IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON THE INTERNET OF ENERGY: ARCHITECTURES, CYBER SECURITY, AND APPLICATIONS

Received December 23, 2017, accepted January 19, 2018, date of publication February 5, 2018, date of current version March 16, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2799543

Fog Computing-Enabled Secure Demand Response for Internet of Energy Against Collusion Attacks Using Consensus and ACE

GAOLEI LI[1], (Student Member, IEEE), JUN WU[1], (Member, IEEE), JIANHUA LI[1], ZHITAO GUAN[2], (Member, IEEE), AND LONGHUA GUO[1], (Student Member, IEEE)

[1]Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
[2]School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China

Corresponding author: Jun Wu (junwuhn@sjtu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61571300 and Grant 61431008 and in part by the National Key Research and Development Program of China under Grant 2016QY01W0104.

ABSTRACT Internet of Energy (IoE) is a novel decentralized energy supplying paradigm, which integrated highly scalable and distributed energy resources to satisfy the various demands in future green applications. The existing works focus on the monitor and control of the state of networked energy storage devices. However, optimizing the security of demand response (DR) management with given energy states under IoE circumstance is rarely studied. Due to the connection to the Internet, the DR management in IoE faces a number of unique cyber-physical security challenges. First, as distributed energy resources have a large number of stakeholders and any illegal skip-level energy access may cause disastrous results, it requires fog computing paradigm to enforce a more secure DR management. Second, in the localized energy networks of IoE, a corrupt DR participator can maliciously read and write DR strategies by using collusion attacks (e.g., reputation-based cheating and unfair competing). To address these issues, we propose a fog computing-enabled secure demand response (FSDR) scheme for IoE against collusion attacks using consensus and access control encryption. In FSDR, the fog node was reconstructed as a sanitizer to randomly transfer encrypted energy states and DR strategies with homomorphic operations. Moreover, a simulated annealing-based consensus algorithm was presented to examine the validity of the energy states and DR strategies. In addition, we establish the mathematical models of collusion attacks and attack defense approaches. The performance evaluation validated its efficiency.

INDEX TERMS Internet of Energy (IoE), fog computing, demand response (DR), consensus, access control encryption (ACE).

I. INTRODUCTION

Internet of energy (IoE) is a decentralized energy supplying paradigm by developing a revolutionary vision of smart grids into the Internet [1], [2]. The IoE has been perceived to provide an interface between distributed alternative energy generating sources and various green applications (e.g., green industry and city). To perform the targeted applications and realize its functionalities, IoE adopts a a series of information and communication technology (ICT) to monitor and control the distributed energy resources and the behavior of consumers to gain useful insights for the optimization of energy utilization. In traditional power grid, a satisfactory demand response (DR) management is critical for operators to enforce peak-load shifting. Nowadays, IoE brings DR management into a revolutionary period [3].

The existing DR management schemes mainly consisted of two branches, namely, centralized and decentralized schemes. In terms of centralized schemes, energy information is collected from individual distributed sources and transmitted back to a central location, usually the cloud, for analyzing and access. In the decentralized case, the energy information is stored locally or at some designated nodes within the network instead of immediately transmitting them to a remote center out of the network. This energy information

can be accessed by IoE users in a distributed way. Compared to the centralized schemes, decentralized DR reduces response latency since the energy information is no longer transmitted to a centralized location out of the network [4]. Meanwhile, it reduces electricity transmission losses. As both distributed alternative energy generating devices and advanced energy storage devices are now possible to be equipped with smart sensors [5]–[8], balancing electricity demands on local aggregator becomes much more efficient than transmitting over cloud [9], [10]. Thus, decentralized DR implies higher energy efficiency. Additionally, decentralized DR improves the robustness of energy supplying against large-area blackout, which is inevitable in the centralized scheme. These advantages together result in the recent increasing popularity of decentralized DR.

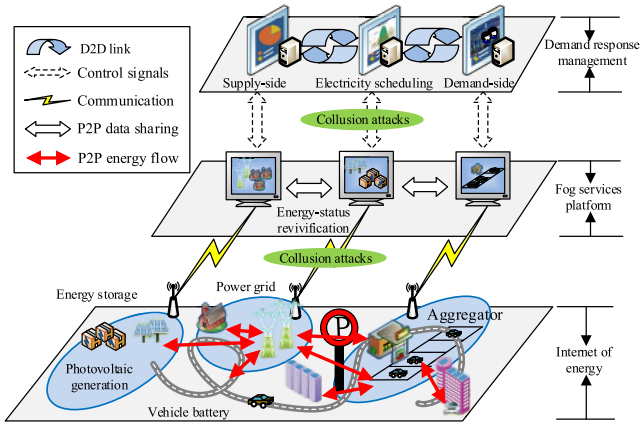


FIGURE 1. The illustration of fog computing based DR management in IoE.

As a large amount of electricity and data are distributedly stored and maintained in individual accumulators, even mobile vehicles, the recent works innovatively exploited some emerging technologies (such as fog computing, big data) to aggregate and mine energy information to achieve the above functions [11]–[13]. Fig. 1 illustrates the architecture of DR management for fog computing in IoE. By pulling down the intelligent data processing services into IoE edge devices, fog computing has presented a number of promising advantages (such as ultra-low latency, context-awareness, and privacy-preserving) [14]. However, fog computing still cannot provide satisfactory decentralized DR management to adapt to the rigorous requirements of future green applications due to a number of security challenges. Actually, it is very distinct that security threats of fog computing in IoE are cyber-physical. Firstly, in many application scenarios, the electricity is closely related to safety issues and should be accessible only to authorized users. Moreover, in some specific application scenes, electricity aggregated from distributed sources may belong to different security levels and thus are meant to be accessed only by specified users. Therefore, it requires fog computing to enable more meticulous DR, in which accessibility of a particular energy to users is exclusively based on access control list and illegal energy occupation may cause disastrous results. Secondly, since fog computing usually serves for distributed energy management, a corrupt aggregator is easy to launch collusion attacks. Moreover, resource-constrained fog node is also easily subject to strong attacks such as distributed denial of service attacks (DDoS) [15]. Thus, illegal reading and writing DR strategies is extremely dangerous.

The existing works on the security of fog computing cannot simultaneously deal with the above two challenges in IoE due to the following reasons. Different from data management that can easily achieve high security by improving traditional security strategies (e.g., authentication, encryption, and access control), secure DR management in IoE needs a trusted, accurate, and tamper-proof enforcement circumstance to resist the collusion attacks. In this paper, we proposed a fog computing-enabled secure demand response (FSDR) scheme for IoE against collusion attacks using consensus and ACE. In FSDR, the fog node was reconstructed as a sanitizer to randomly transfer encrypted energy states and DR strategies with homomorphic operations. Moreover, a simulated annealing based consensus algorithm was presented to examine the validity of the energy states and DR strategies. Contributions of this paper mainly contained the following two aspects. 1) A secure networking circumstance for DR strategies' transmission and enforcement was established. 2) A fog computing based secure DR (FSDR) scheme was proposed based on the consensus and ACE to prevent from convert collusion attacks.3) We designed a simulation approach to the defense utility of FSDR scheme.

The remainder of this paper is structured as follows. Section II gives an overview of the related work and states the strengths of the proposed scheme. Section III describes the architecture of FSDR and its core components. Section IV introduces the design principles of FSDR and discusses the security analysis. Further, the extension of DR for large-scale IoE is also formulated in this section. Performance evaluation is demonstrated in Sections V. Finally, Section VI draws the conclusion and gives the future work.

II. RELATED WORK

Typically, the improvement in energy utilization can be done by DR management [16], [17]. As the increasing popularity of distributed energy, decentralized DR requires deploying more smart devices (such as intelligent electric devices, smart meters, and smart transformers) to monitor and control the energy sources and users' behaviors. As the smart devices increase, the amount and velocity of data lead to communication congest in smart grid, which aggravates the difficulty of decentralized DR management. Meanwhile, Internet of energy (IoE) aims to build a visible, scalable and reliable smart grids for future green applications by the Internet. Large-scale power grid infrastructures connecting to Internet incurs some specific cyber-physical challenges. Thanks to the recent advances in information and communication technology, deploying fog computing in IoE to optimize the decentralized DR in smart grid has drawn increasing attention. Processing energy information on the edge network

elements becomes much more efficient than transmitting over the Internet [18]–[20].

It has been claimed that efficiency, flexibility, and resiliency are the most important requirements of future green applications, and consensus-based distributed energy management (including state estimation, economic dispatch, and optimal power flow) can be as good as the centralized optimal solutions [21]. Especially, in mobile energy network (e.g. vehicle-to-grid [22]), localized electricity trading among plug-in hybrid electric vehicles has better performance on security and users' experience (maximized social welfare), for it doesn't need to transport electricity over long distances and through complex electricity transportation meshes [23]. Since demand side can reliably contribute to primary frequency control [24], the recent works focus on exploiting decentralized DR management to optimize frequency control [25], [26]. In the past, decentralized DR usually served for small-scale power systems such as microgrid, but not suitable to large-scale connected distributed energy resources. Sakurama *et al.* [27] proposed a communication-based decentralized DR, in which control signals (corresponding to prices and/or incentives) are generated in communication networks consisting of smart meters, but not by a central authority. In a word, IoE makes distributed prosumers that can access the Internet to participate in DR management [28]. However, all of the existing solutions required power users to exchange information including their electricity usage, which leads to the leak of privacy data.

The security and privacy-preserving issues of fog computing are still in the initial stage. Studies on security and privacy-preserving for fog computing usually focused on the Internet of things (IoT [29], [30]. For IoE, it has special cyber-physical security requirements (such as meticulous DR, collusion-resistant and geographical interaction). Thus, current proposals cannot be directly applied in IoE. Similar to [31] and [32], the proposed security schemes for fog computing guaranteed the traditional CIA (confidentiality, integrity, and availability) of data transmitted among IoT entities (including fog and cloud), but it cannot resist some strong outside attacks or convert internal corruptions. For example, public power users may be enticed by false incentives to do what they should not do. And also, a user with top-security level may betray and leak sensitive data to others. No existing solutions can address the above two challenges simultaneously.

Recently, consensus-based optimization was applied to energy management systems in the smart grid due to its credible control signals, but these approaches didn't enforce any restriction on what kind of control signals one should do response. For example, resilient decentralized consensus algorithm presented in [33] reliably estimated global state variables replacing local observability and against false data injection. Incremental welfare consensus algorithm proposed by [34] achieved the global optimum not relying on a central energy management but relying on the localized peer-to-peer communications among smart devices, this proposal gained credible DR strategy under an untrustworthy environment. By perceiving neighbors cost variables, the improved consensus algorithm in [35] drives all connected regions of a power system to approach its own optimal state gradually.

Different from the recent approaches, we exploit decentralized consensus algorithm and a novel cryptographic primitive called access control encryption (ACE) [36] to achieve fog computing-enabled secure demand response (FSDR) scheme for IoE against collusion attacks. Originally, the ACE scheme was designed to ensure that one user with high-security level can not tamper the data transmitted on the Internet. The ACE introduces a sanitizer to enforce the key transform and opportunistic encryption. The sanitizer will maintain a transform key, which is exploited to re-encrypt the data randomly. The features of the FSDR scheme included: 1) it ensures that no matter what regulation policy fog nodes publish and what actions power users take (after being processed by fog node) looks like random execution of a random behavior; 2) The FSDR as a typical fog services improved the energy utilization by consensus-based optimization.

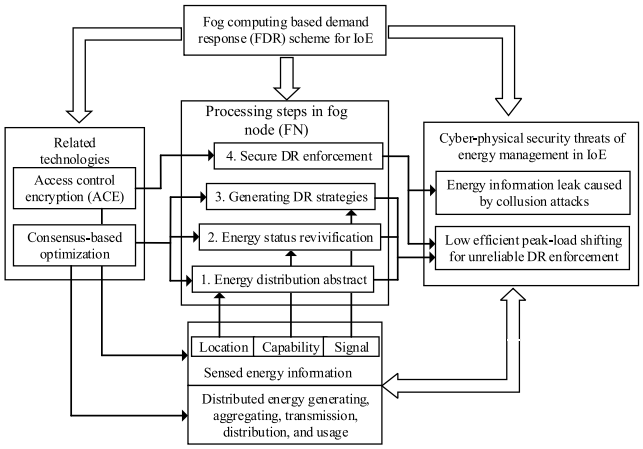


FIGURE 2. The basic architecture of FSDR and its core components.

III. BASIC ARCHITECTURE OF FSDR

IoE plays an important role in future green applications due to real-time energy monitoring and efficient demand response management. meanwhile, fog computing brought great opportunities for IoE to deal with the increasing energy information. To overcome the unique cyber-physical security challenges of energy management in IoE, we proposed fog computing-enabled secure demand response (FSDR) scheme. This scheme facilitated the applicability of fog computing in IoE. The energy management was outsourced to distributed fog nodes. The FSDR achieves high-level security by innovatively integrating consensus-based optimization and access control encryption (ACE) into fog services. The basic architecture of FSDR is shown as illustrated in Fig. 2 and the core components of FSDR were described as follows.

A. GENERALIZED ENTITIES FOR FRDR

Generalized entities for FSDR are described as follows. 1) DR participators: The DR participators act as multiple

roles in fog spot: energy supplier, aggregator, energy user, energy market manager, etc. Each DR participator chooses its role according to current energy status. 2) Fog node (FN): The FN provides a state statistics of local energy resources and broadcasts these energy states to local DR participators. DR participators with corresponding smart devices upload energy information to the FN. In proposed scheme, the FN acts as an actuator to enforce consensus and ACE among DR participators to guarantee IoE's security. (Details on this actuator are introduced in Section IV. 3) Smart devices: Smart devices are responsible for real-time energy monitoring and utility test of DR enforcement. By smart devices (such as smart meters, intelligent electronic devices, and IoT elements), fog node can aggregate a large number of energy states.

B. RANDOMIZED AND ENCRYPTED DATA TUPLE FOR FSDR

All energy information (such as location, capability, and price signal) transmitted between DR participators are encrypted as ciphertext by a specific encryption key, and then the ciphertext and the mentioned encryption key will be sent to the FN. In particular, FN will act as a sanitizer to randomly refresh all of the received ciphertexts by homomorphic operation.

Different from the traditional encryption scheme, the properties of homomorphic operation allow the data administrators to do some simplex statistics (such as addition, subtraction and multiplication) on the ciphertext. Such properties naturally adapt to the demand response (DR) management in IoE, which requires to enforce the secure demand or response fusion. Moreover, in consideration of the privacy-preserving, IoE users do not expect their data that will be processed on the Internet are public so that the data administrators for IoE should have ability to directly handle the encrypted data. In this paper, we focus on the defense of collusion attacks to achieve more secure demand response, the homomorphic operation can provide a satisfactory ciphertext processing functionality.

We exploit the fog nodes to act as the sanitizers of access control encryption (ACE) scheme to execute the ciphertext transforming. Many works has studied the dynamic resources offloading to achieve a smarter fog computing paradigm in which the resources can be configured relying on the context (e.g., data scale, service level) [37], [38]. Moreover, to reduce the processing time on fog nodes, the computing tasks of homomorphic operations can be sliced into several sub-modules and smartly assigned to the idle fog servers. In addition, the fog computing paradigm is implemented with a hierarchical model, time-consuming computing tasks can be uploaded to cloud layer adaptively.

We defined a data tuple as the minimum data unit for FSDR. The format of defined data tuple is denoted as $(\alpha_0, \alpha_1, \alpha_2) = (e_k, E(m), S(e_k + E(m)))$, where e_k is the encryption key of ACE, $E(m)$ is the ciphertext encrypted with e_k, and $S(e_k + E(m))$ is the signature of e_k and $E(m)$.

C. LOCALIZED P2P ENERGY NETWORKING FOR FSDR

As energy in IoE is often aggregated from distributed energy resources and stored at individual accumulators, energy exchanging was achieved in a peer-to-peer (P2P) networking manner [39]. The communication between local DR participators is based on a localized peer-to-peer (P2P) energy networking model. Thus, in such P2P energy networking mode, each DR participator can receive messages and electricity sent by other nodes. This localized P2P energy networking model is the basic communication infrastructure for DR participators to share energy information and electricity. FSDR exploited this P2P energy networking model to achieve consensus-based power grid optimization. Let $\Im_x$ be a set of DR participators joining the group in consensus session x. Let ∂_x be DR strategy set authorized in consensus session x. Let ς_x be a set of security levels of DR participators. All DR strategies in ∂_x should be broadcasted to each DR participator. Each DR participator should select one optimal DR strategy as response securely.

Both energy exchanging and data transmission is optimized by consensus optimization algorithm on fog nodes. The function of fog node in FSDR scheme consists of four processing steps: 1) energy distribution abstract; 2) energy status revivification; 3) generating DR strategies; 4) secure DR enforcement. For each processing step, peers should achieve a collective objective. By consensus between DR participators, the topology discovery, sensed state, received DR strategies of connected energy resources can be trusted unless there exist corrupt peers [40]. In the localized P2P energy networking model, energy usage of peers is verified by all DR participators. As energy information will be published to all DR participators, it is easy for a corrupt DR participator to launch collusion attacks.

IV. PROPOSED FSDR SCHEME AGAINST COLLUSION ATTACKS

In this section, we introduce the designing principles of proposed FSDR scheme against collusion attacks. The collusion attacks are formulated with mathematical models. As mentioned in advance, we use two key technologies 1) consensus-based optimization and 2) access control encryption to securely achieve robust demand response in IoE. Security analysis is also described in this section.

A. MODELING OF COLLUSION ATTACKS IN FSDR

FSDR is designed for the purpose of making robust demand response among the DR participators. In a decentralized architecture, DR participators are unknown to each other. A DR participator makes demand response with another DR partic ipator either on behalf of their reputation value or by another DR participators' recommendations. Malicious DR participators may attack the networks by using the following approaches. For convenience, Table 1 summarizes the main symbols for modelling collusion attacks.

TABLE 1. Symbols and explainations for modelling collusion attacks.

Symbols	Explainations
R_{ij}	The reputation of j with respect to i
t_{ij}	The trust value of i on j
σ_{kj}	The feedback factor after i completes event k
R_j, R_k, R_l	The reputation value of k, j, and l
$\lambda_j, \lambda_k, \lambda_l$	The corresponding coefficients of j, k, l 's influence on user' decision
η_j	User' decision to select j's DR strategy
$\eta_k^{O_i}$	O_i' decision to select k's DR strategy
$t^0_{O_i k}$	The original trust value between O_i and k
ω	The influence of j's cheating
e_ω	The corresponding coefficients of j's influence on O_i's selection
m	The plain text
$E(m)$	The ciphertext
e_k	The encryption key
d_k	The decryption key
r_k	The transform key
$S(e_k + E(m))$	The signature of e_k and $E(m)$

1) UNFAIR COMPETING

IoE enables freedom competitions on prices, power quality, etc. In an open structure, unfair competition is vulnerable to collusion attack. The usual illegal competition methods contain mislead act and defame act. A group of corrupt DR participators can collectively defame some normal peers by giving guidance information. If a large number of power users are misguided to charge during peak time, they will obtain worse power quality, even it may lead power failure.

Reputation can be an algebraic value, which represents the word-of-mouth of the peer's earlier behavior. Reputation value can be calculated by using the following equations:

$$R_{ij} = \sum_{k=1}^{n} (t_{ij} * \sigma_{kj}) \tag{1}$$

$$R_j = \sum_{i=1}^{n} (R_{ij}) \tag{2}$$

Where, R_{ij} denotes the reputation of j with respect to i; t_{ij} denotes the trust value of i on j; σ_{kj} denotes the feedback factor after i completes event k; R_j denotes the reputation value of j in the whole network. Therein, $\sigma_{kj} \in (-1, 1)$.

Each power user may receive the recommendation from multiple other users. Usually, the recommendation from DR participator with a higher reputation value is higher possible to be adopted. We can model user' decision with the equation shown as follows:

$$\eta_j = 1 + \lambda_j R_j - \sum_{k=1}^{j-1} \lambda_k R_k - \sum_{l=j+1}^{n} \lambda_l R_l \tag{3}$$

Where, λ_j, λ_k, and λ_l are the corresponding coefficients of the reputation value' influence on users' decision and are positive. We observe that adopting the recommendation of j directly depends on the reputation values of all DR participator.

Unfair competing means that the corrupt DR participators will illegally actuate λ_j, λ_k, or λ_l. For example, collectively reducing the reputation value of j and rising the reputation value of k or l up, the possibility to adopt recommendation generated by j will decrease. Once one's reputation decreases, the DR participator will switch to the other DR participators to collect available DR strategies.

2) REPUTATION-BASED CHEATING

A DR participator or group of DR participator acts as honest peers and vigorously join some consensus sessions to accumulate reputation. But sometimes corrupt DR participators with higher reputation may cheat with the other DR participators by giving dishonest decisions. For example, if a reputable charging station is corrupt, it may provide bad power quality for users' charging or publish some messages what it should not send into the networks.

The network topology is open to each DR participator. Assuming that DR participator j is attacker and let $O = \{O_1, O_2, \ldots, O_n\}$ denote the victims in the localized P2P energy network. As the existing security and privacy-preserving schemes do not give any restriction on what j with a higher reputation should provide, the victims' decisions under reputation-based cheating circumstance can be formulated as shown in equation (4).

$$\eta_k^{O_i} = t^0_{O_i k} + e^j_{O_i k} \frac{1}{e^{|\omega_0 - \omega|}} \tag{4}$$

Where $\eta_k^{O_i}$ denotes the possibility of O_i to select DR participator k under reputation-based cheating. $t^0_{O_i k}$ denotes the original trust value between O_i and k. ω is the influence of j's cheating. $e^j_{O_i k}$ represents the corresponding coefficients of the influence of j's reputation on O_i's selection. We can observe that reputation-based cheating has a great impact on attacked DR participator's selection. For example, if $\omega < \omega_0$, as the ω increases, $\eta_k^{O_i}$ increases. Otherwise, if $\omega > \omega_0$, $\eta_k^{O_i}$ decreases. Additionally, as $e^j_{O_i k}$ increases, $\eta_k^{O_i}$ increases linearly. In summary, both reputation-based cheating and unfair competing have great threat on the security of decentralized DR management in IoE.

B. COLLUSION-RESISTANT USING CONSENSUS AND ACE

To clearly bring out the designing principles of FSDR against collusion attacks, we first consider a simple network topology with only one fog node. And then, we extended it to generalized scenarios.

1) FSDR SCHEME FOR SINGLE FOG NODE

Assume that there are n providers $P_1, P_2, \ldots, P_n$, n consumers $C_1, C_2, \ldots, C_n$, $n = \{1, 2, \ldots, \}$, and one fog sanitizer (FSan) deployed on the fog node. There is a communication connectivity matrix $M_{n \times n}$, where $M_{ij} \in \{0, 1\}$. Therein, $M_{ij} = 1$ means that C_j is allowed to receive messages sent by P_i, while $M_{ij} = 0$ means that C_j is not allowed to receive messages sent by P_i. We assume that providers

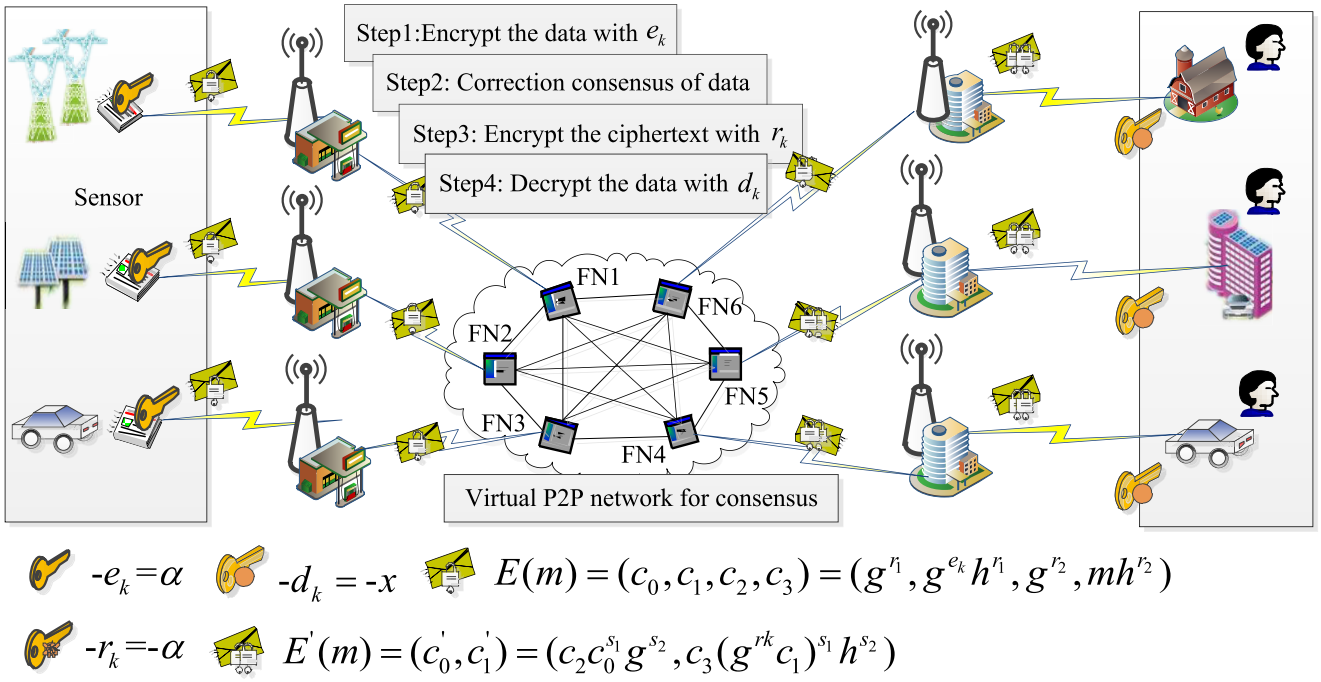


FIGURE 3. The diagrammatic map for data encryption and transmission process of FSDR scheme.

are connected to all consumers with a public Internet. All messages should be sanitized with the transform key r_k and no provider is allowed to send messages to a specific consumer. Meanwhile, each consumer can receive all messages from the providers. Moreover, all messages are transmitted with ciphertext encrypted with random encryption key e_k, and only the illegal consumers will be assigned with decryption key d_k.

Let us denote a set of timestamp for consensus process of DR optimization as $T \triangleq (t_k \mid k \in N)$, where N represents a positive integer. Correspondingly, let us denote a sequence of energy transmission events during t_k as $V \triangleq (DT^{t_k}_{P'_iC'_j} \mid P'_i \in \mathbb{C}, S_j \in \mathbb{Z})$. And also, $\mathbb{M} \triangleq (M^{t_k}_{P'_iS'_j} \mid P'_i \in \mathbb{P}, C'_j \in \mathbb{C})$ is the message sent from P'_i to C'_j, where $\mathbb{P} = \{P_1, P_2, \ldots, P_n\}$ and $\mathbb{C} = \{C_1, C_2, \ldots, C_m\}$. $M^{t_k}_{P'_iC'_j} = null$ means that there is no message that is sent from P'_i to C'_j during the period T_k.

To resist the collusion attacks as mentioned in the equation (3) and (4), we use ACE to randomly encrypt the energy information transmitted between providers and consumers. And also, by using consensus optimization, we minimize the utility functions. The workflow of proposed FSDR scheme is shown as illustrated in Fig. 3.

$$Z_1 = \lambda_j \Delta R_j - \sum_{k=1}^{j-1} \lambda_k \Delta R_k - \sum_{l=j+1}^{n} \lambda_l \Delta R_l \tag{5}$$

$$Z_2 = \Delta t^0_{O_ik}(\omega_0 - \omega) + t^0_{O_ik}\Delta\omega \tag{6}$$

Where, Δ is a mathematical operation that represents the variation of R_j. Usually, Δ is decided by t_{ij} according to the equation (1) and (2).

On the basis of consensus between DR participators, trust value is decided by the security of energy information. Thus, the first thing we do is introducing ACE scheme into FSDR to ensure the CIA (confidentially, integrity, and availability) of energy control signals (such as prices regulating, DR management, and electricity scheduling). This novel encryption primitive achieves a fair energy information sharing, in which the energy control signals sent by attacker looks like randomization. By using this encryption primitive, each consumer is equiprobable to receive energy control signals. Equiprobable DR management prevents the convert collusion attack because attacker can not illegally force up reputation value of some DR participators or maliciously defame one's reputation by spreading rumors to the localized P2P energy networks. In ideal circumstances, this will make objective function of equation (6) be approximate to 0.

To bring out the advantages of ACE's randomization, we describe its workflow and give detail explains as follows.

- Step 1: Initially, fog node enforce a **Setup** algorithm to generate a master key and public parameters for ACE. The input consists of a system security level and the access control structure over the connectivity matrix $M_{n\times n}$. The public parameters for ACE mainly contains message space and ciphertext space.
- Step 2: Secondly, a **key generation** algorithm is executed. The inputs of this algorithm contain the master key, the identities $i, j \in \{1, 2, \ldots, n\}$, and the role of DR participators {Provider, consumer, fog sanitizer}. The outputs of this algorithm include encryption key e_{ki}, transform key r_k, and decryption key d_{kj}.

- Step 3: All keys will be distributed into different types of DR participators according to the access control structure. If the providers obtaining encryption key e_{ki} want to inform consumers to change energy usage states, they should encrypt their energy control signals with e_{ki} and output the corresponding ciphertext.
- Step 4: All ciphertext should be transmitted to fog node and they will be encrypted by **FSan** with transform key r_k. This operation transforms the ciphertext into sanitized ciphertext. Note that the fog node can not learn any information about the original ciphertext except for its arriving time and the **FSan** will send the sanitized ciphertext to all consumers.
- Step 5: After the consumers received the sanitized ciphertext, they will try to decrypt original energy control signals using d_{kj}. Only the correct d_{kj} can decrypt correct message.

The second thing we should do is to minimize the equation (5). In IoE, the DR participators' reputation values frequently change at spatial and temporal dimension. After the consumers decrypt a correct energy control signal, each consumer will compute the η_j according to the equation (3). Because of the competitive nature, we formulate this problem as Nash Equilibrium [41]. All DR participators that can decrypt the energy control signals can join a group for consensus. Let $G = [N, U_j, Z_j(.)]$ denote the non-cooperative game among DR participators with decryption capability. N represents the DR participators with decryption capability in this consensus group, $\{U_j = \eta_j\}$ is the set of user' responses and $Z_j(.)$ is the utility function of DR participator j. For convenience, we use U_{-j} to denote the responses of all DR participator excluding j. Therefore, in the demand response game, each DR participator tries to minimize its own utility by solving the formulated optimization problem for all $j \in N$ as follows.

$$\min_{u_j \in U_j} Z_j(u_j, U_{-j}), \forall j \in N \tag{7}$$

According to the analysis of game-theoretic problem, the optimal strategy set $U_j^\star$ is called Nash Equilibrium, which should make $Z_j(U_j^\star, U_{-j}) < Z_j(U_j, U_{-j})$. In this paper, we follow and simplify the approach of simulated annealing (SA) algorithm [42] to efficiently find the NE point in FSDR scheme, which enables stochastic global optimization. The solving process is shown as illustrated in Table 2.

As a result, it should be characterized that we find a set of DR strategies where all DR participators are satisfied with the utility the obtain.

2) GENERALIZED FSDR TO Γ FOG NODES

We can extend the localized P2P energy network with one fog node to a generalized case with K fog nodes. Let $\Gamma = \{F_1, F_2, \ldots, F_\Gamma\}$ denote a set of localized P2P energy networks, which are connected to fog node τ. The decision

TABLE 2. Solving process for consensus.

Algorithm 1: SA-based consensus in FSDR

1: **Generate** $U = U_0$ and $Z = Z^0{}_j$ as current DR strategy and utility
2: **Initialize** a counter $C = 0$ as the evaluation number
3: **While** $C < C_{max}$ and $Z^C > \{Z_j\}_{max}$
4: **Select** a neighbourly DR strategy U_C randomly
5: **Compute** the utility of U_C
6: **Determine** if the new DR strategy can be accepted according to the Metropolis principle
7: **If** yes, $U = U_C$; $Z = Z_C$; $C = C + 1$; Continue
8: **else**: **return** U_{C-1} and go to Step 1
9: **end**
10: **end**
11: **Publish** the result to all DR participator to verify its legality and validity
12: **If** yes, enforce the received DR strategy;
13: **else**, Go to Step 1
14: **end**

function of each fog node can be defined as equation (8).

$$\eta_{F_i} = 1 + \lambda_{F_i} R_{F_i} - \sum_{\tau=1, \tau \neq i}^{\Gamma-1} \lambda_{F_\tau} R_{F_\tau} \tag{8}$$

In this case, the λ_{F_τ} is the corresponding coefficient of the influence of fog node's reputation value on its decision and are positive. Unfair competing upgrades that the corrupt fog nodes will illegally change λ_{F_τ}. For example, collectively reducing the reputation value of fog node i and rising the reputation value of τ up, the possibility to adopt recommendation generated by i will decrease. Once one fog node's reputation value decreases, the neighbourly fog node will switch to the other fog nodes to collect available DR strategies. Therefore, for DR scheduling between Γ fog nodes, the collusion attack threats still exist. Following the previous section, the minimization problem of each fog node $F_i \in \Gamma$ can be formulated as the following model.

$$Z_1' = \lambda_{F_i} \Delta R_{F_i} - \lambda_{(F_\tau)} \sum_{\tau=1, \tau \neq i}^{\Gamma} \Delta R_{(F_\tau)} \tag{9}$$

The collusion-resistant minimization model against reputation-based cheating between fog nodes can be defined as follows.

$$Z_2' = \Delta t^0_{O_i F_\tau}(\omega_0 - \omega) + t^0_{O_i F_\tau} \Delta\omega \tag{10}$$

It should be noted that the R_{F_i} is the reputation value of fog node F_i. This parameter depends on the resource configuration of the fog node. Usually, one fog node having more resources (like computing, storage, and electricity) will obtain a high reputation value except it is a vicious fog node.

Moreover, in the demand response game, each fog node will try to minimize its own utility by finding the NE point of equation (11).

$$\min_{u_{F_i} \in U_{F_i}} Z_{F_i}(u_{F_i}, U_{(-F_i)}), \quad \forall F_i \in N \tag{11}$$

$U_{(-F_i)}$ denotes the responses of fog nodes excluding F_i.

C. ENERGY UTILIZATION OF FSDR ENFORCEMENT

As mentioned in Section II, the function of fog node in FSDR mainly consists of four processing steps. In terms of the energy distribution abstract and energy status revivification, the FSDR is more suitable to aggregate distributed energy resources (DERs) for enabling location-based services, in which energy demands can be satisfied by localized energy suppliers.

Low latency nature of fog computing can be exploited to reduce the peak time and improve the energy utilization. For generalized FSDR to Γ fog nodes, the fog node classifies energy requests into different types according to the requests' locations. In this case, we consider three kinds of location types: 1) Home area (HA), 2) Local area (LA), and 3) Remote area (RA). Let L_r denote the location of responders, $L_r \in \{HA, LA, RA\}$.

TABLE 3. Workflow of responder placement algorithm.

Algorithm 2: Responder Placement Algorithm for FSDR enforcement

```
for responserr ∈ placeList do
  if r has already placed on fog node f ∈ F then
    Merge r with a far entity
    f = fog node holding the merged entity
    While E_r^req ≥ E_f^aval do
      for demander r' ∈ placeList do
        if r' is not in the higher level than r
        Stop the r' and put into the r' to the queue
        E_f^aval = E_f^aval + E_r'^sup
        end
      end
      f = parent(f)
    end
    Place r on fog node f
  end
  else if E_r^req ≤ E_f^aval
    Place r on fog node f
  end
end
```

Table 3 show the responder placement algorithm for FSDR enforcement. Therein, *placeList* is a list that store the identity of each pending placed responder. E_r^{req} represents for the requested energy of responder r, while $E_{r'}^{sup}$ represents for the supplied energy of responder r'. In addition, E_f^{aval} is the energy capacity of fog node (charging station).

FSDR scheme makes the unoccupied energy in localized domain join DR management of power grid systems, which improved the energy utilization shows as illustrated in next section.

V. PERFORMANCE EVALUATION

The performance evaluation are divided into there different aspects. Firstly, we discuss the quantization of collusion attacks and compare how the victims' decisions varies under the reputation-based cheating circumstance. Secondly, the collusion-resistant utility of proposed FSDR scheme is evaluated. Thirdly, the energy utilization under collusion-resistant is analyzed.

A. QUANTIZATION OF COLLUSION ATTACKS

We consider the communication between DR participators in localized P2P energy network and the interaction between fog nodes. However, we did not evaluate the impact of the dynamics of resources partitioning of fog nodes for the following reasons. Firstly, the collusion attack defense utility of proposed scheme did not closely depend on the efficiency of resources offloading and partitioning in IoE. The resources offloading and partitioning of fog computing can not change the encryption or decryption results. Secondly, although the dynamics of resources offloading and partitioning in fog computing has not been well addressed, we deduce this problem can be resolved by the hot topic of service-oriented computing (SOC) in future [43], [44]. For example, we can design a attribute-based computation allocation algorithm, which can selectively encrypt the passing data on the fog nodes according to the data attributes (such as data popularity, security level and QoS parameters).

In this case, the number of DR participator is set as $n = 100$. The corresponding coefficients of the reputation value's influence on user's decision is configured as $\lambda_j = [0.2\ 0.4\ 0.6\ 0.8\ 1.0]$, while λ_k and λ_l are generated by random function, which can produce random number belong to $(0-1)$. Additionally, the reputation value of DR participator j is set to a group of uniform scores from 0.1 to 1.0.

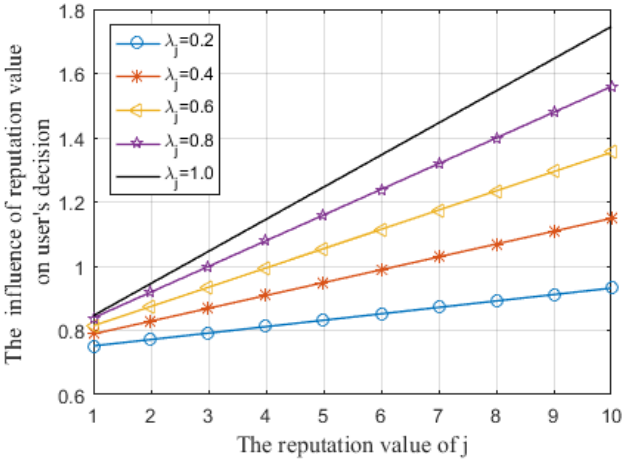


FIGURE 4. The user's response varies as the reputation value increases for different coefficients.

1) UNFAIRNESS

Fig. 4 shows how the user's response varies as the reputation value increases for different coefficients. It can be observed that the reputation value of one DR participator has great impact on user's decision. Collusion attackers often try to do something to impact the DR participator's reputation value to illegally disturb user's decision.

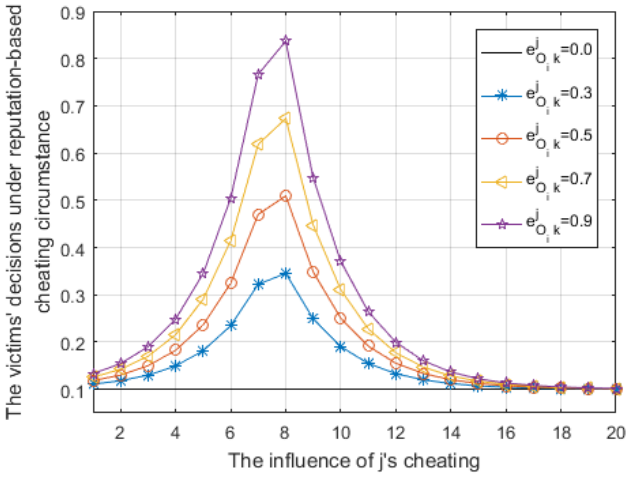


FIGURE 5. The victims' decisions varies under the reputation-based cheating circumstance.

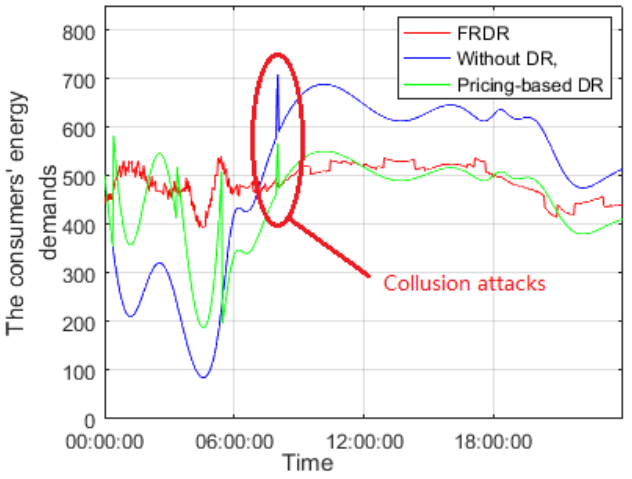


FIGURE 6. The demand curves of different DR schemes under collusion attack circumstance.

2) AUTHENTICITY

Fig. 5 shows how the victim's decision varies under the reputation-based cheating circumstance. In this scenario, the original trust value between O_i and DR participator k is set to 0.1. The corresponding coefficients $e^j_{O_i k}$ of the influence of j's reputation on O_i's selection is generated as [00.30.50.70.9]. The influence of j's cheating is configured as $\omega_0 = 3.8$. If $\omega < \omega_0$, as the ω increases, $\eta_k^{O_i}$ increases. Otherwise, when $\omega > \omega_0$, $\eta_k^{O_i}$ decreases. This result means that the utility of cheating is limited in IoE because widely spreading in the localized P2P energy network will arouse someone's suspicion on the authenticity of attackers' messages sent to the network.

B. COLLUSION-RESISTANT UTILITY OF FSDR

This simulation experiment consists of three steps. Firstly, we collect the energy usage data from some reports on Internet and exploit statistic analysis methods to analyze the daily energy demands in a distinct. Secondly, we generate a outlier on the original energy demand curve to simulate the collusion attack. Thirdly, we implement the pricing-based DR algorithm and the FSDR under this collusion attack circumstance, respectively.

In FSDR scheme, the number of gateway is set to 2 and the number of fog nodes on per gateway is set to 5. Each fog node will maintain [7], [20] power consumers. The energy of each fog node is configured as 30, while the gateway energy is set to 50. The distributed energy sources consists of wind and solar energy. The DR management of FSDR is implemented by responder placement algorithm.

To bring out the benefits of proposed FSDR scheme on resisting collusion attacks, we depict the demand curves of different DR schemes under collusion attack circumstance as illustrated in Fig. 6. It can be observed that FSDR scheme provides better performance on peak-load shifting and the outlier caused by collusion attacks is eliminated.

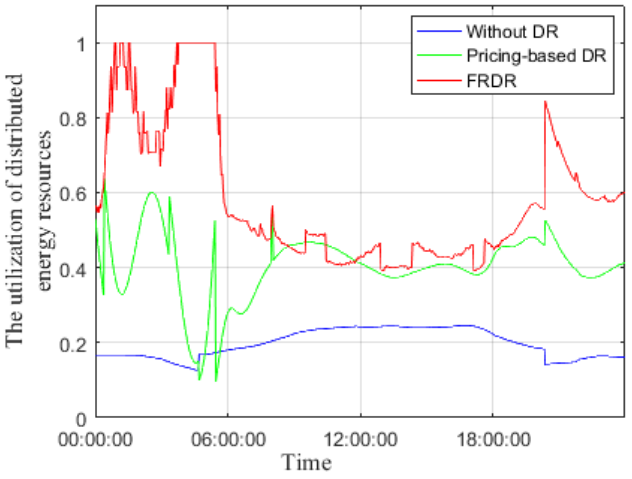


FIGURE 7. The utilization of distributed energy resources at different DR schemes.

C. ENERGY UTILIZATION UNDER COLLUSION RESISTANT

The FSDR enables bidirectional energy exchanging between distributed energy resources and power grid. Moreover, as the fog node provides a temporary storage place for distributed energy, the responder placement algorithm stimulate power consumers to use distributed energy. Different from the pricing-based DR scheme that uniformly use distributed energy resources, FSDR scheme smartly resorts to real-time energy monitoring to schedule the distributed energy resources. Only when the distributed energy is inadequate to cover power consumers' demands, FSDR will request energy from power grid. This scheme significantly improves the utilization of distributed energy resources as shown in Fig. 7.

VI. CONCLUSION AND FUTURE WORK

In this paper, we investigated the security challenges of integrating fog computing into Internet of Energy. To resist the collusion attacks and optimize energy utilization,

we presented a fog computing-enabled robust demand response (FSDR) scheme to achieve smarter, secure, and stabilized demand-side management using consensus and ACE. The main work in this paper can be summarized as follows. Firstly, the mathematical model of collusion attacks and proposed FSDR scheme were described in detail. The accessibility of electricity collected from distributed sources were allocated by fog node, which enables more meticulous demand response. Illegal energy occupation caused by collusion attacks was estimated. Secondly, the data encryption and transmission process of FSDR scheme were introduced by using a diagrammatic map. Thirdly, we exploited the simulated annealing algorithm to find the Nash equilibrium point, which provided stochastic global optimization. And also, a responder placement algorithm was proposed to efficiently and distributedly schedule the consumers' demands. Finally, we verified the feasibility of proposed FSDR scheme by simulations. The influence of collusion attack on power users' behaviors was quantified, the utility of FSDR scheme on collision resistant was demonstrated, and the improvement on energy utilization of distributed energy resources under collusion resistant was achieved. While the FSDR has presented many strengths on both security and efficiency, a lightweight design should be provided in future work to enhance its scalability in more IoE scenarios.

REFERENCES

[1] M. Rana, "Architecture of the Internet of energy network: An application to smart grid communications," *IEEE Access*, vol. 5, pp. 4704–4710, 2017.

[2] K. Wang *et al.*, "A survey on energy Internet: Architecture, approach, and emerging technologies," *IEEE Syst. J.*, to be published, doi: 10.1109/JSYST.2016.2639820.

[3] C.-C. Lin, D.-J. Deng, W.-Y. Liu, and L. Chen, "Peak load shifting in the Internet of energy with energy trading among end-users," *IEEE Access*, vol. 5, pp. 1967–1976, 2017.

[4] M. H. Y. Moghaddam, A. Leon-Garcia, and M. Moghaddassian, "On the performance of distributed and cloud-based demand response in smart grid," *IEEE Trans. Smart Grid*, to be published, doi: 10.1109/TSG.2017.2688486.

[5] N. Saputro and K. Akkaya, "Investigation of smart meter data reporting strategies for optimized performance in smart grid AMI networks," *IEEE Internet Things J.*, vol. 4, no. 4, pp. 894–904, Aug. 2017.

[6] R. Pourramezan, Y. Seyedi, H. Karimi, G. Zhu, and M. Mont-Briant, "Design of an advanced phasor data concentrator for monitoring of distributed energy resources in smart microgrids," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3027–3036, Dec. 2017.

[7] E, U. Ogbodo, D. Dorrell, and A. M. Abu-Mahfouz, "Cognitive radio based sensor network in smart grid: Architectures, applications and communication technologies," *IEEE Access*, vol. 5, pp. 19084–19098, 2017.

[8] L. Li, K. Ota, and M. Dong, "When weather matters: IoT-based electrical load forecasting for smart grid," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 46–51, Oct. 2017.

[9] Y.-W. Chen and J. M. Chang, "Fair demand response with electric vehicles for the cloud based energy management service," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 458–468, Jan. 2018.

[10] M. Tao, K. Ota, and M. Dong, "Foud: Integrating fog and cloud for 5G-enabled V2G networks," *IEEE Netw.*, vol. 31, no. 2, pp. 8–13, Mar./Apr. 2017.

[11] K. Wang, C. Xu, Y. Zhang, G. Song, and A. Zomaya, "Robust big data analytics for electricity price forecasting in the smart grid," *IEEE Trans. Smart Grid*, to be published, doi: 10.1109/TBDATA.2017.2723563.

[12] F. Y. Okay and S. Ozdemir, "A fog computing based smart grid model," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, May 2016, pp. 1–6.

[13] H. Jiang, K. Wang, Y. Wang, M. Gao, and Y. Zhang, "Energy big data: A survey," *IEEE Access*, vol. 4, pp. 3844–3861, 2016.

[14] M. Chiang, S. Ha, C.-L. I, F. Risso, and T. Zhang, "Clarifying fog computing and networking: 10 questions and answers," *IEEE Commun. Mag.*, vol. 55, no. 4, pp. 18–20, Apr. 2017.

[15] K. Wang, M. Du, S. Maharjan, and Y. Sun, "Strategic honeypot game model for distributed denial of service attacks in the smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2474–2482, Sep. 2017.

[16] Z. Liu, C. Zhang, M. Dong, B. Gu, Y. Ji, and Y. Tanaka, "Markov-decision-process-assisted consumer scheduling in a networked smart grid," *IEEE Access*, vol. 5, pp. 2448–2458, 2017.

[17] N. Saxena, A. Roy, and H. Kim, "Efficient 5G small cell planning with eMBMS for optimal demand response in smart grids," *IEEE Trans. Ind. Informat.*, vol. 13, no. 3, pp. 1471–1481, Jul. 2017.

[18] M. A. A. Faruque and K. Vatanparvar, "Energy management-as-a-service over fog computing platform," *IEEE Internet Things J.*, vol. 3, no. 2, pp. 161–169, Apr. 2016.

[19] K. Wang, H. Li, Y. Feng, and G. Tian, "Big data analytics for system stability evaluation strategy in the energy Internet," *IEEE Trans. Ind. Informat.*, vol. 13, no. 4, pp. 1969–1978, Aug. 2017.

[20] P. G. V. Naranjo, M. Shojafary, L. Vaca-Cardenasz, C. Canaliy, R. Lancellottiy, and E. Baccarelli, "Big data over SmartGrid—A fog computing perspective," in *Proc. SOFTCOM Workshop*, 2016, pp. 1–6.

[21] S. Kar, G. Hug, J. Mohammadi, and J. M. F. Moura, "Distributed state estimation and energy management in smart grids: A consensus + innovations approach," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 6, pp. 1022–1038, Dec. 2014.

[22] K. Wang *et al.*, "Distributed energy management for vehicle-to-grid networks," *IEEE Netw.*, vol. 31, no. 2, pp. 22–28, Mar./Apr. 2017.

[23] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[24] A. Molina-García, F. Bouffard, and D. S. Kirschen, "Decentralized demand-side contribution to primary frequency control," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 411–419, Feb. 2011.

[25] G. Benysek, J. Bojarski, R. Smolenski, M. Jarnut, and S. Werminski, "Application of stochastic decentralized active demand response (DADR) system for load frequency control," *IEEE Trans. Smart Grid*, to be published, doi: 10.1109/TSG.2016.2574891.

[26] J. Lian, J. Hansen, L. D. Marinovici, and K. Kalsi, "Hierarchical decentralized control strategy for demand-side primary frequency response," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2016, pp. 1–5.

[27] K. Sakurama and M. Miura, "Communication-based decentralized demand response for smart microgrids," *IEEE Trans. Ind. Electron.*, vol. 64, no. 6, pp. 5192–5202, Jun. 2017.

[28] K. Wang, X. Hu, H. Li, P. Li, D. Zeng, and S. Guo, "A survey on energy Internet communications for sustainability," *IEEE Trans. Sustain. Comput.*, vol. 2, no. 3, pp. 231–254, Jul./Sep. 2017.

[29] L. Zhang, L. Wei, D. Huang, K. Zhang, M. Dong, and K. Ota, "MEDAPs: Secure multi-entities delegated authentication protocols for mobile cloud computing," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3777–3789, 2016.

[30] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the Internet of Things: Security and privacy issues," *IEEE Internet Comput.*, vol. 21, no. 2, pp. 34–42, Mar./Apr. 2017.

[31] M. Dong, K. Ota, and A. Liu, "RMER: Reliable and energy-efficient data collection for large-scale wireless sensor networks," *IEEE Internet Things J.*, vol. 3, no. 4, pp. 511–519, Aug. 2016.

[32] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

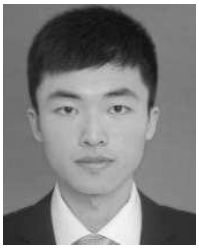
[33] R. H. Etemad and F. Lahouti, "Resilient decentralized consensus-based state estimation for smart grid in presence of false data," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Mar. 2016, pp. 3466–3470.

[34] N. Rahbari-Asr, U. Ojha, Z. Zhang, and M.-Y. Chow, "Incremental welfare consensus algorithm for cooperative distributed generation/demand response in smart grid," *IEEE Trans. Smart Grid*, vol. 5, no. 6, pp. 2836–2845, Nov. 2014.

[35] Z. Yang, J. Xiang, and Y. Li, "Distributed consensus based supply–demand balance algorithm for economic dispatch problem in a smart grid with switching graph," *IEEE Trans. Ind. Electron.*, vol. 64, no. 2, pp. 1600–1610, Feb. 2017.

[36] I. Damgård, H. Haagh, and C. Orlandi, "Access control encryption: Enforcing information flow with cryptography," in *Theory of Cryptography*, vol. 9986. New York, NY, USA: Springer-Verlag, 2016, pp. 547–576.

[37] S. Mubeen, P. Nikolaidis, A. Didic, H. Pei-Breivold, K. Sandström, and M. Behnam, "Delay mitigation in offloaded cloud controllers in industrial IoT," *IEEE Access*, vol. 5, pp. 4418–4430, 2017.
[38] R. M. Shukla and A. Munir, "An efficient computation offloading architecture for the Internet of Things (IoT) devices," in *Proc. IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2017, pp. 728–731.
[39] S. Salinas, M. Li, and P. Li, "Privacy-preserving energy theft detection in smart grids: A P2P computing approach," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 257–267, Sep. 2013.
[40] N. K. Saini, V. K. Sihag, and R. C. Yadav, "A reactive approach for detection of collusion attacks in P2P trust and reputation systems," in *Proc. IEEE Int. Adv. Comput. Conf. (IACC)*, Feb. 2014, pp. 312–317.
[41] K. Wang, Z. Ouyang, R. Krishnan, L. Shu, and L. He, "A game theory-based energy management system using price elasticity for smart grids," *IEEE Trans. Ind. Informat.*, vol. 11, no. 6, pp. 1607–1616, Dec. 2015.
[42] H. A. Oliveira, Jr., and A. Petraglia, "Solving generalized Nash equilibrium problems through stochastic global optimization," *Appl. Soft Comput.*, vol. 39, pp. 21–35, Feb. 2016.
[43] T. Nishio, R. Shinkuma, T. Takahashi, and N. B. Mandayam, "Service-oriented heterogeneous resource sharing for optimizing service latency in mobile cloud," in *Proc. IEEE Int. Conf. Cloud Comput. Technol. Sci.*, Jul. 2013, pp. 19–26.
[44] A. Bajpai, B. Choudhury, and S. Choudhury, "An adaptive and elastic cloud based framework for service oriented computing in Internet of Things," in *Proc. Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2017, pp. 460–463.



GAOLEI LI (S'15) received the B.S. degree in electronic information engineering from Sichuan University, Chengdu, China, in 2015. He is currently pursuing the Ph.D. degree with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China. He participates in many national projects, such as the National Natural Science Foundation of China, the National "973" Planning of the Ministry of Science and Technology, China, and so on. His research interests are focusing on the Internet of Energy, fog computing, cyberspace security, and so on. He is a TPC Member of the International Conference on Internet of Things in 2017.

JUN WU (S'08–M'12) received the Ph.D. degree in information and telecommunication from Waseda University, Japan. He was a Post-Doctoral Researcher with the Research Institute for Secure Systems, National Institute of Advanced Industrial Science and Technology, Japan, from 2011 to 2012. He was a Researcher with the Global Information and Telecommunication Institute, Waseda University, from 2011 to 2013. He is currently an Associate Professor with the Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, School of Cyber Security, Shanghai Jiao Tong University, China, and the Vice Director of the National Engineering Laboratory for Information Content Analysis Technology. He has hosted and participated in several research projects for the National Natural Science Foundation of China, the National 863 Plan and 973 Plan, the Japan Society of the Promotion of Science Projects, and so on. His research interests include the advanced computing and communications techniques of smart grids, Internet of Things, industrial security, and so on. He has been a Guest Editor of the IEEE Sensors Journal and a TPC Member of over ten international conferences, including WINCON, ICC, GLOBECOM, and so on. He is an Associate Editor of the IEEE Access.

JIANHUA LI received the B.S., M.S., and Ph.D. degrees from Shanghai Jiao Tong University, Shanghai, China, in 1986, 1991, and 1998, respectively. He was the Chief Expert in the information security committee experts of National High Technology Research and Development Program of China (863 Program) of China. He is currently a Professor/Ph.D. Supervisor and the Dean of the Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, School of Information Security Engineering, Shanghai Jiao Tong University. He is also a Committee Expert of the Information Technique Standardization Committee, Shanghai. He was the Leader of over 30 state/province projects of China, and he has published over 200 papers. He received the second prize of the National Technology Progress Award of China in 2005, the first prize of the National Technology Progress Award of Shanghai in 2003 and 2004, and two first prizes of the National Technology Progress Awards of Shanghai in 2004. His research interests include cyber-space security, data science, next-generation networks, and so on.

ZHITAO GUAN (M'13) received the B.Eng. and Ph.D. degrees in computer application from the Beijing Institute of Technology, China, in 2002 and 2008, respectively. He is currently an Associate Professor with the School of Control and Computer Engineering, North China Electric Power University, China. His current research focuses on smart grid security, wireless security, and cloud security. He has authored over 20 peer-reviewed journal and conference papers in these areas.

LONGHUA GUO (S'15) received the B.S. degree in electronic information engineering from Tianjin University, Tianjin, China, in 2013. He is currently pursuing the Ph.D. degree with Shanghai Jiao Tong University, Shanghai, China. He was a Visiting Student with Temple University from 2016 to 2017. He participates in many national projects, such as the National Natural Science Foundation of China, the National "973" Planning of the Ministry of Science and Technology, China, and so on. His research interests include sensor network security, social network analysis, and so on.