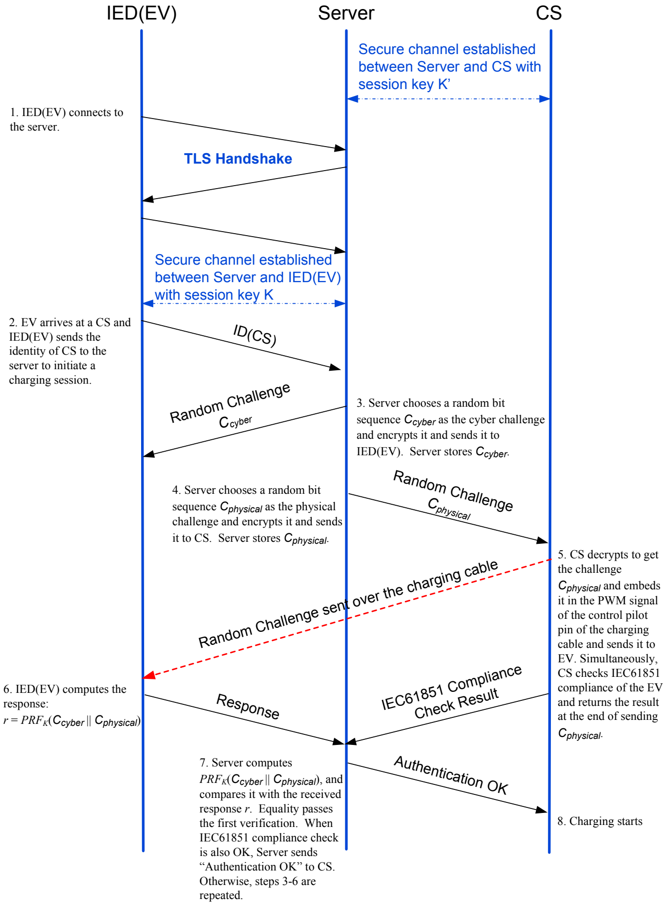

IED(EV)
Server
CS
Secret channel established between Server and CS with session key K'
1. IED(EV) connects to the server.
TLS Handshake
Secure channel established between Server and IED(EV) with session key K
2. EV arrives at a CS and IED(EV) sends the identity of CS to the server to initiate a charging session.
ID(CS)
Random Challenge C_{cyber}
3. Server chooses a random bit sequence C_{cyber} as the cyber challenge and encrypts it and sends it to IED(EV). Server stores C_{cyber}.
4. Server chooses a random bit sequence $C_{physical}$ as the physical challenge and encrypts it and sends it to CS. Server stores $C_{physical}$.
Random Challenge $C_{physical}$
5. CS decrypts to get the challenge $C_{physical}$ and embeds it in the PWM signal of the control pilot pin of the charging cable and sends it to EV. Simultaneously, CS checks IEC61851 compliance of the EV and returns the result at the end of sending $C_{physical}$.
Random Challenge sent over the charging cable
6. IED(EV) computes the response: $r = PRF_K(C_{cyber} || C_{physical})$
Response
IEC61851 Compliance Check Result
7. Server computes $PRF_K(C_{cyber} || C_{physical})$, and compares it with the received response r. Equality passes the first verification. When IEC61851 compliance check is also OK, Server sends "Authentication OK" to CS. Otherwise, steps 3-6 are repeated.
Authentication OK
8. Charging starts

Fig. 3. Execution of Cyber-Physical Device Authentication Protocol

Figure 3 shows the execution of the protocol. The charging station and the IED onboard of the EV are denoted by CS and $IED(EV)$ respectively. Step 1 is a typical TLS handshake to establish a session key K which is used to secure the channel between $Server$ and $IED(EV)$. A similar TLS handshake is executed to establish a secure channel between $Server$ and CS with another session key K'. From Step 2 onwards, all communication between $Server$ and CS is secured against eavesdropping and message modification, similarly for the communication between $Server$ and $IED(EV)$. In Step 2, the EV sends a request to initiate a new charging session to access the power grid, with the cyber-physical device authentication protocol starting at Step 3.

In Step 3, $Server$ randomly picks a bit sequence C_{cyber} as the cyber challenge and then sends it to $IED(EV)$ through the secure channel. The challenge should be at least 80 bits long.[2] $Server$ stores C_{cyber} for later verification. At the same time (Step 4), $Server$ randomly picks another independent bit sequence $C_{physical}$ as the physical challenge and sends it to CS securely. The challenge should be of similar length with C_{cyber} (but it is not necessarily strictly enforced[3]). $C_{physical}$ is kept secret from $IED(EV)$ and stored in $Server$ for later verification. Step 3 and 4 could be placed in reverse sequence without affecting the operation of the protocol.

In Step 5, CS decrypts the encrypted challenge received from $Server$ to get back $C_{physical}$ and computes a parity check code[4] for it. CS then embeds $C_{physical}$ and its parity bits in the PWM (Pulse Width Modulation) signal of the control pilot pin of the charging cable. More specifically, using a lookup table, CS maps the bit sequence of $C_{physical}$ and its parity bits into a sequence of duty cycle or pulse width values. According to IEC61851, these duty cycle values inform an EV to adjust its maximum charging current whose values could be read from the CAN bus of the EV.

As $C_{physical}$ is sent, the charging current consumed by the EV is also measured at CS at an interval corresponding to each symbol and compared with the maximum allowable current set forth by the corresponding PWM duty cycle values. If the measured current is larger than the maximum allowable current, it is considered as a failure for that symbol. After $C_{physical}$ is completely sent, the percentage of failures (which is the IEC61851 Compliance Check Result in Fig. 3) is sent to $Server$. If this percentage exceeds a certain predefined threshold, the authentication is considered as failed.

In Step 6, $IED(EV)$ reads the sequence of maximum allowable current values from the CAN bus, and looks up from a table the corresponding bit sequence of $C_{physical}$. The parity is checked. If the verification fails, $IED(EV)$ requests CS ($Server$) to resend $C_{physical}$ (which is ideally a new value), possibly after a request to use a quantization scheme with a coarser granularity on the duty cycles. $IED(EV)$ then uses K to generate the response $r = PRF_K(C_{cyber}||C_{physical})$ and sends it to $Server$. Both $C_{physical}$ and K, corresponding to the two authentication factors, are needed for generating a correct r to pass $Server$'s verification.

In Step 7, upon receiving r from $IED(EV)$, $Server$ computes $PRF_K(C_{cyber}||C_{physical})$ to verify the correctness of r. Equality means $IED(EV)$ has the correct key K and correct $C_{physical}$ (implying that the EV is connected to the specified CS as $IED(EV)$ claims). If the verification of IEC61851 compliance also passes, the server sends an "Authentication OK" to CS to inform it to start the charging session and grant access to the EV. If the verification fails, $Server$ would inform CS and $IED(EV)$ to repeat Steps 3-6 again, possibly with a longer symbol duration for the PWM pulses. The probability of a verification failure should be practically negligible. After a predefined number of authentication failures, $Server$ could inform CS to terminate the charging session setup.

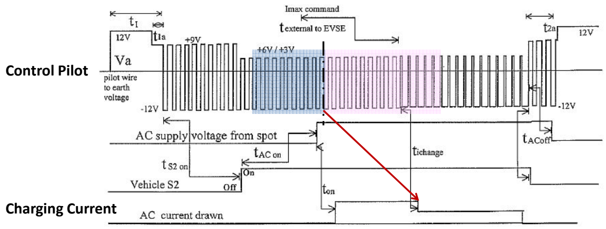


Fig. 4. PWM Pulses over the Control Pilot Pin of SAE J1772

IV. Prototype Implementation

A full proof-of-concept prototype is implemented to demonstrate the two-factor cyber-physical device authentication. The NXP-ATOP platform [19], a system-on-chip module including two ARM7 and one ARM9 processors, is used to implement the IED and the controller for the charging station. Power circuits are built for the charging station. The backend server is implemented, running the Ubuntu OS. The IED and charging station communicate with the server using GPRS (General Packet Radio Service). The prototype includes several optimizations, including a tailored coding scheme to embed the physical challenge into the PWM pulses of the SAE J1772 control pilot, and a specially designed secure CAN bus interface to ensure the binding between the IED and the EV.

A. Mapping the Physical Challenge into the PWM Signal of the SAE J1772 Control Pilot Pin

A scheme, similar to modulation, is designed for sending the physical challenge over a standard SAE J1772 charging cable. The scheme does not require any powerline communication modem installation on the EV. The basic idea is to use existing signaling of the charging cable to embed the bits of the physical challenge. According to IEC61851 (adopted by IEC62196 and SAE J1772), square pulses are continuously sent from the charging station to the EV over the control pilot pin of the charging cable. As shown in Figure 4, by changing the duty cycle/pulse width of these pulses, the charging station can request the EV to adjust the maximum charging current. In this paper, the physical challenge is sent as a sequence of different duty cycle values over the control pilot pin. The PWM pulses of different duty cycle values are in essence a set of symbols embedding the physical challenge. The IED onboard of the EV reads off the maximum allowable charging current values from the CAN bus, and looks up the bit strings constituting the physical challenge.

As the physical challenge is sent, the maximum charging current consumed by the EV also changes accordingly if it complies to IEC61851. In the proposed protocol (Step 5), the charging station simultaneously measures this changing current to check whether it matches with the duty cycle of the PWM pulses. The protocol leverages this to check the controllability of the connected EV in response to the control pilot signalling, that is, IEC61851 compliance of the EV.

Two lookup tables are pre-stored in the charging station (Table_CS) and the IED onboard of the EV (Table_EV). Upon

[2] A 64-bit sequence is also acceptable because the protocol is run in real time and an attacker cannot repeatedly fail. The offline brute force attack is inapplicable: once a test is failed, a new random sequence is used in the next.

[3] Since HMAC is used, the input to PRF could be arbitrary in length. Consequently, the two challenges need not be equally long.

[4] An 8-bit parity check code should be sufficient.

receiving the physical challenge $C_{physical}$, the charging station divides it into n-bit sub-strings denoted by r_j, where n is predetermined. For each r_j, the charging station looks up from Table_CS the corresponding duty cycle value to adjust the control pilot PWM pulses accordingly. The IED can only read maximum charging current values from the CAN bus, rather than duty cycle values. Table_EV maps these charging current values back to the n-bit sub-strings constituting $C_{physical}$.

1) Lookup Table Creation: To create the lookup table, the following procedure is adopted:

```
Lookup Table Creation (Table_CS and Table _EV)

1) Set the minimum duty cycle value $T_{MIN}$ to the minimum allowable value in IEC61851. Determine the maximum duty cycle value $T_{MAX}$ based on the power rating of the charging station.
2) Divide $[T_{MIN}, T_{MAX}]$ into partitions of equal length: $T_1, T_2, \ldots, T_i, \ldots, T_N$. The number of physical challenge bits represented by each $T_i$ is then $n = \lfloor \log_2 N \rfloor - 1$.
3) Compute the minimum charging current value for each partition: $I_1^{MIN}, I_2^{MIN}, \ldots, I_i^{MIN}, \ldots, I_N^{MIN}$, based on IEC61851.
4) For each $n$-bit string $r_j \in \{0,1\}^n$, randomly pick 2 elements $i_1, i_2 \in [1, N]$. That is, $r_j$ is mapped to $i_1, i_2$ at the same time.
5) Create Table_CS as follows: for each $r_j \in \{0,1\}^n$, create two rows, filling in the first with $r_j$ and the mid-value of $T_{i_1}$ and the second with $r_j$ and the mid-value of $T_{i_2}$. That is, each $r_j$ is mapped to two duty cycle values.
6) Create Table_EV as follows: for each $r_j \in \{0,1\}^n$, create two rows, filling in the first with $r_j$ and $I_{i_1}^{MIN}$, and the second with $r_j$ and $I_{i_2}^{MIN}$; sort the table in ascending order of $I_i^{MIN}$.
```

Note that each r_j is intentionally mapped to two different duty cycle values. The purpose is to eliminate the need of synchronization between the charging station and the IED. Such an encoding scheme ensures that two consecutive sub-strings of the physical challenge, though with the same r_j value, will always be mapped to different duty cycle values or symbols in the PWM pulse sequence, so that adjacent symbols always differ and can be recognized as two distinct symbols or sub-strings, rather than one, at the EV side. That is, the encoding serves to delimit adjacent symbols of the PWM pulse sequence with the same r_j.

2) Table Lookup: Table_EV is used in the IED onboard of the EV for recovering the physical challenge and its parity bits from the maximum negotiated current values read from the CAN bus. For each negotiated current value I_{CAN}, the IED looks up from Table_EV the maximum I_i^{MIN} which is still smaller than I_{CAN} and appends the corresponding r_j to the previously recovered portion of the physical challenge. Then the parity bits are checked to detect any transmission error.

B. CAN Interface Security

In order to withstand the swapping attack wherein an attacker moves the IED from a valid EV to a stolen EV to bypass the cyber-physical verification, a tailored security mechanism is designed to ensure the binding of the IED and the EV such that the secret key inside the IED can be treated as a proof of identity for the EV. The mechanism ensures that each IED can be plugged into the OBD-II socket once only; subsequent removals and plug-in's would disable its CAN bus interface. This assures that only the IED installed by the authority can function properly to obtain the physical challenge, and moving it to another EV would render it *defunct*.

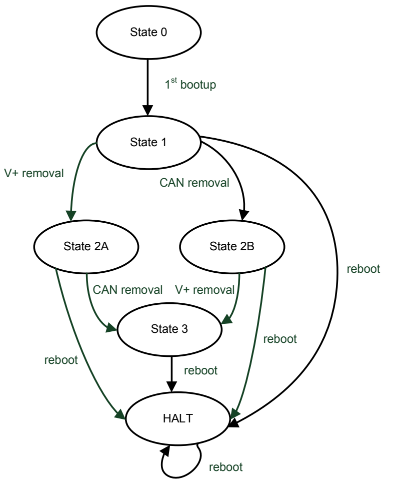


Fig. 5. State Diagram for Secure CAN Bus Interface in the IED

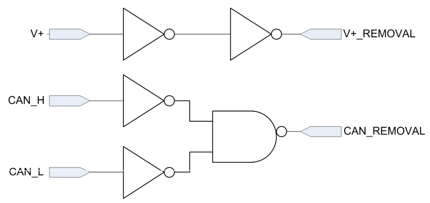


Fig. 6. Glue Logic for the State Transition Signals

The basic idea is that different states (as depicted in Figure 5) are defined for the IED to operate at. The states are defined based on the number of reboots, and whether the CAN bus interface has been unplugged and re-plugged. It is assumed that a trusted computing base (TCB) is available, which is provided by the secure element of the NXP-ATOP. The current state of the IED is appended with a digital signature generated by the TCB. In other words, the TCB is purely used to generate the digital signature. It is not mandatory in the design; the need of the TCB could be *waived* if the IED has no backup battery and draws its power only from the ODB-II socket.

1) IED Bootup Sequence: When the IED is rebooted, whether the CAN bus interface is enabled depends on the signed state which is denoted as current_state. The IED bootup sequence is as follows:

```
Subroutine IED_Boot

1) Verify the signature of current_state.
2) If (current_state = State_0 ) and signature verification is OK, do:
    a) Enable the CAN bus interface.
    b) Generate a digital signature for State_1.
    c) Update current_state to State_1.
3) Else, do:
    a) Disable the CAN bus interface.
```

The bootup sequence is designed in such a way that activation of the CAN bus interface is allowed only in State 0. All other states, after reboot, will end up in the HALT state with the CAN bus interface disabled. After the first activation of the CAN bus interface by an authorized party, the IED will transit into State 1 which disallows subsequent activation of the CAN bus interface upon reboot. An attacker is not able to revert the IED to State 0 because he should not have the digital signature for State 0, which has been erased upon IED installation. In the design, moving the IED from one EV to another would trigger a reboot, which leads to the deactivation of the CAN bus interface, thus preventing the attacker from connecting the IED to the CAN bus of the second EV. The IED is thus defunct to obtain the physical challenge through the CAN bus of the second EV, and will fail the cyber-physical authentication. Remote code attestation protocol could also be used to verify the integrity of the software if necessary.

2) State Transition Signals and Glue Logic: The signals V+, CAN_H, CAN_L of the OBD-II socket of the EV are used, through some glue logic, to trigger state transition of the IED.[5] Depicted in Figure 6 is the glue logic. The output signals V+_REMOVAL and CAN_REMOVAL are fed as input to two edge-sensitive GPIO (General Purpose Input/Output) pins of the NXP-ATOP. A downward transition of any of these two signals triggers an ISR (Interrupt Service Routine) to update the current state of the IED. When V+ is removed, there will be a downward transition of the signal level at V+, which in turn triggers the transition from State 1 to State 2A. In normal situations, CAN_L and CAN_H would move in the opposite direction. However, when the plug is removed, both CAN_L and CAN_H will go downward in voltage level simultaneously. A downward transition at both CAN_L and CAN_H could be used to trigger the state transition from State 1 to State 2B. The two corresponding ISRs are as follows.

```
Subroutine V_plus_removal

1) Verify the signature of current_state.
2) If (current_state = State_1) and signature verification is OK, do:
     a) Generate a digital signature for State_2A.
     b) Update current_state to State_2A.
3) If (current_state = State_2B) and signature verification is OK,
   do:
     a) Generate a digital signature for State_3.
     b) Update current_state to State_3.
```

```
Subroutine CAN_removal

1) Verify the signature of current_state.
2) If (current_state = State_1) and signature verification is OK, do:
     a) Generate a digital signature for State_2B.
     b) Update current_state to State_2B.
3) If (current_state = State_2A) and signature verification is OK,
   do:
     a) Generate a digital signature for State_3.
     b) Update current_state to State_3.
```

V. Security Analysis

A. Security of Cyber-Physical Device Authentication Protocol

The cyber-physical device authentication protocol could withhold most attacks, except sophisticated tampering of the charging cable, involving relatively deeper technical know-how difficult for most adversaries. Simple tapping or tampering of the charging cable would give a wrong impedance value and should fail the verification of IEC61851. Even for those more sophisticated attacks, the protocol still can assure that the malicious load is a *controllable* one which is responsive to the load curtailing requests made through the control pilot pin signaling. That is, a car may be plugged in with the wrong identity using a sophisticated tampering attack, but passing the authentication protocol in this case means that it would still follow the grid's instructions when demanded.

The security analysis of the cyber-physical device authentication protocol is similar to that of a typical challenge-response authentication protocol, a formal proof of which might not be available. In order to compute a correct response that can pass the verification by the server, the IED needs to have the knowledge of the secret key K and all the inputs (C_{cyber} and $C_{physical}$) to the PRF. This is based on the unpredictability assumption of the PRF which in turn is a result of the well-known indistinguishability assumption of PRFs. While an attacker might use a second car with a valid K, he has to plug in that car, rather than the malicious load, in order to obtain $C_{physical}$. The key of the security against the substitution attack [7] hinges on the access to $C_{physical}$. There should be no other way than tapping onto the control pilot pin of the charging cable to obtain $C_{physical}$ as the encryption used between the charging station and the server is assumed to be secure. Simple tampering of the charging cable fails the IEC 61851 impedance verification. The attack of transferring the charging cable from the car to the malicious load after the car has obtained $C_{physical}$ and passed the cyber-physical authentication would cause an immediate cut-off of the power supply by the charging station, as stipulated in IEC61851.

In order to launch the relay attack [27] successfully, the proposed cyber-physical authentication protocol imposes an additional requirement that physical access to the second EV is necessary. While the first EV (as a malicious relayer) can obtain $C_{physical}$, it has to pass $C_{physical}$ to the second EV through a certain channel. Unless the attacker could modify the IED firmware of the second EV — which is difficult in general due to tamper resistance of the IED — the IED has to accept $C_{physical}$ through the CAN bus of the second EV. Feeding another input to the IED's CAN interface is highly unlikely due to the CAN security implemented (Section IV-B). The only possible means to feed $C_{physical}$ to the IED of the second EV is through its charging cable again. In other words, the attacker has to launch the relay attack over the charging cable, and IEC61851 has safe-guarded simple tampering techniques.

For the more sophisticated cable tampering attacks, we should distinguish between two cases: that the second EV is cooperative in the attack, and that the second EV is innocent and unaware of its involvement in the attack (the preceding discussions apply). In both case, physical access to the second EV is inevitable, which already imposes an additional layer of difficulty for the attacker, making a massive attack unlikely. For the former case with a cooperative EV, a complete defeat of the attack might be impossible. Even the distance bounding protocol [4], [27] might not work well. Imagine the relay at-

[5] It should be noted that, in the simplest case, using these state transition signals may not be compulsory. They are included in the design for finer granularity of control and later expansion.

tack to access a car as in [27]: if the car owner holding the key cooperates with the attacker, how can any meaningful defence be possible? This is the same for the case of substitution attack, if the attacker builds sophisticated tampering devices to relay the charging cable signals. The distance bounding protocol over the charging cable might not be able to withhold the substitution attack with a cooperative second EV. First, the delay difference between the two cars could be too small to obtain a clear resolution with high confidence. Second, the delay could be tampered as physical access to the two cars is assured. Besides, the equipment required makes it impractical. On the contrary, the cyber-physical authentication protocol still gives a better protection guarantee for the power grid reliability in this case. First, the malicious car would be responsive to load curtailing commands as it is verified to be compliant to IEC61851 in the cyber-physical authentication protocol. Second, the relaying task is made more difficult.

B. Analysis of CAN Interface Security

Transferring the IED from a valid EV for use in an illegitimate EV is guarded against by the CAN interface security mechanism (Section IV-B). The unplugging of the IED would makes it defunct for subsequent use. The only state which allows the IED to boot up with the CAN bus interface enabled is State 0. Once an IED is deployed, it would never have a signed state for State 0. The signature for State 0 would be immediately erased after the first installation by the authorized dealer. In State 1, the IED can operate normally with the CAN bus interface enabled. However, once rebooted, the CAN bus interface will be disabled at the next bootup. Since the attacker has no knowledge of a valid signature for State 0, this check cannot be bypassed in the next bootup. It is possible that the attacker can obtain a new IED from the manufacturer but this new IED does not have the necessary credentials (including the secret key and certificates) pre-stored. In other words, the attacker could only get an IED with CAN bus interface enabled but without the needed credentials or an IED with proper credentials but with the CAN bus interface disabled.

VI. Experiment Results

We conducted a number of experiments to demonstrate demand response on a real EV, the substitution attack, how the cyber-physical authentication protocol withholds the substitution attack and detects a malicious load. We have built a charging station as shown in Figure 7 and implemented a basic demand response system. We demonstrated a successful substitution attack wherein several malicious loads including water kettles and hairdryers are plugged in, instead of the EV. The normal challenge-response protocol run by the EV is passed without detecting any anomaly and the charging station supplies power to the kettles and dryers. When a load curtailing command was issued, these loads were irresponsive. We then tested the cyber-physical authentication protocol on the same attack setting and it was able to detect the malicious loads at the start. The verification fails. On average the protocol takes 40s to 100s to complete. Since it could be done automatically after plugging in without demanding active human attention, the latency of the protocol is still reasonable. We also tested the protocol on an EV emulator with an 8051 microcontroller, to illustrate the PWM duty cycle change.

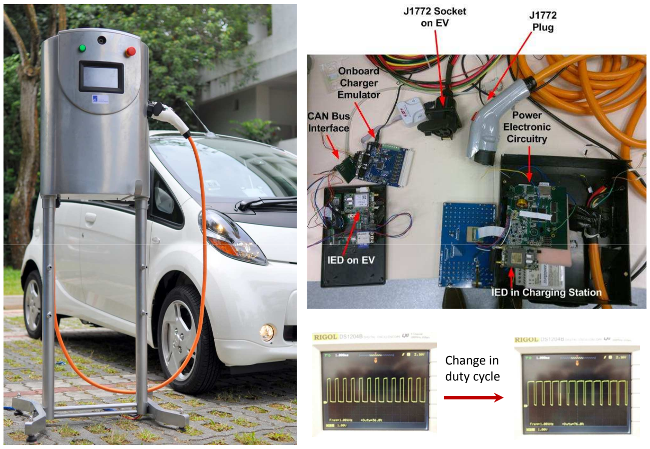


Fig. 7. Experiment Setup

VII. Related Work

Man-in-the-middle (MitM) attacks are not an entirely new problem in security engineering. Anderson [1] has a fairly comprehensive discussion. The problem has been addressed in various contexts including web browsers [2], [14] and physical access control [4]. This paper considers the specific context of the smart grid to illustrate the potential impact of such attacks.

Multi-factor entity authentication has also been addressed in different applications [2], [3], [6], [13], [14], [22]–[24], [29]. In addition to the existing forms of authentication factors, namely, what the prover has, what the prover knows, and what the prover is, we introduce a new factor of authentication based on where the prover is or where the prover is physically connected in the smart grid. This shares some similarity with [14], yet different. The main difference lies in that human involvement is avoided in the current context, which is desirable. While the distance bounding protocol [4], [27] could partly solve the problem of substitution attacks, it poses stringent requirements on the physical channel for running it; besides, there is still chance that physical proximity may not guarantee physical connectivity. Similarly, limiting the wireless range may not work well. Besides, using RFID tags on EVs may not provide the desired strength of binding between the RFID tag and the EV. This is the very problem addressed by the CAN security mechanism (Section IV-B). On the contrary, the proposed method in this paper assures that the EV passing the authentication is the one plugged in. Although there is possibility that the attacker tailors a special charging cable to bypass the protocol, this requires deep technical expertise.

It is fair to say most research in smart grid security focuses on cyber mechanisms. For instance, [25] develops a secure Intelligent Electronics Device (IED) which is safe for connecting to the Internet. Entity authentication and key management in the smart grid is also actively studied [5], [9]–[11], [15], [21], [29]. However, nearly all of the existing works only consider purely cybersecurity issues and it is unsure whether such approaches could defend coordinated cyber-physical attacks in real deployment scenarios. It is true that combined cyber-physical considerations have to take into account specific details of the contexts or application scenarios — say, what equipment is being secure and where it is connected to the power grid — which might limit the range of applications of the resulting schemes. However, considering specific contexts also means optimized performance in the targeted application. There is tradeoff between generality and optimization. More importantly, a generic design might not be able to withstand even the simplest form of coordinated cyber-physical attacks. It is important that coordinated cyber-physical attacks be considered early on in smart grid security designs, which is attempted by this paper.

VIII. Conclusion

This paper addresses a specific type of coordinated cyber-physical man-in-the-middle attack, called the substitution attack, in the smart grid. We propose a cyber-physical device authentication protocol to withhold the substitution attack, and a CAN security mechanism to provide a strong binding between the IED and the EV. A proof-of-concept prototype is implemented to demonstrate the strength of the combined cyber-physical approach to defend coordinated cyber-physical attacks in the smart grid. This idea could be extended to other equipments in the smart grid. By taking specific details of the context of the EV ecosystem and EV standards into consideration, no intrusive modifications on EVs is necessary. The advantages of our design over NFC (Near Field Communication)/RFID and IEC15118 are as follows.

	Physical Connectivity Assurance	Minimum Modification On EV	Demand Response Compliance
NFC/RFID	NO	YES	NO
IEC15118	YES	NO	NO
Our Approach	YES	YES	YES

Acknowledgment

The authors thank Ang Chiew Kok, Wong Jun Wen, Wang Xian, Lee Chang Fatt, Goh Lee Kee for building the prototype.

References

[1] R. J. Anderson, *Security Engineering: A Guide to Building Dependale Distributed System*, 2nd ed. Wiley, 2008.

[2] A. Ben-David, O. Berkman, Y. Matias, S. Patel, C. Paya, and M. Yung, "Contextual OTP: Mitigating Emerging Man-in-the-Middle Attacks with Wireless Hardware Tokens," in *F. Bao, P. Samarati and J. Zhou (Eds.): ACNS'12, Springer LNCS, vol. 7341*, p. 30-47, 2012.

[3] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung, "Fourth-Factor Authentication: Somebody You Know," in *ACM CCS'06*, p.168-178, 2006.

[4] S. Brands, and D. Chaum, "Distance-Bounding Protocol," in *Eurocrypt'93*, 1993.

[5] T. Baumeister, "Adapting PKI for the Smart Grid," in *IEEE SmartGridComm'11*, p.249-254, 2011.

[6] X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky, and A. Smith, "Secure Remote Authentication using Biometric Data," in *R. Cramer (Ed.): Eurocrypt'05, LNCS, vol. 3494*, p.147-163, 2005.

[7] A. C-F. Chan, and J. Zhou, "On Smart Grid Cybersecurity Standardization: Issues of Designing with NISTIR 7628," *IEEE Communications Magazine* 51(1), p.58-65, January, 2013.

[8] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A Lightweight Message Authentication Scheme for Smart Grid Communications," *IEEE Trans. on Smart Grid*, vol. 2, no. 4, p.675-685, 2011.

[9] H. Khurana, R. Bobba, T. Yardley, P. Agarwal, and E. Heine, "Design Principles for Power Grid Cyber-Infrastructure Authentication Protocols," in *HICSS'10*, January, 2010.

[10] N. Kuntze, C. Rudolph, I. Bente, J. Vieweg, and J. von Helden, "Interoperable Device Identification in Smart-Grid Environments," in *IEEE PES General Meeting*, p.1-7, July, 2011.

[11] S. Lakshminarayanan, "Authentication and Authorization for Smart Grid Application Interfaces," in *IEEE/PES PSCE'11*, March, 2011.

[12] IETF, *RFC 2104 — HMAC: Keyed-hashing for Message Authentication*.

[13] M. S. Mannan, and P. C. van Oorschot, "Using a Personal Device to Strengthen Password Authentication from an Untrusted Computer," in *FC'07, Springer LNCS vol. 4886*, p.88-103, 2007.

[14] J. M. McCune, A. Perrig, and M. K. Reiter, "Seeing-is-believing: Using Camera Phones for Human-verifiable Authentication," in *IEEE Symposium on Security and Privacy*, p.110-124, 2005.

[15] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Efficient Authentication and Key Management Mechanisms for Smart Grid Communications," to appear in *IEEE System Journal*, 2013.

[16] NIST, *NISTIR 7628: Guidelines for Smart Grid Cyber Security, vol. 1-3*, August, 2010.

[17] NIST, *NIST SP1108: Framework and Roadmap for Smart Grid Interoperability Standards*, Release 1.0 (Jan, 2010), Release 2.0 (Feb, 2012).

[18] NERC, *Critical Infrastructure Protection (CIP-001 to CIP-009).*

[19] NXP, *ATOP datasheet*, accessed at http://www.nxp.com/documents/leaflet/939775016910.pdf.

[20] SGIP-CSWG, *Standard Review Report on "Security Assessment of SAE J2847-1: Communication between Plug-in Vehicles and the Utility Grid,"* November, 2010.

[21] A. J. Paverd, and A. P. Martin, "Hardware Security for Device Authentication in the Smart Grid," in *J. Cuellar (Ed.): SmartGridSec'12, Springer LNCS vol. 7823*, p. 72-84, 2013.

[22] D. Pointcheval, and S. Zimmer, "Multi-factor Authenticated Key Exchange," in *S. M. Bellovin, R. Gennaro, A. D. Keromytis, and M. Yung (Eds.): ACNS'08, Springer LNCS, vol. 5037*, p.277-295, 2008.

[23] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. Mitchell, "Stronger Password Authentication using Browser Extensions" in *USENIX Security'05*, p.17-32, 2005.

[24] B. Schneier, "Two-factor Authentication: Too Little, Too Late," Communications of the ACM 4(4), 2005.

[25] J. Zhang, C. Grier, S. T. King, and C. A. Gunter, "Secure Intelligent Electronic Devices," accessed at http://tcipg.org.

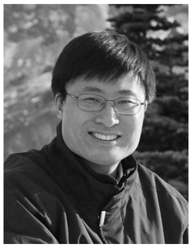
[26] ISO/IEC, *ISO/IEC 15118-2: Vehicle-to-Grid Communication Interface — Part 2: Network and Application Protocol Requirements (Draft International Standard)*, 2012.

[27] A. Francillon, B. Danev, S. Capkun, "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars," in *NDSS'11*, February, 2011.

[28] Z. Sumic, *Gartner Research Report: Hype Cycle for Smart Grid Technologies, 2012*, July, 2012.

[29] F. Zhao, Y. Hanatani, Y. Komano, B. Smyth, S. Ito, and T. Kambayashi, "Secure Authenticated Key Exchange with Revocation for Smart Grid," in *IEEE ISGT'12*, 2012.

Aldar C-F. Chan [SM] is currently Principal Engineer of Hong Kong Applied Science and Technology Research Institute. He received his PhD from the University of Toronto and BEng(EEE) with First Class Honours from the University of Hong Kong. He has worked in both academia and industry, and is a full member of the Hong Kong Computer Society. His research interests include network security, cloud security, cyber-physical system security, smart grid security, and malware analysis.



Jianying Zhou is a senior scientist at Institute for Infocomm Research, and the head of Infocomm Security Department. He received PhD in Information Security from University of London and BSc in Computer Science from University of Science and Technology of China. His research interests are in computer and network security, cyber-physical system security, mobile and wireless security. He is a co-founder and steering committee member of International Conference on Applied Cryptography and Network Security (ACNS).