A Secure, Intelligent Electric Vehicle Ecosystem for Safe Integration with the Smart Grid

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

***Abstract*—The availability of the charging infrastructure is critical for a smooth rollout of wide-scale electric vehicle (EV) adoption. Safe integration of the charging infrastructure with the power grid relies heavily on an intelligent platform to support demand-side management, and a secure information and communication system to coordinate events. However, security has been identified as an area falling short of the desired expectation in the smart grid, possibly introducing considerable risk to the reliability and stability of the power grid. Besides, a concrete demand-side management system compatible with state-of-the-art electric vehicles is also lacking. This paper fills the gap by proposing a scalable defence-in-depth cybersecurity architecture for the charging infrastructure, and a demand response scheme for smart electric vehicle charging. The feasibility of the system is demonstrated by implementation and testing on a real vehicle.**

I. Introduction

Successful wide-scale adoption of electric vehicles (EVs) and their acceptance by users hinge on the availability of the charging infrastructure. This is particularly critical to issues like range anxiety as, for the current state-of-the-art battery technology, a typical EV necessitates daily charging. Nevertheless, it is still challenging to integrate the EV charging infrastructure into the existing power grid or the envisioned smart grid for a number of reasons. First, charging a typical EV today draws 3-7.2 kW of power (at level 2 charging), which is greater than a typical household's consumption. Load curtailing is thus desirable for EV charging in practice. Second, utility operators tend to support EV charging at off-peak times when the power grid resources are under-utilized [12], [27], [33]. During peak times, an EV could sell back electricity to fill the shortfall of the power generation amidst a demand surge. While essential for achieving low carbon emission, both of these operation models strongly rely on information exchange between different parties to coordinate events, as well as, a secure, reliable billing system to support EVs both as mobile loads and distributed power sources [11], [12]. Hence, a smooth integration of the EV charging infrastructure with the power grid relies heavily on an ICT (Information and Communication Technology) system [9], [11], [12], [33], the security of which is of foremost importance.

Without security, a malicious attacker could possibly forge and inject fake coordination messages to cause EVs all charging at the maximum power rating during peak times, or becoming irresponsive to load curtailing commands, thus bringing instability and possibly an outage to the power grid. On the other hand, integration of the charging infrastructure and the power grid (inevitable for demand-side load management) could possibly open up new attack vectors to the power grid which is still largely protected by obscurity and physical isolation. Despite its significance, cybersecurity has been identified as an area falling short of expectation in the envisioned smart grid [4], [23], [27].

This paper aims to fill this gap by presenting the design and architecture of a secure, intelligent EV ecosystem with a strong digital identity assurance, which can support demand-side charging load management and secure billing and event coordination, and is ready for safe integration with the power grid. The term 'ecosystem' is used to reflect that the system is comprised of different types of devices owned by different parties. More specifically, the system architecture of an ICT infrastructure for the EV ecosystem and a demand-response mechanism to enable smart charging are presented. A comprehensive defence-in-depth cybersecurity architecture is designed to secure the EV ecosystem, according to the NISTIR 7628 [27], wherein different mechanisms are applied in different layers to defend a particular type of attack. It should be noted that the NISTIR 7628 only stipulates high-level security objectives and this paper fills in the gap by proposing a concrete design — with an emphasis on digital identity assurance — to achieve those objectives, specific for the EV ecosystem. A number of lightweight security variants are tailored, with their security carefully analyzed. The system is built and tested with a real EV — Mitsubishi i-MiEV.

The contribution of this paper is two-fold. First, a demand-response system is constructed. The system achieves a fast response time (in seconds), which can enable a wide range of demand response models and allow utility operators to have real-time control of EV charging loads. Second, a comprehensive defence-in-depth cybersecurity architecture is proposed to secure the EV ecosystem, fulfilling all the security requirements posed by the NISTIR 7628. The design emphasizes a strong assurance of digital device identities, which is the crux for secure machine-to-machine (M2M) communication [19], [37], safe integration with the power grid, and reliable billing. Besides, the proposed architecture is modular and scalable such that its components can be composed in different ways to achieve different levels of security, depending on the available physical protection.

The paper is organized as follows. The next section presents related work. Section III and IV present the design of the ICT system for the EV ecosystem and the demand-response system. Section V stipulates the security requirements. Section

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.

The authors would like to thank EMA, Singapore for funding support.

VI discusses the proposed cybersecurity architecture, with the performance evaluation and security analysis in Section VII.

II. Related Work

While smart meter security and privacy has been widely addressed — for example, in consumer privacy [2], [8], [32], key management [5], [17], firmware integrity [16] and threat analysis [31] — securing the EV charging infrastructure is rarely discussed in the literature. Security research taking into account the integration of EVs and the smart grid is especially lacking. Although [4], [14], [15], [22] poses security concerns of plug-in vehicles to the smart grid, no security solution has been proposed. It is fair to say this paper gives the first concrete solution to securing the EV ecosystem.

Both [22] and [15] investigate attack vectors for the EV charging infrastructure in different settings and stipulate security requirements. While [22] is based on a model of generic logical connections and communication types for three different use cases (at home, at work and at public places), [15] analyzes security of a concrete standard [13]. However, the security implications of the integration of the EV ecosystem and the smart grid seem possibly overlooked. In contrast, this paper views the EV ecosystem and the smart grid as a whole system, stipulating security requirements based on the NISTIR 7628 [27] and the ENISA guidelines [7]. [14] has an in-depth analysis of the risk of consumer privacy breach as a result of continuous connectivity between EVs and the smart grid from the technical, legal and socio-ethical perspectives, but gives no technical solution. [35] proposes a hybrid public key infrastructure for cross-certifications in vehicle-to-grid (V2G) applications, whereas, this paper presents a more comprehensive architecture covering both V2G and demand-response. [3] proposes a novel cyber-physical device authentication protocol for the EV ecosystem to withhold the newly identified substitution attack, but does not address the overall architecture.

III. ICT Infrastructure for EV Ecosystem

The high-level system architecture of the proposed ICT infrastructure is depicted in Figure 1. A key component is the IED (Intelligent Electronics Device), installed onboard of an EV or embedded inside a charging station, to provide tamper-resistant storage for secret keys and strong assurance of device identities. The IED is different from the devices typically used in power substations to sense conditions and control processes. The use of IEDs in the charging infrastructure is supported by the industrial need, as identified by Gartner [10], which states that "the disruptive nature of electric vehicles comes from the fact that, due to their nomadic nature as a roaming appliance, they must be *identified and located* whenever and whatever they connect to a utility network; this requires integration with *onboard vehicle information systems*."

There are four types of servers, namely, Charge Management Server (CMS), Vehicle Management Server(VMS), Billing Management Server (BMS), and Grid Management Server (GMS). These servers are connected to one another via IPsec tunnels with pre-shared keys. In contrast to conventional configurations, authentication is applied to both the header (AH) and IP payload (ESP) to address recent attacks [6]. No specific requirement on the physical connections is needed.

IEDs communicate directly to the CMS, which can be seen as the frontend server managing charging sessions and coordinating between EVs, charging stations and the other backend servers, BMS and GMS included. A wide range of networks could be used to connect IEDs to the CMS, including GPRS, 3G. IEDs could also possibly connect to one another through ZigBee or TV White Space. The VMS can be seen as a third party service provider in the NIST Logical Reference Model [27], [28]. It provides EVs with information about charging stations (such as locations, occupancy status, etc.). The GMS acts as a proxy for the power grid, and is the only interface between the EV ecosystem and the power grid, to minimize the attack surface. In the proposed security architecture, the GMS is hardened with strong access control and stringent traffic filtering. The communication between an IED and the CMS/VMS is through a secure socket built on a tailored secure session establishment protocol. Besides, the implementation adopts an "encrypt-then-MAC" paradigm to withhold attacks like [36]. AES-CBC and SHA1-HMAC are respectively used for encryption and payload integrity protection. Interfacing logics are implemented at each server to run JDBC (Java Database Connectivity) over the secure sockets for direct database update and message exchange.

Upon receiving a request to initiate a charging session, the CMS authenticates the EV through running a typical challenge-response protocol with the IED onboard of the EV. User authentication and payment processing then proceed. The CMS acts on behalf of the vehicle in the background to coordinate with the BMS (for verifying the validity of the user registration and billing account, and carrying out billing transactions) and GMS (for granting permission of a charging session based on grid and generator capacity, for interpreting and responding to demand-response or load shedding signals, and for signaling in electricity sell-backs from vehicles). The CMS also updates the VMS on charging station status. When a charging session is terminated or completed, the CMS is responsible for closing all communication sessions. The CMS can be seen as the head-end for all IEDs. In practice, there are multiple CMSs, one for each charging infrastructure provider.

IV. Demand-Response for Smart EV Charging

Built on the ICT infrastructure, a basic demand-response system is implemented for the EV ecosystem, as depicted in Figure 2. The PWM (Pulse Width Modulation) signaling over the control pilot pin of the SAE J1772 plug is leveraged to adjust the charging load. Details of the signaling protocol could be found in [26] or IEC 61851. In brief, by changing the duty cycle of the PWM pulses, a charging station can signal the connected vehicle to adjust its input impedance so as to change the input charging current and power. Through the control pilot pin, the power drawn by the EV can be adjusted between 1 and 19 kW, subject to the onboard charger's rating.

The demand-response system is essential for wide-scale EV adoption. The overloading problem is not purely a mismatch between the supply and demand of electricity, but could be

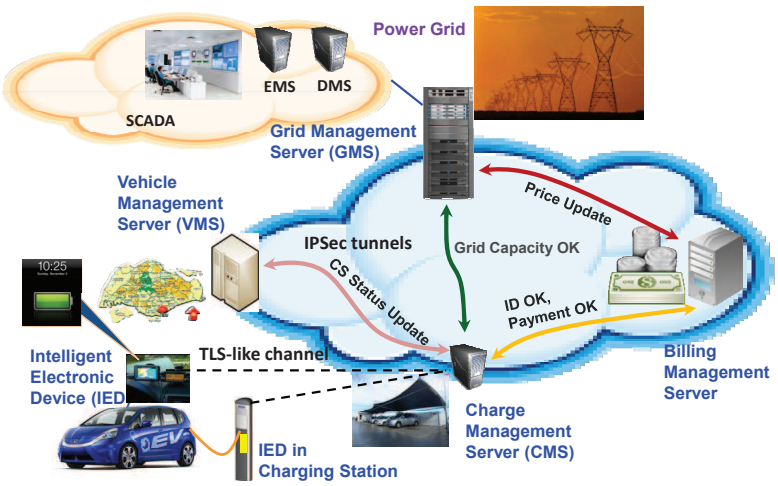

Fig. 1. EV Ecosystem: Architecture and Software Implementation.

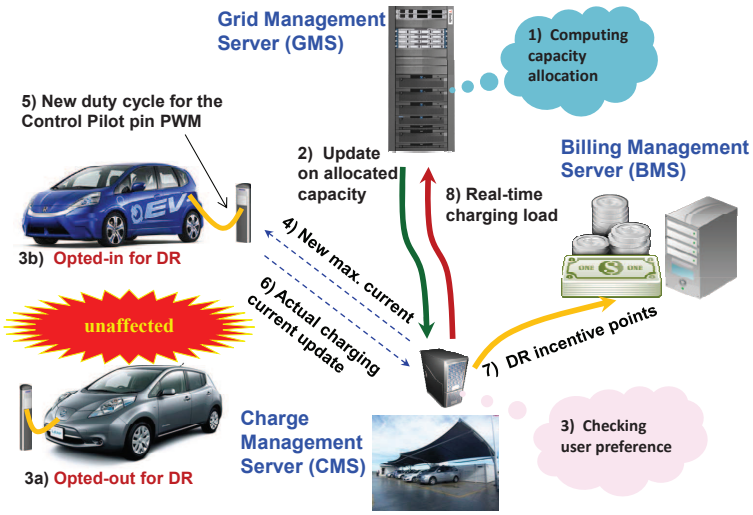

Fig. 2. Demand-response Mechanism for Smart EV Charging.

the overloading of local transformers during peak times. The demand-response system runs as follows:

1) The GMS, based on a certain resource allocation algorithm (using inputs from CMSs and VMS), computes the power allocated for different CMSs.
2) The GMS updates each CMS's allocated power capacity.
3) Through interacting with the VMS, the CMS checks user preference for demand response participation. Only opt-in vehicles will participate in the subsequent load curtailing. Opt-out vehicles will be left unaffected. The CMS then assigns new power consumption caps for all opt-in vehicles to fulfill the constraint.
4) The charging station of each active opt-in vehicle receives a new charging current cap.
5) By moderating the duty cycle of the PWM pulses over the SAE J1772 control pilot pin, the charging station can coordinate with the opt-in vehicle to charge at a new (possibly lower) current value.
6) The charging station then reports the new, actual charging current value back to the CMS.
7) The CMS computes the amount of demand-response incentive points gained by each opt-in vehicle and communicates it to the BMS for recording. Depending on the business model, these incentive points could be used to offset part of the charging cost.
8) The CMS updates the GMS with the actual load.

V. Cybersecurity Requirements

A. Security Objectives for EV Ecosystem

Be it for charging session management or demand response, the EV ecosystem relies heavily on secure message exchange. Message integrity or authenticity is the most important criterion, whereas, availability is also essential but with a relaxed timeliness requirement (in seconds). Confidentiality is important for some messages such as those involving financial information or linked to driver privacy. In addition, M2M communication — widely believed to be the most common

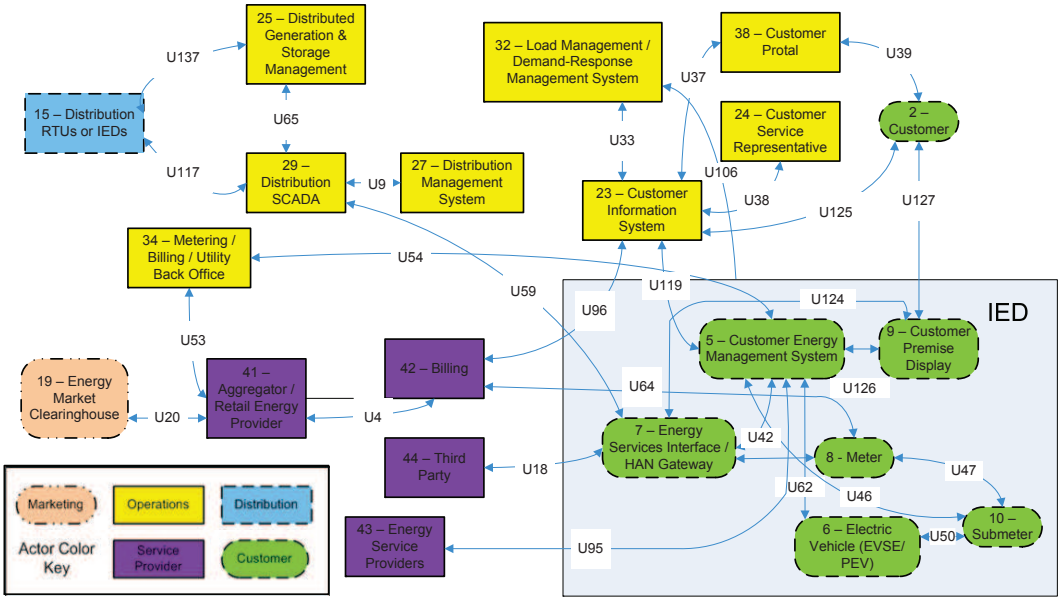

Fig. 3. Identified NISTIR 7628 Actors and Logical Interfaces for EV Charging Infrastructure.

mode of communication in the smart grid — demands a strong assurance of device identities.

Any reasonable security architecture for the EV ecosystem should achieve the following security objectives: 1) correct information with source authenticity for charging coordination; 2) secure payment/transaction processing to achieve transaction integrity/authenticity, consumer non-repudiation and privacy; 3) a safe integration with the power grid information system, requiring strong device security in the EV ecosystem and a secure integration interface with controlled information flow; 4) a strong device identity assurance to ensure secure M2M communication. These objectives are essential to protecting the revenue of utility operators and maintaining the stability of the power grid, while introducing EVs as a new type of mobile appliances and distributed power sources.

An assurance of device identities is particularly important for a number reasons. First, EVs would draw much more power than typical households. Secure device identification is necessary to match up with the increased risk of the large charging load. Besides, to achieve demand side management, an EV must be properly authenticated. Second, for secure M2M communication, devices must be able to authenticate one another automatically without human involvement. Third, in order to support V2G, it is suggested that battery profiling would be necessary to ensure safety and efficiency [13]. Without proper device authentication, such operations could possibly lead to injection of false information into the power grid. Finally, in flat rate charging which is on trial in some countries, sharing a user account for charging multiple EVs would lead to a revenue loss for utility operators. It is thus necessary to identify each EV correctly for each account.

B. NISTIR 7628 Security Requirements

The NISTIR 7628 [27] — a set of guidelines and recommendations for smart grid cybersecurity — and the ENISA counterpart [7] are used to stipulate security requirements for the EV ecosystem. Both have comparable guidelines but ENISA offers recommendations for three different levels of security to accommodate architectural diversity. This paper bases the requirements on the NISTIR 7628 and gives a scalable architecture accommodating 3 different levels of security.

The NISTIR 7628 identifies 46 actors, which are partitioned into seven operation domains: Bulk Generation, Transmission, Distribution, Customer, Markets, Operations, and Service Provider. Over 130 logical interfaces between these actors are identified to provide a concrete specification for the types of information exchanged. Logical interfaces with similar security requirements are grouped into one of the 22 categories, each with a specific set of security requirements and priority values (High, Medium, Low) for the security objectives of confidentiality (C), integrity (I) and availability (A).

In this paper, 21 actors and 28 logical interfaces are identified as relevant to the EV ecosystem, as depicted in Figure 3. The actors in the rectangle are implemented inside the IED platform (both on board of the EV and in the charging station) while the rest are implemented on the four servers: the CMS implements actors 2 and 7; the BMS implements actors 2, 23, 34, 38, 42 and 43; the VMS implements actor 44; the GMS implements actors 15, 19, 25-32, 38, 41 and 43. Table I shows the logical interfaces connecting among these actors, and the security categories these logical interfaces belong to, as well as, the security requirements for these categories. The collective unique security requirements and the common technical requirements needed for the EV ecosystem are summarized in Table II. As a result, the link between any two servers may have different security requirements, which are fully determined by the security criteria of the logical connections (between actors) over that physical link. Instead of stipulating security requirements on a server-to-server link basis, a finer granularity (per actor-to-actor logical connection) is adopted for stipulating the security requirements in this paper, for the sake of efficiency and finer security control.

Category	Logical Interface	C	I	A	Security Requirements
1	U117	L	H	H	SG.AC-14, SG.IA-04, SG.IA-05, SG.IA-06, SG.SC-03, SG.SC-05, SG.SC-07, SG.SC-08, SG.SC-09, SG.SI-07
2	U117, U137	L	H	M	SG.AC-14, SG.IA-04, SG.IA-05, SG.IA-06, SG.SC-03, SG.SC-05, SG.SC-07, SG.SC-08, SG.SC-09, SG.SI-07
3	U117, U137	L	H	H	SG.AC-14, SG.IA-04, SG.IA-05, SG.IA-06, SG.SC-03, SG.SC-05, SG.SC-07, SG.SC-08, SG.SC-09, SG.SI-07
4	U117, U137	L	H	M	SG.AC-14, SG.IA-04, SG.IA-05, SG.IA-06, SG.SC-03, SG.SC-05, SG.SC-07, SG.SC-08, SG.SC-09, SG.SI-07
5	U9	L	M	M	SG.AC-14, SG.IA-04, SG.SC-05, SG.SC-06, SG.SC-07, SG.SC-08, SG.SI-07
7	U96	L	H	M	SG.AC-12, SG.AC-14, SG.IA-04, SG.IA05, SG.SC-03, SG.SC-05, SG.SC-06, SG.SC-08, SG.SC-26, SG.SI-07
9	U4, U20, U53	H	H	L	SG.AC-14, SG.IA-04, SG.SC-05, SG.SC-06, SG.SC-07, SG.SC-08, SG.SC-09, SG.SI-07
10	U33, U59	H	H	H	SG.AC-14, SG.IA-04, SG.SC-05, SG.SC-06, SG.SC-07, SG.SC-08, SG.SC-26, SG.SI-07
13	U95, U119	H	M	L	SG.AC-14, SG.IA-04, SG.SC-03, SG.SC-06, SG.SC-07, SG.SC-08, SG.SC-09, SG.SC-26, SG.SI-07
14	U95, U119	L	H	L	SG.AC-14, SG.IA-04, SG.SC-03, SG.SC-05, SG.SC-06, SG.SC-07, SG.SC-08, SG.SC-09, SG.SC-26, SG.SI-07
16	U18, U37, U38, U39, U125	L	M	M	SG.AC-14, SG.IA-04, SG.SC-03, SG.SC-05, SG.SC-06, SG.SC-07, SG.SC-08, SG.SC-09, SG.SC-26, SG.SI-07
18	U46, U47, U50, U54	L	M	M	SG.AC-14, SG.IA-04, SG.SC-03, SG.SC-05, SG.SC-06, SG.SC-07, SG.SC-08, SG.SC-09, SG.SC-26, SG.SI-07

TABLE I
LOGICAL INTERFACES AND THEIR CATEGORIES FOR EV ECOSYSTEM

	Unique security requirements	**Proposed security solution**
SG.AC-12	Session Lock	account lock and certificate revocation through PKI+OCSP
SG.AC-14	Permitted Actions without Identification or Authentication	electro-mechanical protection + governance, e.g. level 1 charging
SG.IA-04	User Identification and Authentication	PKI+OCSP, authentication
SG.IA-05	Device Identification and Authentication	PKI, challenge-response device authentication, tamper-resistance
SG.SC-03	Security Function Isolation	VLAN, memory/hardware partitioning
SG.SC-05	Denial of Service Protection	a wide range of possible solutions depending on the context, e.g. frequency hopping, overlay DoS protection, robust control, DR compliance
SG.SC-06	Resource Priority	task scheduler, packet tagging
SG.SC-07	Boundary Protection	firewall, network partitioning, VLAN, data diode, intrusion detection
SG.SC-08	Communication Integrity	HMAC, IPsec
SG.SC-09	Communication Confidentiality	AES-CBC, IPsec
SG.SC-26	Confidentiality of Information at Rest	AES-CBC or AES-CCM
SG.SI-07	Software and Information Integrity	signed software update, remote code attestation, HMAC
	Common technical requirements	**Proposed security solution**
SG.AC-06	Separation of Duties	Role Based Access Control (RBAC)
SG.AC-07	Least Privilege	Role Based Access Control (RBAC)
SG.AC-08	Unsuccessful Login Attempt	account lock-out, identity blacklisting
SG.AC-09	Smart Grid Information System Use Notification	implementation details
SG.AC-16	Wireless Access Restrictions	device authentication + wireless security
SG.AC-21	Passwords	password storage in salted hashes
SG.AU-02	Auditable Events	SIEM + governance
SG.AU-03	Content of Audit Records	SIEM + governance
SG.AU-04	Audit Storage Capacity	SIEM + governance
SG.AU-15	Audit Generation	SIEM + governance
SG.AU-16	Non-Repudiation	digital signature used in authentication
SG.CM-07	Configuration for Least Functionality	through governance
SG.CM-08	Component Inventory	through governance
SG.SA-10	Developer Security Testing	through governance
SG.SA-11	Supply Chain Protection	through governance
SG.SC-02	Communications Partitioning	VLAN, AEC-CBC, HMAC, IPsec
SG.SC-11	Cryptographic Key Establishment and Management	PKI+OCSP, challenge-response device authentication
SG.SC-12	Use of Validated Cryptography	through governance
SG.SC-15	Public Key Infrastructure Certificates	PKI
SG.SC-16	Mobile Code	signed code update
SG.SC-18	System Connection	challenge-response authentication, IPsec
SG.SC-19	Security Roles	Role Based Access Control
SG.SC-20	Message Authenticity	HMAC, IPsec
SG.SC-21	Secure Name /Address Resolution Service	PKI
SG.SC-22	Fail in Known State	implementation details
SG.SC-30	Smart Grid Information System Partitioning	VLAN, memory/hardware partitioning
SG.SI-02	Flaw Remediation	through governance
SG.SI-08	Information Input Validation	implementation details
SG.SI-09	Error Handling	implementation details

TABLE II
NISTIR 7628 SECURITY REQUIREMENTS FOR EV ECOSYSTEM

VI. Scalable Cybersecurity Architecture

Figure 4 presents a comprehensive view of security components in the proposed cybersecurity architecture. The mapping between these security components and the NISTIR 7628 security requirements addressed is depicted in Table II. For requirements which can only be satisfied by governance or implementation details (with no specific technologies), no specific security mechanisms are listed. Due to space limitation, a full description of all the components will not be discussed here. In particular, some components, such as firewalls, SIEM (Security Incident and Event Management) and VLAN (Virtual Local Area Network), are standard tools. Yet, a more focused discussion on mechanisms for assurance of device identities is presented, especially those unique in this paper, including the mutual authentication and certificate issuing protocol, and the RBAC schema (Figure 4).

The NISTIR 7628 does not specify whether symmetric key or asymmetric key techniques should be used. In fact, the security requirements could possibly be satisfied by either. However, for scalability, the asymmetric key approach is preferable, because symmetric key management for the multi-party setting (multiple charging infrastructure operators and multiple EVs) could be complex, in particular, when compromised parties is a practical reality, and huge key storage is necessary for a large EV ecosystem.

As shown in Figure 4, different components could be combined to achieve three levels of security (High, Medium, Low), based on the available physical protection and the maximum power consumption. The rationale is two-fold. First, if the charging station is deployed in a physically protected area (meaning a smaller attack surface), a low security level should be sufficient. Second, if the actual usage involves only low power consumption, the EV could simply be treated as a usual home appliance with a low security level needed.

A defence-in-depth approach [1] is taken. In general, multiple mechanisms or components are used to offer protection against a given type of risk or attacks, so that the failure of one component would not cause a total compromise or complete security breach. In the cybersecurity architecture, users and EVs have separate certificates. While the former is used for billing and financial transaction processing, the latter is largely for device identification. There are two level of security mechanisms to assure device identities, namely, challenge-response authentication and certificate management (concerning certificate issuing, storage and revocation). It is assumed that a binding between the IED and EV exists, say, through some CAN bus hardware security mechanism.

A. Challenge-Response Device Authentication

The identity of an IED is based on a 3-tuple $(sk_I, pk_I, cert(pk_I))$ where sk_I and pk_I are its private and public keys, and $cert(pk_I)$ is the certificate signed by the VMS to certify pk_I's authenticity. Both sk_I and pk_{VMS} (the VMS's public key) need to be stored in the tamper-resistant storage or secure element of the IED, as physical tampering is practically possible. Such storage is provided by the NXP-ATOP [25].

Shown in Figure 5 is the protocol for mutual authentication between an EV and the server (CMS/VMS). The structure of the protocol is mainly based on the TLS handskake, except for a number of optimizations. First, version checking is skipped. Second, $state_{IED}$ (indicating the CAN bus status of the IED) is included in the client's response for verifying the IED's binding status. The protocol is based on Diffie-Hellman key exchange, which can be seen as two interleaving challenge-response instances. The protocol works with a generator g of a multiplicative group, say, $\mathbb{Z}_p^*$ for a large prime p. The client hello includes a challenge g^a for the server, and g^a also functions as the nonce to prevent the playback attack. The server replies by signing on g^a and g^b (g^b is a new nonce chosen by the server) to prove its knowledge of the private key sk_S. g^b is a challenge for the IED, which signs on it, along with the $state_{IED}$, to prove its knowledge of sk_I. If signature verification passes on both sides, the authentication succeeds, and g^{ab} is hashed to form the session keys of a new private and authenticated channel for subsequent message exchange.

B. Digital Certificate Management

A typical initiation process for installing an IED is shown in Figure 6. When an owner registers his EV, the VMS generates a public/secret key pair (pk_I, sk_I), and signs a certificate $cert(pk_I)$ for pk_I. All these will be installed on the IED along with the VMS's public key pk_{VMS}. Only sk_I and pk_{VMS} need to be stored in tamper-resistant storage. The crux is that even the owner has no access to sk_I and cannot modify pk_{VMS}, since the owner could be a potential adversary.

The VMS keeps a CRL (Certificate Revocation List) listing all the revoked certificates. The IED has to regularly obtain from the VMS an OCSP (Online Certificate Status Protocol) proof that its certificate remains legitimate. The VMS needs not be online for each session establishment. The idea is as follows: the VMS signs (with a date) the root of a Merkle tree formed over the revoked certificates (as leaves) in sequential order by iteratively applying a cryptographic hash function such as SHA1; to generate a proof of validity for a particular certificate C_{EV}, the VMS look up two adjacent certificates in the tree such that C_{EV}'s serial number lies in between; the proof then includes the VMS's signature of the root, the two adjacent certificates, and all the hash values of the nodes off the path from the two certificates to the root (those marked blue in Figure 7). To verify the proof, any verifier just needs to reconstruct the hash value of the root of the Merkle tree from the given hash values and certificates, and checks whether the signature matches for the root hash.

VII. Evaluation and Security Analysis

The proposed system is evaluated in terms of key storage requirements, computational complexity, response time of demand response, and security. The communication between the CMS and an IED is secured with AES-CBC for confidentiality and SHA1-HMAC for integrity. The two sessions keys are established using Diffie-Hellman (DH) key exchange over a 1024-bit prime p. A 320-bit DSA (Digital Signature Algorithm) — with p as the modulus and a 160-bit exponent q — is adopted for entity authentication and certificate signing.

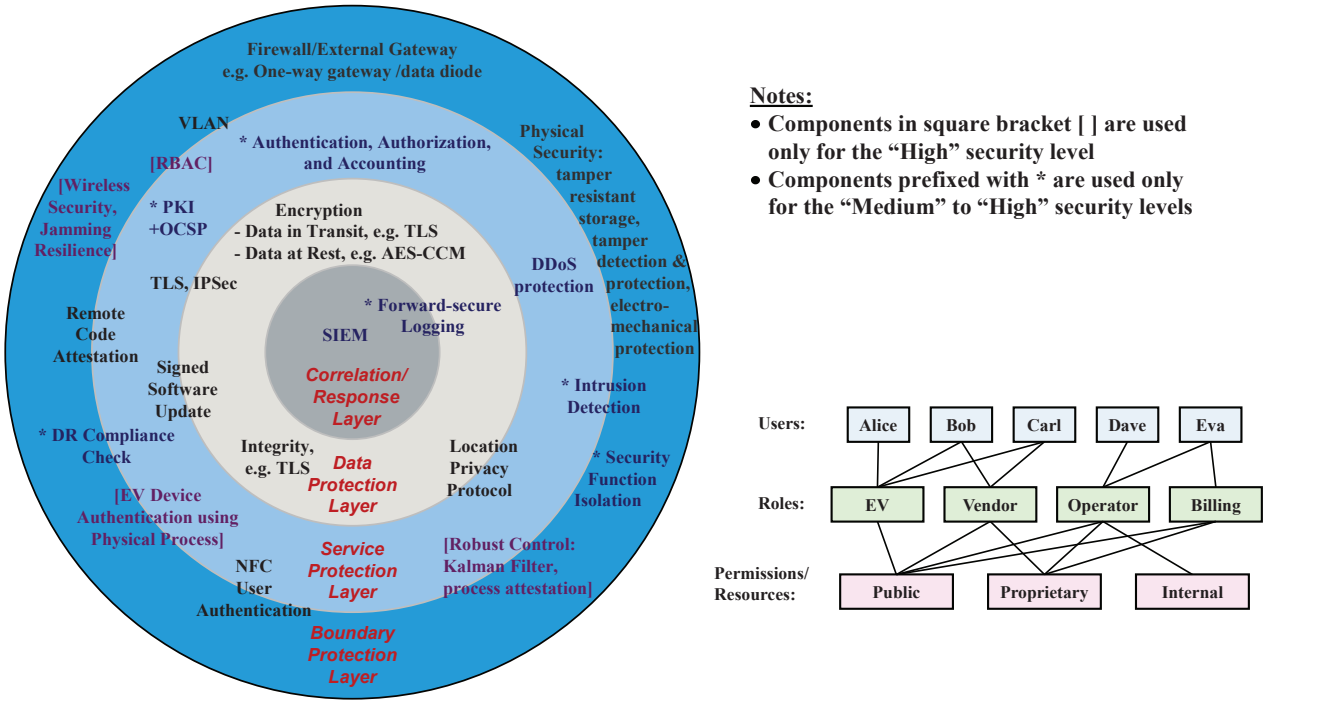

Fig. 4. A Scalable Defence-in-depth Cybersecurity Architecture.

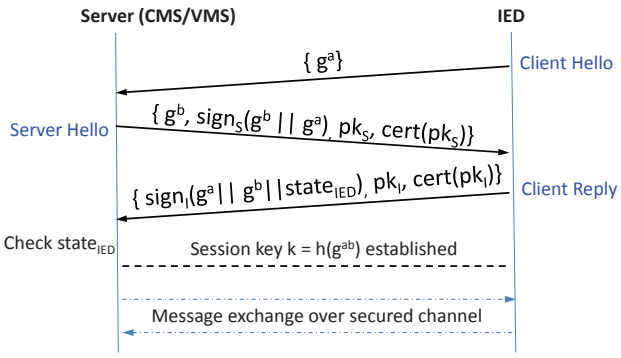

Fig. 5. Challenge-Response Device Authentication for EV Ecosystem.

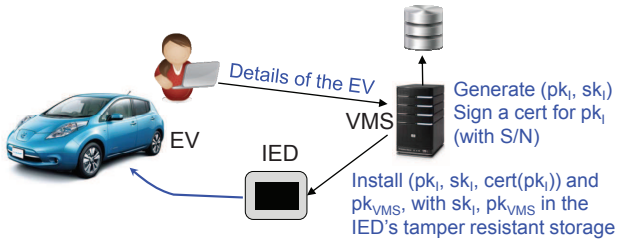

Fig. 6. Certification Initialization for EV Ecosystem.

In the experiment, the IED with its security mechanisms is implemented on an NXP-ATOP OM12000 module, an ARM9 processor with tamper-resistant storage for private keys, and GPRS for communication to the CMS which is the hub. The NXP-ATOP is a reasonable benchmark platform since it is commonly used in embedded onboard units for typical automobile applications. The BouncyCastle Java security library is

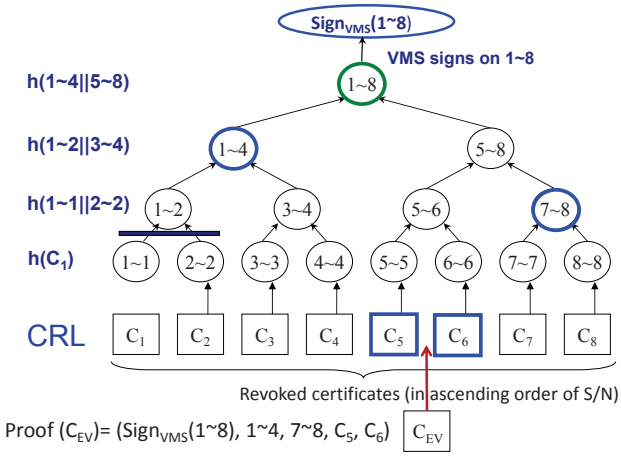

Fig. 7. OCSP and CRL for Certification Revocation.

used to implement the cryptographic algorithms.

A. Storage and Computational Complexity

Storage and computational complexity is usually a major impediment to securing resource-constrained embedded systems in the smart grid. The complexity of the proposed security architecture is summarized by the following theorem.

Theorem 1: Given p, the modulus for the Diffie-Hellman key exchange and DSA, and q, the modulus for the DSA exponent, the session key establishment takes $O(4 \cdot |p|^3 + 1.5 \cdot rtt)$ where rtt is the round-trip time for sending a message between the IED and the backend server. For an l-bit message m, the computational time of the security mechanisms in the data transfer phase is $O(\lceil \frac{l}{n} \rceil \cdot t_{cipher} + 2 \cdot t_{hash})$, where n is the block size of the block cipher, t_{cipher} and t_{hash} are the

computational complexity of the block cipher (AES) and the hash function (SHA1) respectively. Tamper-resistant storage needed on the IED is then $(|p| + |q|)$ bits.

Proof: With reference to Figure 5, the session key setup involves sending two messages from the IED to the server and one message in the reverse direction, thus making up a transmission time of approximately $1.5 \times rtt$, and the computation of: (1) the client hello involving an exponentiation in mod p, with a complexity of $O(|p|^3)$; (2) the server hello involving 2 signature verification operations requiring $2 \cdot t_{verify}$ and a hash computation on a message of length $2|p|$ requiring t_h; (3) the client reply involving 1 signing operation requiring t_{sign} and a hash computation on a message of length $2|p| + |state_{IED}|$ taking approximately t_h (since $|state_{IED}| << |p|$); and (4) hashing g^{ab} (of length $|p|$) to generate the session key requiring $t_h/2$. Summing up, the total computation time is $O(|p|^3) + 2 \cdot t_{verify} + t_{sign} + 2.5 \cdot t_h$. For DSA, $t_{sign} \approx O(|p|^3 + 3 \cdot |q|^2 + |q|) \sim O(|p|^3)$, and $t_{verify} \approx O(2 \cdot |p|^3 + |p|^2 + 3 \cdot |q|^2) \sim O(2 \cdot |p|^3)$. The total computation time is: $O(4 \cdot |p|^3)$ (since $|p|^3 >> t_h$). Adding in the transmission time and the processing time by the server (denoted by t_{server}), the session key establishment takes $O(4 \cdot |p|^3) + 1.5 \cdot rtt + t_{server}$. Since the server is much more powerful than the IED, t_{server} could be assumed negligible compared with the IED computation time. Hence, the session key establishment takes $O(4 \cdot |p|^3 + 1.5 \cdot rtt)$. For a message m sent or received by the IED, the security mechanisms involves 1 CBC and 1 HMAC operation. The CBC operation involves $\lceil \frac{l}{n} \rceil$ invocations of the block cipher algorithm, while the HMAC operation involve evaluating the hash function twice. The computation time is therefore: $O(\lceil \frac{l}{n} \rceil \cdot t_{cipher} + 2 \cdot t_{hash})$.

For storage, the IED needs to store its own private key requiring $|q|$ bits and the VMS's public key (for verifying authenticity of certificates) requiring $|p|$ bits. A total of $(|p|+|q|)$ bits of tamper-resistant storage is thus required. ■

In the actual experiment, $|p|$ is 1024 bits and $|q|$ is 160 bits. As a result, the proposed architecture requires 148 bytes of tamper-resistant storage on the IED (20 bytes for the IED's secret key and 128 bytes for the VMS's public key), altogether taking up <1% of the 80 kbytes capacity of the NXP-ATOP, which is also insignificant for typical tamper-resistant storage.

Table III shows the computational time for establishing the session keys and securing a message in the data transfer phase, which are representative to indicate the computational efficiency of the proposed architecture, because the former is a key step for the root of trust and the latter is the most frequent security computation. The average time taken to establish a session key using Diffie-Hellman over a 1024-bit p is 17.77s, without using the SMX (security processor) of the NXP-ATOP, and is substantially reduced to 2.8s with the SMX. For a 2048-bit p, the time is 148.21s and 22.8s respectively. The processing time at the CMS is also measured, which is in the range of tens of ms (negligible compared to that at the IED), thus confirming the assumption of Theorem 1. To measure the performance in the bulk data transfer phase, a fixed-sized packet is repeatedly sent from the IED to the CMS which acknowledges the receipt. The average round-trip response time is measured with and without the security mechanisms activated; the difference divided by two is used as an estimate for the computational overhead introduced by the security mechanisms. Different-sized packets are used in the experiments, but only representative cases are shown. Without security enabled, the round-trip response time is 2.85s and 3.53s respectively for a message size of 292 bytes and 548 bytes. The similar response time is possibly because each message for the two cases fills in the same number of GPRS frames. The average latency caused by the security mechanisms (without the SMX) for the two cases is respectively 18% and 26% of the round-trip latency; for most of the tested cases, the security mechanism overhead is no more than 26%. With the SMX, the overhead is only about 2-4% of the round-trip latency. In other words, the developed security mechanisms are sufficiently lightweight even for typical embedded platforms (especially when the SMX is used), thus easing the deployment of full security coverage for all devices in the smart grid.

	without SMX	with SMX
session key setup (in sec)		
$\|p\|$ = 1024 bits	17.77	2.8
$\|p\|$ = 2048 bits	148.21	22.8
securing data transfer (in sec)		
l = 292 bytes	0.521	0.071
l = 548 bytes	0.915	0.125

TABLE III
COMPUTATIONAL TIME

B. Demand Response Performance

Demand response experiments are carried out on a Mitsubishi i-MiEV to measure the proposed system's response time, a key performance metric for demand response mechanisms [29], [34]. A faster response time usually translates into greater usability in a wider range of applications and demand response models. In the experiments, load curtailing instructions are sent from the GMS. A charging session is started with the maximum allowable current (13A) and the current is subsequently reduced in 2A steps. The time lapse from instruction issuing to reaching the new steady current is: 2.92s (average), 1.47s (min), 4.83s (max). The experiments are repeated but the current is reduced in a single step from 13A to 6A (IEC61851's minimum allowable current). The corresponding delay is: 3.45s (average), 1.72s (min), 5.01s (max). Note that this delay only involves a message flow in one direction and the GMS and CMS are virtual machines on the same physical machine. The proposed system could fully respond in seconds, comparable with the highest grades in different standards: the 'Regulation' grade (best grade) of [29] requires time to respond <30s and time to fully respond <5 min; the 'Frequency Response' or 'Fast Reserve' grade of [34] requires a response time <2s and <2 min respectively.

According to [29], the proposed mechanism's performance is sufficient for continuously accommodating random unscheduled deviations in the net load, that is, capable to support real-time demand side management. Indeed, the system fulfils the timing requirement of the smart load which suffices for all range of demand response models in [30], from energy

efficiency to virtual spinning reserve. In other words, the proposed ICT and cybersecurity architecture is lightweight enough to attain a latency guarantee sufficiently covering all the existing demand response models. Besides, the proposed system (focusing on the design of demand response mechanisms at the lower level) is complementary to the existing work in the literature focusing on business models [20] and resource allocation strategies [18], [21], [24] of demand response. It provides a logical interface for these higher level mechanisms for implementing a concrete demand response system for EVs.

C. Security

The proposed security architecture could withstand different kinds of attacks: eavesdropping, message injection/modification, device impersonation, replaying a previous session, IED cloning, gaining access with a compromised or blacklisted IED. The architecture emphasizes a strong assurance of digital identities, more concretely, device identification, for different devices. As the power grid has to accept and connect mobile loads (EVs) owned by a large number of other parties which are not necessarily trusted, this is an essential criterion for safe integration of the EV ecosystem and the smart grid, allowing the power grid to have full access control. In fact, the ability to identity and locate where and when an EV is connected to the power grid is a determining factor for a successful rollout of EVs in a large scale [10].

A successful run of the entity authentication protocol in Section VI-A results in a *unique* session key k, through which a private and authenticated channel can be established between an IED and the CMS and other servers. The security properties of AES-CBC and HMAC (keyed by k) — more specifically, indistinguishability against chosen plaintext attacks and unforgeability against chosen message attacks — respectively ensure the confidentiality and integrity of all messages. Provided that the private keys of the IED and CMS remain secret, the challenge-response authentication protocol guarantees that nobody besides the designated EV and the CMS has knowledge of k. Other EVs would not know k either. With k, any injected or modified messages could be easily detected through HMAC verification, and thus neglected without deceiving innocent EVs into carrying out harmful actions on the power grid. Similarly, encryption based on AES-CBC assures confidentiality of all messages. As long as k is regularly updated, the confidentiality of each message could be guaranteed with high probability. Nonetheless, availability has to rely on other mechanisms such as robust control and denial of service protection which are not in this paper's scope.

Possessing the designated secret key sk_I and a valid certificate $cert(pk_I)$ is necessary for an EV to pass the device authentication (Fig. 5), leading to two implications: first, impersonation by an attacker is guarded; second, the access privilege of a valid but malicious EV can be revoked by the power grid. Without knowledge of sk_I, there is negligible probability for any attacker to generate a valid signature $sign_I(g^a||g^b||state_{IED})$ to pass the CMS's verification. Similarly, in the reverse direction, an attacker could not impersonate the CMS. Since new random numbers a and b are used for each new session, replay attacks would not succeed.

For the case of malicious or compromised EVs, IED cloning is guarded against by the IED's tamper-resistant storage and a rigorous key issuing procedure (Fig. 6). Storing the server public key in the tamper-resistant storage also ensures that the root of trust lies in the key issuing procedure, withstanding server impersonation. If a legitimate EV is detected malicious, the power grid can blacklist it through certificate revocation to ban its subsequent access. If a blacklisted EV attempts to connect, it has to prove the validity of its public key through the necessary data in the Merkle tree (Fig. 7) which can only be obtained from the VMS. The security properties of the Merkle tree and the digital signature scheme ensure that these validation data cannot be easily forged.

D. Scalability for Large Scale Deployment

The experimental results of this paper should remain holding as the number of EVs in the ecosystem increases. Adding a new EV can simply be done by installing a new IED. Since asymmetric key cryptography is used, the size of the tamper-resistant storage needed on each IED for storing the keys remain constant, regardless of the number of EVs or charging stations. Only one private key of the IED and one public key of the VMS need to be stored. The computational overhead for securing data in the transfer phase remains the same for each IED despite the addition of a new EV since no shared server resources are used in such computation. For session key establishment, the shared resources include the backend servers and the communication network (which is GPRS in this case). Since the servers are virtual machines (VMs), the server resources could be readily scaled up by adding VMs. In fact, the proposed architecture already assumes multiple CMS servers. Besides, the capacity of a GPRS network is able to support hundreds of thousands devices; in other words, the results for the key establishment and demand-response in this paper remain holding for a significantly larger EV ecosystem. The bottleneck of key establishment remains at the IED computation overhead, which is independent of the number of EVs. Hence, the proposed architecture is scalable.

VIII. Conclusions

To fill the gap for integrating a large-scale electric vehicle ecosystem with the smart grid, a secure, intelligent ICT infrastructure is designed and implemented. To facilitate utility operators to handle wide-scale adoption of EVs, a demand response system is presented. The system achieves a fast response time and has a generic interface to support a wide range of demand response models. Besides, a comprehensive cybersecurity architecture tailored for the envisioned EV ecosystem is given, with lightweight security mechanisms, which provides a strong assurance of device identities — a needed basis for M2M communications and secure networked control in the smart grid. The design is implemented on the NXP-ATOP and the overheads are practically reasonable.

Acknowledgment

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

REFERENCES

[1] National Secuity Agency. Defence in depth: A practical strategy for achieving information assurance in todays highly networked environments. At http://www.nsa.gov/ia/_files/support/defenseindepth.pdf.

[2] M. Badra and S. Zeadally. Design and performance analysis of a virtual ring architecture for smart grid privacy. *IEEE Trans. on Information Forensics and Security*, 9(2):321–329, 2014.

[3] A. C.-F. Chan and J. Zhou. Cyber-physical device authentication for the smart grid electric vehicle ecosystem. *IEEE JSAC*, 32(7):1509–1517, 2014.

[4] H. Chaudhry and T. Bohn. Security concerns of a plug-in vehicle. In *IEEE ISGT'12*, pages 1–6, 2012.

[5] S. Das, Y. Ohba, M. Kanda, D. Famolari, and S. K. Das. A key management framework for AMI networks in smart grid. *IEEE Comm. Magazine*, 50(8):30–37, 2013.

[6] J. P. Degabriele and K. G. Paterson. Attacking the IPsec standards in encryption-only configurations. In *IEEE Symposium on Security and Privacy*, pages 335–349, 2007.

[7] ENISA. *Smart Grid Security — Recommendations for Europe and Member States*. July 2012.

[8] C.-I. Fan, S.-Y. Huang, and Y.-L. Lai. Privacy-enhanced data aggregation scheme against internal attackers in smart grid. *IEEE Trans. on Ind. Inf.*, 10(1):666–675, 2014.

[9] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymious, G. Kalogrids, M. Sooriyabandara, Z. Zhu, S. Lambotharan, and W. H. Chin. Smart grid communications: Overview of research challenges, solutions, and standardizations activities. *IEEE Communications Surverys & Tutorials*, 15(1):21–38, 2013.

[10] Gartner. Hype cycle for smart grid technologies, 2012, July 2012.

[11] V. G. Gungo, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke. Smart grid technologies: Communication technologies and standards. *IEEE Trans. on Ind. Inf.*, 7(4):529–539, November 2011.

[12] V. G. Gungo, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke. A survey on smart grid potential applications and communication requirements. *IEEE Trans. on Ind. Inf.*, 9(1):28–42, February 2013.

[13] ISO/IEC. *ISO/IEC 15118: Vehicle to grid communication interface*. 2013.

[14] C. Jouvray, G. Pellischek, and M. Tiguercha. Impact of a smart grid to the electric vehicle ecosystem from a privacy and security perspective. In *EVS27*, pages 1–10, 2013.

[15] S. Lee, Y. Park, H. Lim, and T. Shon. Study on analysis of security vulnerabilities and countermeasures in ISO/IEC 15118 based electric vehicle charging technology. In *ICITCS'14*, pages 1–4, 2014.

[16] M. LeMay and C. A. Gunter. Cumulative attestation kernels for embedded systems. *IEEE Trans. on Smart Grid*, 3(2):744–760, 2013.

[17] N. Liu, J. Chen, L. Zhu, J. Zhang, and Y. He. A key management scheme for secure communications of advanced metering infrastructure in smart grid. *IEEE Trans. on Ind. Elect.*, 60(10):4746–4756, 2013.

[18] T. Logenthiran, D. Srinivansan, and T. Z. Shun. Demand side management in smart grid using heuristic optimization. *IEEE Trans. on Smart Grid*, 3(3):1244–1252, September 2012.

[19] G. Lu, D. Seed, M. Starsinic, and C. Wang. Enabling smart grid with ETSI M2M standards. In *WCNCW'12*, pages 148–153, 2012.

[20] J. Ma, J. Deng, L. Song, and Z. Han. Incentive mechanism for demand side management in smart grid using auction. *IEEE Trans. on Ind. Inf.*, 5(3):1379–1388, May 2014.

[21] A.-H. Mohsenian-Rad, V. W. S. Wong, J. Jatskevich, R. Schober, and A. Leon-Garcia. Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid. *IEEE Trans. on Smart Grid*, 1(3):320–331, December 2010.

[22] M. A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan. Smart electric vehicle charging: Security analysis. In *IEEE ISGT'13*, pages 1–6, 2013.

[23] North American Electric Reliability Corporation (NERC). *Reliability Considerations from the Integration of Smart Grid*. December 2010.

[24] K. H. S. V. S. Nunna and S. Doolla. Responsive end-user-based demand side management in multimicrogrid environment. *IEEE Trans. on Ind. Inf.*, 10(2):1262–1272, May 2014.

[25] NXP. *NXP Automotive Telematics On-board unit Platform (ATOP)*. http://www.nxp.com/documents/leaflet/939775016910.pdf.

[26] Society of Automobile Engineers (SAE). J1772: Electric vehicle and plug in hybrid electric vehicle conductive charge coupler, 2012.

[27] National Institute of Standards and Technology (NIST). *NISTIR 7628: Guidelines for Smart Grid Cyber Security, Vol. 1-3*. August 2010.

[28] National Institute of Standards and Technology (NIST). *NISTSP 1108: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*. January 2010.

[29] D. J. Olsen, N. Matson, M. D. Sohn, C. Rose, J. Dudley, S. Goli, S. Kiliccote, M. Hummon, D. Palchak, P. Denholm, J Jorgenson, and O. Ma. Grid integration of aggregated demand response, part I: Load availability profiles and constraints for the western interconnection, September 2013. LBNL Report LBNL-6417E.

[30] P. Palensky and D. Dietrich. Demand side management: Demand response, intelligent energy systems, and smart loads. *IEEE Trans. on Ind. Inf.*, 7(3):381–388, August 2011.

[31] M. A. Rahman, E. Al-Shaer, and P. Bera. A noninvasive threat analyzer for advanced metering infrastructure in smart grid. *IEEE Trans. on Smart Grid*, 4(1):273–287, 2013.

[32] C. Rottondi, G. Verticale, and C. Krauss. Distributed privacy-preserving aggregation of metering data in smart grids. *IEEE JSAC*, 31(7):1342–1354, 2013.

[33] W. Su, H. Eichi, W. Zeng, and Chow M.-Y. A survey on the electrification of transportation in a smart grid environment. *IEEE Trans. on Ind. Inf.*, 8(1):1–10, February 2012.

[34] Energy UK. Smart demand response: A discussion paper. Available at http://www.energy-uk.org.uk/publication/finish/5/701.html.

[35] B. Vaidya, D. Makrakis, and H. T. Mouftah. Security mechanism for multi-domain vehicle-to-grid infrastructure. In *Globecom'11*, pages 1–5, 2011.

[36] S. Vaudenay. Security flaws induced by CBC — applications to SSL, IPSEC, WTLS ... In *Eurocrypt'02*, pages 534–546, May 2002.

[37] Y. Ye, Q. Yi, and R. Q. Hu. A secure and efficient scheme for machine-to-machine communications in smart grid. In *IEEE ICC'12*, pages 167–172, 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 on the editorial board of China Communications. 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).