Contract-Based Incentive Mechanisms for Honeypot Defense in Advanced Metering Infrastructure

Wen Tian, *Graduate Student Member, IEEE*, Miao Du, Xiaopeng Ji, *Member, IEEE*, Guangjie Liu, Yuewei Dai, and Zhu Han, *Fellow, IEEE*

***Abstract*—Honeypot defense deployment is considered as a promising technology to protect the industrial Internet of Things (IIoT), especially Advanced Metering Infrastructure (AMI), threatened by cyber-attacks. AMI defensive effectiveness depends on the honeypot deployment of the small-scale electricity suppliers (SESs) in sharing defense data. However, since the honeypot system is an additional defensive tool deployed by SESs, traditional power retailers (TPRs) cannot confirm in advance that the defense data shared by SES is valid. Therefore, it is necessary to design an incentive mechanism based on the information asymmetry to encourage SES to share defense data honestly. In this paper, we propose a honeypot deployment contract-theoretic model (HDCM) to improve the defensive effectiveness of AMI, where SES will honestly share defense data and the defense cost of TPR will be reduced. We first divide the SESs' contribution into finite types, and model the defense data sharing contract between the TPR and SESs. Then, the contract feasibility of HDCM is derived in necessary and sufficient conditions. At last, we analyze the optimal contract offered by TPR in the continuous case of SESs. Numerical simulations show that the HDCM can incentivize SESs to deploy honeypot and honestly share defense data, and make defensive effectiveness of AMI close to the information symmetry case.**

***Index Terms*—Honeypot, contract theory, information asymmetry, industrial Internet of Things, advanced metering infrastructure.**

Manuscript received August 2, 2020; revised January 19, 2021 and March 9, 2021; accepted April 2, 2021. Date of publication April 7, 2021; date of current version August 23, 2021. This work was supported in part by NSF under Grant EARS-1839818, Grant CNS1717454, Grant CNS-1731424, and Grant CNS-1702850; in part by the National Natural Science Foundation of China under Grant U1836104, Grant 61602247, Grant 61702235, and Grant U1636117; in part by the Natural Science Foundation of Jiangsu Province under Grant BK20160840; in part by Fundamental Research Funds for the Central Universities under Grant 30918012204; and in part by the Talent Start-Up Fund of Nanjing University of Information Science and Technology under Grant 1521082101007. Paper no. TSG-01187-2020. *(Corresponding author: Xiaopeng Ji.)*

Wen Tian is with the School of Automation, Nanjing University of Science and Technology, Nanjing 210094, China (e-mail: csusttianwen@163.com).

Miao Du is with the Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mail: dumiao0118@163.com).

Xiaopeng Ji, Guangjie Liu, and Yuewei Dai are with the School of Electronic and Information Engineering, Nanjing University of Information Science and Technology, Nanjing 210044, China (e-mail: jixiaopeng_nj@163.com; gjieliu@gmail.com; dywjust@163.com).

Zhu Han is with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004 USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul 446-701, South Korea (e-mail: zhan2@uh.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2021.3071513.

Digital Object Identifier 10.1109/TSG.2021.3071513

I. Introduction

THE PROLIFERATION of highly capable electrical equipment in the industrial Internet of Things (IIoT), such as smart homes [1], has led to a shortage of traditional electricity supply. With the development of smart grid [2], households, as small-scale electricity suppliers (SESs), set up small wind turbines on their rooftops to sell excess electricity to reduce the pressure of traditional power retailers (TPRs) [3]. Hence, advanced metering infrastructure (AMI) [4], an important component of smart grid, is expanded through SESs. Moreover, a tremendous amount of consumption data is rapidly attracting the focus of cyber attackers [5], [6]. Consequently, a novel SES defense paradigm is needed to face the serious growth challenge in the demand for the AMI defense.

To deal with cyber-attacks, honeypot has recently been proposed as a complementary defense tool to enhance AMI defense [7], [8]. AMI defense benefits from the fact that SESs can establish independent small-scale defense systems to obtain corresponding rewards from sharing defense data instead of TPR paying a higher cost from the security retailers for the defense data. One common form of the honeypot is the high-interaction one in which the honeypot simulates the normal meter operation to attract the attacker to hack and analyze attackers' behavior [9]. If SESs deploy honeypot and share defense data reasonably, the AMI's defensive effectiveness can be improved while the defense cost of TPR can be reduced. In addition, the TPRs' defensive pressure can be reduced, while their defensive coverage can be extended.

Local TPR will compensate accordingly to encourage SESs to share defense data. For example, if SESs share the defense data collected and captured by the honeypot with TPR, the TPR will give electricity fee discounts or updates vulnerabilities [10] for the SES in return. By doing so, instead of bearing the defensive pressure alone, the TPR would make the AMI defense system more effectively. To achieve this goal, incentivizing SESs to deploy honeypot system and cooperate with TPR is the design challenge. If most SESs refuse to deploy honeypot, the TPR will still need to bear the defensive pressure alone and cost more to obtain defense data from security retailers. Hence, the defensive effectiveness of AMI is not improved. The willingness of SESs to deploy honeypot and share defense data is significant to improve the defensive effectiveness of AMI.

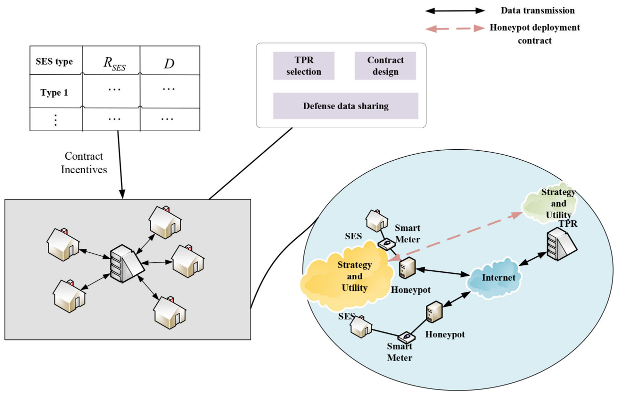


Fig. 1. Incentive mechanism for deploying honeypot and sharing VDD in AMI.

Indeed, an effective incentive mechanism [11] is necessary to introduce and encourage SESs to deploy honeypot and share defense data. To encourage SESs participation, the TPR will offer rewards to SES for sharing its resources (honeypot, electricity, defense data, time, etc.) especially for honeypot, because SES itself cannot capture defense data. Obviously, the rewards of SESs should be positively related to its contribution: SESs share more defense data must receive a higher reward than SESs share less. However, each SES will claim to have more defense data and try to get more rewards, which will result in rewards not being offered correctly. The core of the reward offer design is information asymmetry [12]—the TPR does not know the actual defense data owned by SESs in advance. Hence, proposing an incentive mechanism based on information asymmetry is our main goal in AMI as shown in Fig. 1.

In this respect, a mechanism, where SESs will be rewarded in accordance with their valid defense data, needs to be designed. Contract theory [13]–[15], a powerful framework, can model the incentive mechanisms based on information asymmetry. In the defense data sharing process, we study the interaction between TPRs (defense data receivers) and SESs (sharers whose defense data are not known to the TPRs) through contract theory. Specifically, rewards are provided to SESs, which will transmit defense data via deploying honeypot in the light of the contracts. We list the advantages of using contract theory in AMI as follows: 1) integrating defensive effectiveness in which the SES can deploy honeypot and share defense data with TPR; and 2) devising optimal incentive mechanisms to reduce TPR's defense data cost based on the information asymmetry.

Motivated by this, we propose a honeypot deployment contract-theoretic model (HDCM) where the TPR encourages the SESs to deploy the honeypot and share the defense data. For HDCM, the contract feasibility is proved through necessary and sufficient conditions. Moreover, contract feasibility indicates that SESs' reward must compensate for their deploying honeypot cost and defense data sharing cost. Furthermore, the contract is proved as a self-revealing contract. To implement the HDCM, a new algorithm, which encourages the TPR and SESs to negotiate and improve the defensive effectiveness of AMI, is proposed. Numerical simulations show that the HDCM helps SESs to obtain nonnegative utilities and reduce the defense data cost of TPR.

The main contribution of this work is characterized by the following:

- We are the first to study deploying honeypot against cyber-attacks in SES through self-revealing contract theory. The proposed HDCM can protect AMI, and further protect the security of the smart grid.
- We introduce incentive mechanics into HDCM to encourage SESs to voluntarily deploy the honeypot system, which is an additional deployment, based on the information asymmetry and honestly share the valid defense data to TPR.
- We study and analyze the feasibility and optimization process of HDCM in discrete and continuous cases.
- We conduct experiments on an AMI testbed to evaluate the performance of our proposals. The results show that the proposed HDCM can help SESs to obtain nonnegative utility, reduce the defense data cost of TPR, and further improve the defensive effectiveness of AMI.

The rest of this paper is organized as follows. A detailed literature survey of security issues in IIoT, honeypot against cyber-attacks, and contract game theory application are discussed in Section II. The system model and AMI welfare are studied in Section III. The contract feasibility conditions and optimization process are presented in Section IV. The numerical simulations are shown in Section V. Finally, conclusions are drawn in Section VI.

II. Related Work

In this section, we first introduce the security issue of AMI, then describe the honeypot, which is an active defense tool, against cyber attacks in AMI, and finally introduce contract game theory application which is a typical incentive mechanisms based on the information asymmetry.

A. *Security Issues in AMI*

As an important part of IIoT, the security issues have been widely studied in recent years. For example, Du and Wang [9] studied the defense strategy against cyber-attacks in IIoT. In [9], the authors assumed that cyber attackers have strong vulnerability identification capabilities. Li *et al.* [16] exploit the consortium blockchain technology to reduce the transaction limitation in IIoT. Nevertheless, little research is about the individual components' security issues with respect to AMI environments. There are several detection techniques related to AMI. Ye *et al.* [17] proposed a security protocol in AMI, which protects the privacy information and delivers control messages safely and timely. Fasial *et al.* [18] analyze the possibility of using data stream mining for enhancing the security of AMI through an intrusion detection system (IDS). Yan *et al.* [19] present a security protocol for AMI in smart grid. In [19], the authors consider various security vulnerabilities of deploying AMI.

B. Honeypot Against Cyber-Attacks in AMI

Honeypot is one of the active security tools [20], which is used as vulnerabilities trap to deceive cyber attackers, and has long been used to improve defensive performance in various systems [7], [9], [21]. Tian *et al.* [21] used the honeypot to defense the APT attack in bus nodes of the smart grid. He divided the honeypot system into two modes: high- and low-interaction honeypot. Wang *et al.* [7] proposed a honeypot architecture with different mixed distribution to capture attack traffic for the AMI system. Hence, the honeypot is introduced into the AMI defense. However, Wang *et al.* did not consider that deploying honeypot sytem can reduce TPR's defensive pressure and enhance the AMI's defensive effectiveness. Du and Wang [9] used honeypot to capture DDoS attacks in AMI. Their work is to use the incomplete information static game to study non-cooperative problem through honeypot deployment. To the best of our knowledge, the TPR and SESs can cooperate with each other, for example, it will be the universe to set up small wind turbines on the individual companies to sell excess electricity [3]. Hence, SESs will also become the target of cyber-attacks. It should be noted that voluntarily deploying the honeypot system into SESs can effectively improve defense capabilities and has been ignored in previous studies. In addition, how to maximize the defensive effectiveness of the discrete honeypot system through the Internet is a problem.

C. Contract Game Theory Application

Although there is a lot of defensive management and cost allocation in the security of the AMI, however, few existing works have studied that incentivize SES to deploy individual defense equipment in AMI. Contract game theory, as a typical incentive mechanic under asymmetric information, can solve the problem of security cooperation between TPR and SESs and the defensive effectiveness improvement. Furthermore, honeypot deployment through contract theory, an effective method for maximizing the capabilities of discrete components, has not been studied in the AMI.

For the contract theory, there are some works focused on mobile networks and direct electricity trading. For example, Li *et al.* [22] used contract theory to improve the revenue of the cloud server's economy in cloud computing. Zhang *et al.* [3] proposed a novel contract-based incentive scheme to efficiently encourage electricity consumers and SESs to participate in direct energy trading. Zhang *et al.* [23] used contract theory to handle Device-to-Device communication based on information asymmetry. In [23], mobile users are encouraged to transmit data with each other to reduce the communication bandwidth pressure of the base station. Zhang [14] used contract theory to study mobile crowdsourcing, where the base station provides incentives to encourage mobile users to process location data. However, mobile devices such as mobile phones are universally owned by mobile users and the base station can process location information by itself. For the AMI, they cannot collect defense data by themselves, so they need to deploy honeypot system or purchase defense data from security retailers. Therefore, implementing the existing mobile users' contract-theoretic model into AMI's honeypot deployment directly is very difficult. Since honeypot system is not universally deployed by SESs, deploying honeypot system requires additional deployment costs. Hence, encouraging SES to deploy the honeypot system and honestly share defense data is a huge challenge.

In summary, while defense management in AMI has been studied a lot, there is no literature study on the issue of using self-revealing contract theory to provide incentives for SESs to participate in honeypot deployment. Our proposal introduces an incentive mechanism in HDCM to encourage SESs to deploy the honeypot system and share the defense data to TPR. Moreover, we study and analyze the HDCM in the discrete case and continuous case, respectively.

III. System Model

As shown in Fig. 1, there is a TPR that is going to acquire defense data from the SESs in AMI. In this paper, the scenario we considered is one TPR and N SESs. At first, we describe the models for the sharer (i.e., SES) and receiver (i.e., TPR) in detail, and show why their interaction is a framework of contract. Traditionally, TPR obtains defense data through security retailers. In IIoT, the TPR can receive defense data from the SES, which has deployed the honeypot, in the cyber layer. In order to obtain multiple sources of defense data, the TPR will offer a contract that can encourage the SESs to deploy honeypot to capture cyber-attacks and package the defense data and forward it to TPR through the network.

Although it is feasible for SES to share defense data in AMI, intuitively, information asymmetry exists between the TPR and the SES. The SES knows its valid defense data (VDD) while the TPR does not. In this paper, VDD represents the unknown attack interaction log, which has been employed by the current TPR defense database, collected by the honeypot system. The database contains the existing defense methods of TPR and typical defense logs. VDD will be used to update the defense database by adding a new defense method and further enhance the security performance of AMI. If the attack can be defended through the existing defense database, the defense data collected by honeypot system is not VDD, vice versa. Therefore, to solve the problem of information asymmetry, a VDD-reward bundle contract $(R_{SES}(D), D)$ will be designed, where R_{SES} is the reward of SES, D is the VDD, which specifically refers to the log generated by honeypot, and the unit of D is MByte. To encourage SES to provide more VDD, the R_{SES} is positively related to D.

A. Sharer Modeling

We define the SES type as the VDD contribution of each SES in the AMI such as the log volume and the detection rate of honeypot system, etc. Since the reward is positively related to VDD, high-type SES is more willing to provide VDD, while the TPR prefers a high-type SES. Hence, when there are N SES, the SESs's VDD are classified into N types in ascending order. We use the T_i to indicate the SES's type and meet $T_1 < \cdots < T_i < \cdots < T_N$, i.e., higher T is eager to deploy the honeypot share VDD. Besides, (R_{SES_i}, D_i) represents the contract of type-i SES's. Although the VDD of SES is private information, the type-i SES's probability q_i is historical prior knowledge, with $\sum_{i=1}^{N} q_i = 1$.

Since the VDD of SESs is different, the TPR will provide the different contract due to SES's type T. For SESs, they can decide whether to accept the provided contract or not. If the SES refuses to accept the contract, we think that the SES accept a special contract $(R_{SES}(0), 0)$, where $R_{SES}(0) = 0$. Considering the feathers of contract, the type-i SES's utility function is expressed below:

$$U_{SES}(i) = T_i v\big(R_{SES_i}\big) - Y(D_i) - C_h, \tag{1}$$

where $v(R_{SES_i})$ is the reward function and meet $v'(R_{SES}) > 0$ and $v''(R_{SES}) < 0$. $T_i v(R_{SES_i})$ represents the reward that the TPR offer to the SES of type i, $Y(D_i)$ is the SES's cost function on sharing VDD, which is related to the hardware performance or interactive ability of honeypot, and meet $Y'(D_i) > 0$, such as time and energy consumption, etc. C_h is the honeypot deployment cost that SES needs to spend additionally. The SES does not know whether it will be attacked, therefore, each SES tends to deploy a standardized honeypot system with the same cost. In this case, the SES will select the optimal contract to maximizes its utility. The optimization process of contract is described in Section IV-B.

B. Receiver Modeling

Traditionally, when the TPR needs defense data, it procures defense data in bulk from security retailers. As we all know, security retailers usually increase prices due to their monopoly. Therefore, if the price offered by SESs is lower than that in the security retailers, the TPR will turn to these SESs. Normally, the price proposed by SES can be replaced with electricity fee discounts or vulnerabilities update, etc. Meanwhile, due to the limited VDD shared by a single SES, TPR will obtain VDD from multiple SES.

If the TPR obtain the VDD from the type-i SES, the related utility function is defined as:

$$U_{TPR}(i) = E(D_i) - \kappa R_{SES_i}, \tag{2}$$

where κ is the coefficient of TPR's defense cost, D_i is the VDD, $E(D_i)$ is the economic value function of VDD and R_{SES_i} is TPR's defense cost, i.e., the reward of SES. Here, the reward to the SES is firewall upgrade and vulnerabilities update, etc. For honeypot deployment to be beneficial for the TPR, it is clear from (2) that we must have $E(D_i)-\kappa R_{SES_i} > 0$. Otherwise, the TPR will not receive VDD from SES. Hence, TPR's utility function can be expressed as:

$$U_{TPR} = \sum_{i=1}^{N} q_i\big(E(D_i) - \kappa R_{SES_i}\big). \tag{3}$$

After discussing the utilities of the TPR and SESs, we then analyze the utility of the AMI.

C. AMI Welfare

Since the AMI is composed of SES and TPR, the AMI welfare [24] is the summation of the TPR and SESs' utilities. We assume that the SESs' types follow a uniform distribution, we have

$$\Pi = \sum_{i=1}^{N} \big[T_i v\big(R_{SES_i}\big) + E(D_i) - Y(D_i) - \kappa R_{SES_i} - C_h\big]. \tag{4}$$

In addition, we summarize the detailed notations in Table I.

TABLE I
LIST OF SYMBOLS IN THE HDCM

Symbols	Description
N	Numbers of SESs in the power grid
R_{SES_i}	The reward of SES i
D	The valid defense data
T_i	The type of SES i
q_i	The probability that an SES belongs to type-i
C_h	The SES's cost on deploying honeypot
κ	The TPR's defense cost coefficient
U_{TPR}	The expected utility of the TPR
U_{TPR}	The expected utility of the SES

IV. Optimization Solution

In order to improve defensive effectiveness in AMI, we first will derive the HDCM feasibility constraints in Section IV-A. We then optimize the HDCM contract, and study it under continuous case in Section IV-B. At last, we propose the algorithm to deal with practical implementation in Section IV-C.

A. HDCM Feasibility Analysis

To encourage the SESs to deploy honeypot and share defense data, the proposed HDCM should meet the following constraints.

$$U_{SES}(i) = T_i v\big(R_{SES_i}\big) - Y(D_i) - C_h \geq 0. \tag{5}$$

Hence, the SES should ensure that $U_{SES}(i)$ is nonnegative though selecting the contract, i.e., individual rationality (IR) [3].

To increase the enthusiasm of SES's deploying honeypot, the honeypot deployment cost must also be compensated by rewards except for VDD cost. If $U_{SES}(i) < 0$, the SES will not deploy the honeypot and further share VDD, i.e., the SES will select the contract $(R_{SES}(0), 0)$. In order to obtain more rewards, SESs will falsely report their VDD. If type-i SES accepts the (R_{SES_j}, D_j) for type-j SES, the type-i SES's utility is expressed by

$$U_{SES}{}^{j}(i) = T_i v\big(R_{SES_j}\big) - Y(D_i) - C_h. \tag{6}$$

In order to prevent false reporting, a rational unique choice contract is designed in HDCM for the SES and the TPR. To put it from another angle, the type-i SES will obtain the utility under (R_{SES_i}, D_i) not less than others, i.e.,

$$T_i v\big(R_{SES_i}\big) - Y(D_i) - C_h \geq T_i v\big(R_{SES_j}\big) - Y(D_i) - C_h. \tag{7}$$

This we called incentive compatible (IC). In addition to IR and IC restrictions, we will verify the positive relationship between type and utility.

Lemma 1: For (R_{SES}, D), $R_{SES_i} > R_{SES_j}$ if and only if $T_i > T_j$.

Proof: We add the two inequalities (8) and (9) together to get (10)

$$T_i v\big(R_{SES_i}\big) - Y(D_i) - C_h \geq T_i v\big(R_{SES_j}\big) - Y(D_j) - C_h, \quad (8)$$
$$T_j v\big(R_{SES_j}\big) - Y(D_j) - C_h \geq T_j v\big(R_{SES_i}\big) - Y(D_i) - C_h. \quad (9)$$
$$v\big(R_{SES_i}\big)\big(T_i - T_j\big) \geq v\big(R_{SES_j}\big)\big(T_i - T_j\big). \quad (10)$$

When $T_i > T_j$, we have $v(R_{SES_i}) > v(R_{SES_j})$. Then, owing to the definition of $v(R_{SES})$, $v(R_{SES_i}) > v(R_{SES_j})$ with $i \neq j$. Furthermore, when $v(R_{SES})$ holds, the $T_i > T_j$ always holds.

After proving the sufficiency of Lemma 1, we prove the necessity as follows: if $R_{SES_i} > R_{SES_j}$, then $T_i > T_j$. Similar to the previous proof process, we can obtain the expression (11) through IC constraints

$$T_i\big(v\big(R_{SES_i}\big) - v\big(R_{SES_j}\big)\big) \geq T_j\big(v\big(R_{SES_i}\big) - v\big(R_{SES_j}\big)\big). \quad (11)$$

Therefore, when $R_{SES_i} > R_{SES_j}$, $v(R_{SES_i}) > v(R_{SES_j})$ holds. Hence, we have $T_i > T_j$. In a nutshell, we have proved that $R_{SES_i} > R_{SES_j}$ if and only if $T_i > T_j$. ■

Obviously, high-type SES will get more utilities than low-type SES after compensating for the cost of deploying honeypot system and sharing VDD. Therefore, considering $T_1 < \cdots < T_i < \cdots < T_N$, we further have $R_{SES_1} < \cdots < R_{SES_i} < \cdots < R_{SES_N}$. The monotonicity of utilities indicate that higher types of SES will be more willing to participate in deploying honeypot and sharing defense data. Considering that sharing VDD requires power and time, therefore, D also satisfies the following monotonicity, i.e., $0 < D_1 < \cdots < D_i < \cdots < D_N$, which is the incentive-compatibility contracts [3]. It should be emphasized here that the honeypot deployment cost is the same for all SESs. We extend the Lemma 1 to get Lemma 2.

Lemma 2: For (R_{SES}, D), each SES's utility meet the following condition

$$0 < U_{SES}(1) < \cdots < U_{SES}(i) < \cdots < U_{SES}(N). \quad (12)$$

Proof: According to the monotonicity of R_{SES} and D, if the SES want to obtain more reward, it must provide more VDD to TPR, i.e., $R_{SES_i} > R_{SES_j}$ and $D_i > D_j$ are imposed together. If $T_i > T_j$, then

$$\begin{aligned} U_{SES}(i) &= T_i v\big(R_{SES_i}\big) - Y(D_i) - C_h \\ &> T_j v\big(R_{SES_j}\big) - Y(D_j) - C_h = U_{SES}(j). \end{aligned} \quad (13)$$

Therefore, when $T_1 < \cdots < T_i < \cdots < T_N$, we have $0 < U_{SES}(1) < \cdots < U_{SES}(i) < \cdots < U_{SES}(N)$. ■

Hence, we can draw the following conclusions:

- If the high-type SES chooses the low-type SES's contract, even if the high-type SES can share more VDD, it will still obtain the reward of the low-type SES. Therefore, high-type SES does not maximize its utility.
- If the low-type SES chooses the high-type SES's contract, since the low-type SES cannot share more VDD, it will purchase VDD from other places, such as security retailers, to prevent defaults. However, this behavior will increase the VDD cost. Therefore, the low-type SES does not maximize its utility.

B. The Optimization of HDCM

In discrete type, the type of SESs is classified into N. However, the SESs' types can be infinite in practice. Therefore, we study the continuous type which has the probability density function (PDF) $f(T)$ (with cumulative distribution function (CDF) $f(T)$ on the interval $[\underline{T}, \overline{T}]$. The contract that the SES obtained from the TPR can be written as $(R_{SES}(T), D(T))$. When there is no VDD shared between the TPR and the SES, the contract is represented by $R_{SES}(T) = 0$ and $D(T) = 0$. The core of HDCM is the optimization problem of TPR, therefore, TPR's optimization problem can be written by:

$$\begin{aligned} \max \ & {}_{\{R_{SES}(T), D(T)\}} \int_{\underline{T}}^{\overline{T}} [E(D(T)) - \kappa R_{SES}(T)] f(T) dT, \\ s.t. \ & (a) T v(R_{SES}(T)) - Y(D(T)) - C_h \geq 0, \\ & (b) T v(R_{SES}(T)) - Y(D(T)) \geq T v\Big(R_{SES}\Big(\hat{T}\Big)\Big) - Y(D(T)). \end{aligned} \quad (14)$$

Obviously, this is not a convex optimization problem, so we need to solve this problem through the following steps [3].

Step 1 (IR Constraints Reduction): Since the expression (14)(b) holds, we can get

$$T v(R_{SES}(T)) - Y\big(D\big(\underline{T}\big)\big) \geq \underline{T} v\big(R_{SES}\big(\underline{T}\big)\big) - Y\big(D\big(\underline{T}\big)\big). \quad (15)$$

Then, if the expression (14)(a) of $\underline{T}$ satisfied, all T under the IR constraints will automatically hold.

Step 2 (IC Constraints Reduction): We use the following Lemma 3 to express the monotonicity and local incentive compatibility and reduce the IC constraints.

Lemma 3: The IC constraints can be expressed by:

$$\frac{dR_{SES}(T)}{dT} \geq 0, \ \frac{d^2 R_{SES}(T)}{dT^2} < 0. \quad (16)$$
$$T v'(R_{SES}(T)) \frac{dR_{SES}(T)}{dT} = Y'(D(T)) D'(T), T \in \big[\underline{T}, \overline{T}\big]. \quad (17)$$

Proof: According to monotonicity of R_{SES} and T, (16) is easy to obtain at first. Then, we prove the (17) through self contradiction. Suppose both the (16) and (17) are satisfied, and the (7) is not satisfied. Hence, there must be a $\hat{T}$ that does not satisfy the (7) and we express it below

$$0 \leq T v(R_{SES}(T)) - Y(D(T)) < T v\Big(R_{SES}\Big(\hat{T}\Big)\Big) - Y\Big(D\Big(\hat{T}\Big)\Big). \quad (18)$$

Meanwhile, we integrate expression (18) and have

$$\int_T^{\hat{T}} \left[T v'(R_{SES}(x)) \frac{dR_{SES}(x)}{dx} - Y'(D(x)) D'(x)\right] dx > 0. \quad (19)$$

However, according to expression (19), we have

$$T v'(R_{SES}(T)) \frac{dR_{SES}(T)}{dT} - Y'(D(x)) D'(x) = 0. \quad (20)$$

If $T < x < \hat{T}$, we have $T \frac{dv(R_{SES}(x))}{dx} \leq x \frac{dv(R_{SES}(x))}{dx}$ and further obtain

$$\int_T^{\hat{T}} \left[T v'(R_{SES}(x)) \frac{dR_{SES}(x)}{dx} - Y'(D(x)) D'(x)\right] dx < 0. \quad (21)$$

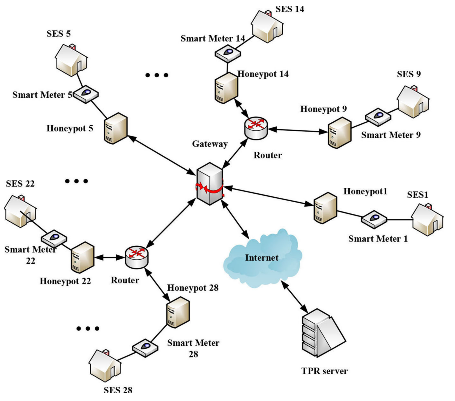


Fig. 2. AMI testbed.

Hence, a self contradiction happens. Similarly, if $T > \hat{T}$, another contradiction happens. In a nutshell, the SES's incentive-compatibility constraints in HDCM are guaranteed. ■

Step 3 (Optimization): In order to optimize problem, the (14) can rewritten as (22) according to (16) and (17).

$$\begin{aligned} \max_{\{R_{SES}(T), D(T)\}} & \int_{\underline{T}}^{\overline{T}} [E(D(T)) - \kappa R_{SES}(T)] f(T) dT, \\ s.t. \quad & (a) T_1 v(R_{SES}(T_1)) - Y(D(T_1)) - C_h = 0, \\ & (b) T_i v(R_{SES}(T_i)) - Y(D(T_i)) = T_i v(R_{SES}(T_{i-1})) \\ & \quad - Y(D(T_{i-1})). \end{aligned} \tag{22}$$

The relaxed problem without monotonic constraints is solved at first, and the standard process of Lagrange multipliers is considered based on the [3]. Furthermore, we check whether the solution satisfies the monotonic constraints or not [13], [25]. The purpose of optimization is to improve AMI welfare, so the defense cost of TPR needs to be reduced as much as possible.

C. Practical Implementation

In order to implement the proposed HDCM in the AMI system, we have the initial information such as the honeypot deployment cost C_h, the cost of VDD $Y(D)$, the number of SES types N, and the SES's probability distribution. Hence, the TPR will offer the optimal contract set (R_{SES}, D). Once the TPR receives the VDD from SESs, the TPR will perform the following operations. At first, TPR will analyze whether "VDD," such as the normal operation data of SES, claimed by SES is true. If the "VDD" is true, TPR will provide the related contract to SES. By evaluating the contract, SES will feedback on whether they are willing to share VDD. After receiving the acceptance response from SES, the contract is officially effective. If no SESs accept the contract, TPR has to purchase VDD directly from the security retailers at a high price. After the contract process is successfully completed many times, TPR will be able to propose the optimal contract, that is to say, the utility of SES is zero under the information symmetry. We summarized the single contract process in Algorithm 1.

TABLE II
SIMULATION SETTINGS

Parameter	Value
Network scale	300m*300m
N	30
λ	0.6
β	5
s	1
κ	0.05
Distribution of q	$q_i = 1/N$
Gateway to Router	0.6 Gbps
Router to Gateway	100 Mbps
Smart meter to Router	0.64 Mbps
Router to Smart meter	0.4 Mbps
Demand length	1,000 bytes
Demand per period	6 s
Answer length	1,000 bytes
Answer per period	12 s
Response time	5 ms
Compared mechanism	NIA and LC incentive mechanism

V. SIMULATION RESULTS AND ANALYSIS

In this section, we first construct an AMI testbed and then evaluate the feasibility and optimization of HDCM, and finally verify the defensive effectiveness of the HDCM.

A. AMI Testbed

As shown in Fig. 2, we construct an AMI testbed with 30 SESs, and each SES is voluntarily embedded with a honeypot. In the testbed, the VDD of each SES is transmitted directly to the TPR through the Internet, the network scale is 300m*300m. The demand length of VDD is 1,000 bytes and the demand per period is 6 seconds. The answer length is 1,000 bytes and the answer per period is 12 seconds. The transmission rate from gateway to router is 0.6 Gbps while the transmission rate from router to gateway is 100 Mbps. In addition, the transmission rate from router to smart meter is 0.4 Mbps while the transmission rate from smart meter to router is 0.64 Mbps. The detailed values are shown in Table II.

B. The Feasibility and Optimization of HDCM

We compare our HDCM based on the information asymmetry with other two incentive mechanisms, the contract under no information asymmetry (NIA) and the linear pricing (LC), are introduced. For the NIA, the types of SESs are public information and this contract is the upper bound we can achieve. For LC, the type of SES is consistent with the assumption in HDCM as private information, however, the reward provided by TPR is positively linearly related to the VDD provided by SES. Specifically, the TPR will only specify a unit price for VDD sharing, and the SESs will request the amount of reward corresponding to a certain amount of VDD, to maximize their own utilities [23]. For simplicity, we consider the SES types in a uniform distribution, i.e., $q_i = 1/N$, the cost function is $Y(D_i) = D_i^{\lambda} + \beta$ and the economic value function is $E(D_i) = s * D_i$.

As shown in Fig. 3, with the increase of honeypot deployment cost, the utility of SES changes from positive to negative.

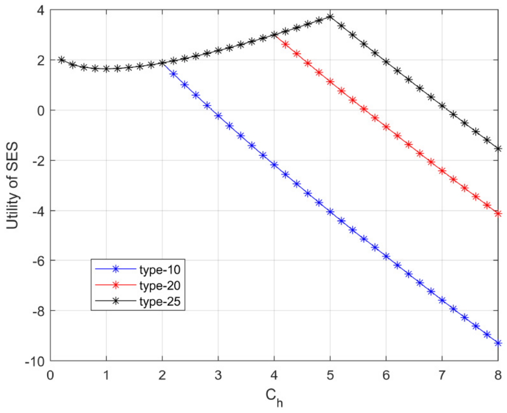


Fig. 3. The feasibility of honeypot deployment.

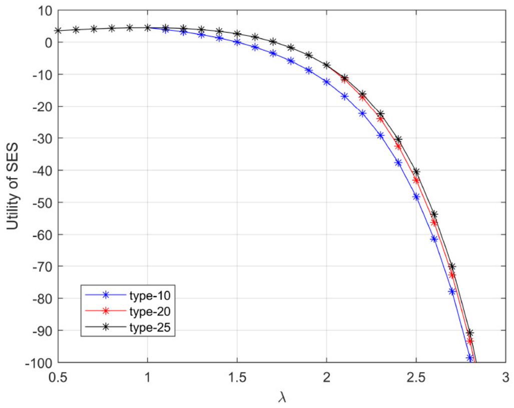


Fig. 4. The feasibility of the contract.

Specifically, if $C_h \leq 2.8$, the utility of SES of type 10 is positive and the SES will voluntarily deploy the honeypot and accept the contract. On the contrary, if $C_h > 2.8$, the SES of type 10 will not deploy the honeypot and reject the contract. Similarly, the SES of type 20 and the SES of type 25 will voluntarily deploy the honeypot and accept the contract when $C_h \leq 4.2$ and $C_h \leq 6$, respectively. On the contrary, the SES of type 20 and the SES of type 25 will not deploy the honeypot and reject the contract when $C_h > 4.2$ and $C_h > 6$, respectively.

As shown in Fig. 4, with the increase of sharing VDD cost parameter λ, the utility of SES changes from positive to negative. Specifically, if $\lambda < 1.5$, the utility of SES of type 10 is positive and the SES will accept the contract. On the contrary, if $\lambda \geq 1.5$, the SES of type 10 will reject the contract. Analogously, the SES of type 20 and the SES of type 25 will accept the contract when $\lambda < 1.7$ and reject the contract when $\lambda \geq 1.7$.

As shown in Figs. 5(a) and (b), the shared VDD and the SESs' rewards are compared based on three mechanisms. Obviously, in Fig. 5(a), the defense contribution increases with the SES type increases. For these three mechanisms, shared VDD under NIA and LC is a linear function of type, while shared VDD under HDCM is a concave function of type. Obviously, the NIA contract obtains the highest defense contribution from the SES, followed by the HDCM. Analogously, as shown in Fig. 5(b), our assumption is proved that reward is positively related to the SES type. As shown in Fig. 5(c), the optimal contract of HDCM is verified. The type-10, 20, and 25 SESs select all the contracts offered by TPR and achieve the corresponding utilities. Obviously, the SES will actively tell the TPR about its VDD honestly since the utilities of dishonesty is lower than the utilities of honesty. Meanwhile, the utilities follow the inequality $U_{10} \leq U_{20} \leq U_{25}$, which corroborates the Lemma 2. Furthermore, the optimal contract is verified in Fig. 5(c). Specifically, we find that if the high-type SES selects the high-type contract, its utility is the same as that the low-type SES selects the low-type contract. In this case, the reward provided by TPR is the lowest, i.e., the defense cost of TPR is the lowest.

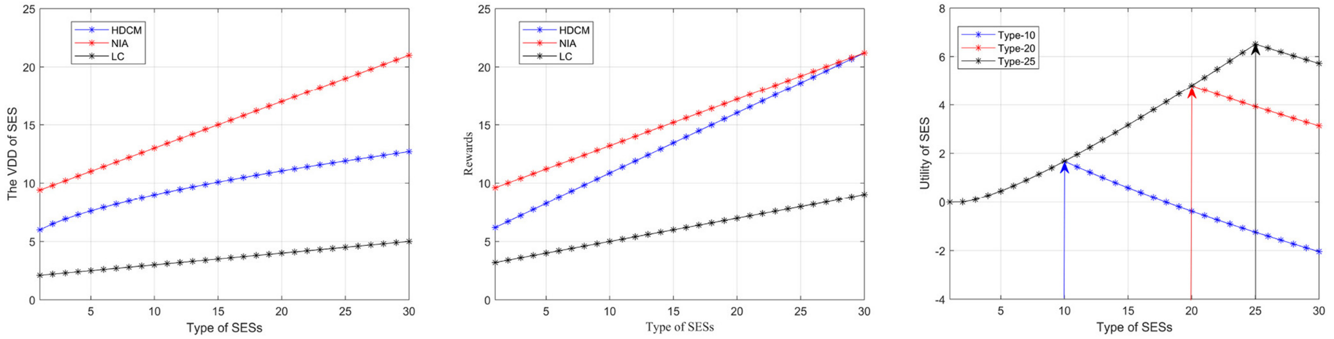
Algorithm 1: Optimal Contract Implementation in AMI

```
Input: $N, C_h, q, T, Y(D), \kappa$
Ouput: the Optimal Contract: $(R_{SES}, D)$
1. Provide Contract
while TPR receives a description of defense data captured from the SES do
    Analyze the types of cyber-attacks mentioned and whether other SESs have been shared before
if the cyber-attacks are of concern to TPR then
    TPR provides contract $(R_{SES}, D)$
    Accept the contract or not
else
    TPR will not provide contract
end if
2. Execute the Contract
while SESs agrees to sign contracts with TPR do
    shares defense data to TPR
if defense data is valid and successfully shared then
    TPR offers a reward
else
    No reward will be offered
end if
3. Obtain the Optimal Contract
if The utility of TPR meet the (22) then
    Output the optimal contract
else
    Reduce the defense cost and repeat 1 and 2
end if
```

C. The Defensive Effectiveness of HDCM

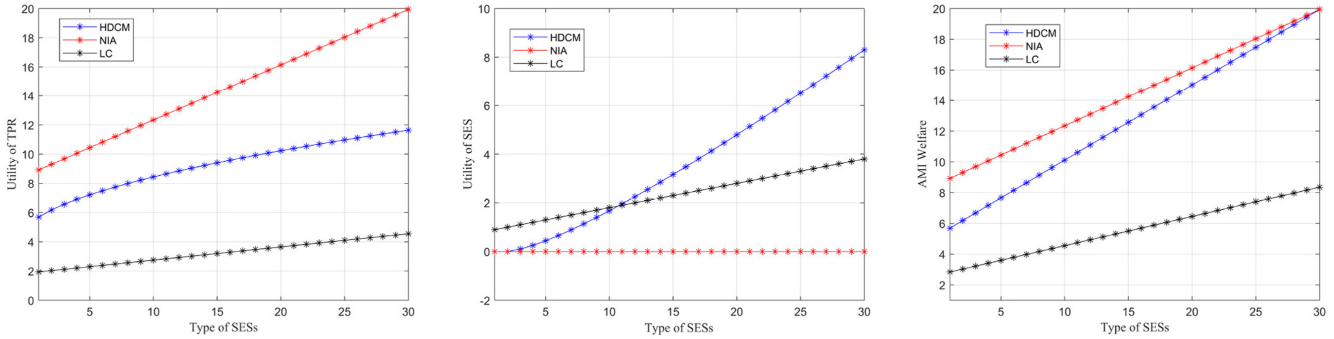
To evaluate the defensive effectiveness of HDCM in AMI, we study the impact of type and number on the TPR's utilities, SESs' utilities, and AMI welfare.

As shown in Fig. 6, higher type will bring larger utility to the TPR, SESs, and the AMI welfare, which is consistent with the monotonicity of HDCM. As shown in Fig. 6(a), the TPR achieves the highest utility under NIA because the TPR can confirm the VDD shared by SES. Nonetheless, our proposed TPR solution with HDCM has a higher utility than the LC incentive mechanism. Moreover, we note that although



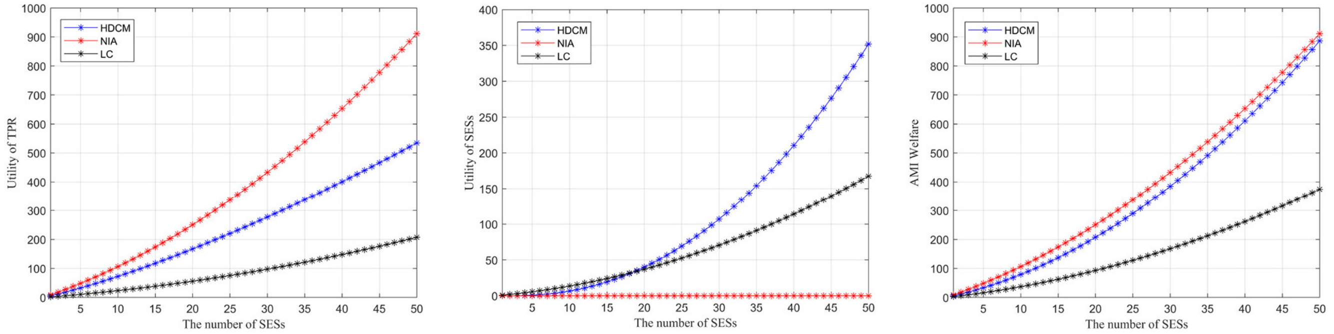
(a) The VDD of SESs (b) The SESs' rewards (c) The optimization contract of HDCM

Fig. 5. The feasibility and optimization of HDCM.



(a) TPR's utilities (b) SESs' utilities (c) AMI Welfare

Fig. 6. The impact of type on the utilites of SESs, TPR and AMI welfare.



(a) TPR's utilities (b) SESs' utilities (c) AMI Welfare

Fig. 7. The impact of number on the utilites of SESs, TPR and AMI welfare.

the solution based on the HDCM can prevent SES from concealing its type, its specific defense data is still unknown by TPR. Hence, with the increase of SES types, the TPR's utility gap between the HDCM and the NIA has increased. As shown in Fig. 6(b), the SES's utility remains zero under NIA because TPR will maximize its utility and decrease the defense cost as much as possible. However, as the types of SES increase, TPR provides contract rewards become more complicated. Therefore, SES is more likely to get high rewards in HDCM. Overall, the SES can achieve a higher utility under the LC incentive mechanism when the type of SES is low. For some higher type SESs, they can achieve a higher utility from the HDCM than the LC through their VDD. In Fig. 6(c), we see that the highest type of SES has the same AMI welfare under NIA and HDCM. This result indicates that the highest type of SES's VDD can be seen as public information, which is consistent with the conclusion we reached in Fig. 5(b).

In Fig. 7, we study the impact of the number of SES types on the utilities of TPR, SESs and AMI welfare. Obviously, more SES types will obtain more utilities of the TPR and SES, and the AMI welfare. In addition, the TPR has the highest utility under NIA and the TPR achieves the second-highest utility through the HDCM since the TPR can minimize the

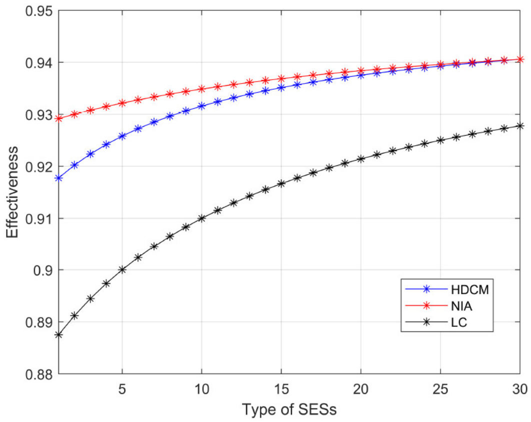


Fig. 8. Effectiveness of different types of SES.

offered reward under the NIA. In Fig. 7(b), the SES's utility remains zero under NIA because TPR will maximize its utility and decrease the defense cost as much as possible. Overall, the SES can achieve a higher utility under the LC incentive mechanism when the type of SES is low. For some higher type SESs, they can achieve a higher utility from the HDCM than the LC. In Fig. 7(c), the AMI welfare gap between the NIA and HDCM is not large, which shows that our HDCM can effectively improve AMI welfare.

In Fig. 8, we find that the higher SES type improves the AMI's defenive effectiveness compared with low SES type. Furthermore, when the type of SES is higher, the defensive effectiveness based on the HDCM is closer to the defensive effectiveness under NIA. This is consistent with the conclusion the highest type of SES can be seen as the public information even in information asymmetry.

VI. Conclusion

In this paper, we have proposed a honeypot deployment contract-theoretic model (HDCM) to encourage SESs to deploy honeypot and share the valid defense data (VDD) to TPR, which improves the effectiveness of AMI's defense. In the case of information asymmetry, TPS cannot obtain the authenticity of SES's VDD, and the incentive mechanism based on contract theory can make SES honestly reveal its VDD. In addition, the SESs will obtain the reward to compensate for the cost of deploying honeypot system and sharing VDD. Moreover, we have studied the feasibility and optimization process of HDCM. The numerical simulations have shown that the HDCM can encourage SES to deploy honeypot system and share VDD with TPR. Meanwhile, the SES will honestly choose a contract related to its type. Furthermore, the defensive performance of HDCM is close to the NIA ideal performance and better than the LC performance based on the information asymmetry.

References

[1] W. Li, T. Logenthiran, V.-T. Phan, and W. L. Woo, “A novel smart energy theft system (SETS) for IoT-based smart home,” *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5531–5539, Jun. 2019.

[2] W. Saad, Z. Han, H. V. Poor, and T. Basar, “Game-theoretic methods for the smart grid: An overview of microgrid systems, demand-side management, and smart grid communications,” *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 86–105, Sep. 2012.

[3] B. Zhang, C. Jiang, J.-L. Yu, and Z. Han, “A contract game for direct energy trading in smart grid,” *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2873–2884, Jul. 2018.

[4] M. Mustapa, M. Y. Niamat, A. P. D. Nath, and M. Alam, “Hardware-oriented authentication for advanced metering infrastructure,” *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1261–1270, Mar. 2018.

[5] W. Tian *et al.*, “Prospect theoretic study of honeypot defense against advanced persistent threats in power grid,” *IEEE Access*, vol. 8, pp. 64075–64085, 2020.

[6] W. Chen, D. Ding, H. Dong, and G. Wei, “Distributed resilient filtering for power systems subject to denial-of-service attacks,” *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1688–1697, Aug. 2019.

[7] 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.

[8] Q. D. La, T. Q. S. Quek, J. Lee, S. Jin, and H. Zhu, “Deceptive attack and defense game in honeypot-enabled networks for the Internet of Things,” *IEEE Internet Things J.*, vol. 3, no. 6, pp. 1025–1035, Dec. 2016.

[9] M. Du and K. Wang, “An SDN-enabled pseudo-honeypot strategy for distributed denial of service attacks in industrial Internet of Things,” *IEEE Trans. Ind. Informat.*, vol. 16, no. 1, pp. 648–657, Jan. 2019.

[10] S. Liu, M. Dibaei, Y. Tai, C. Chen, J. Zhang, and Y. Xiang, “Cyber vulnerability intelligence for Internet of Things binary,” *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2154–2163, Mar. 2020.

[11] H. Gao *et al.*, “A survey of incentive mechanisms for participatory sensing,” *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 918–943, 2nd Quart., 2015.

[12] R. Zhang and Q. Zhu, “FlipIn: A game-theoretic cyber insurance framework for incentive-compatible cyber risk management of Internet of Things,” *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2026–2041, 2020.

[13] P. Bolton and M. Dewatripont, *Contract Theory*, Cambridge, MA, USA: MIT Press, 2004.

[14] Y. Zhang, “Contract theory framework for wireless networking,” Ph.D. dissertation, Dept. Elect. Comput. Eng., Univ. Houston, Houston, TX, USA, 2016.

[15] K. Hamidouche, W. Saad, M. Debbah, M. T. Thai, and Z. Han, “Contract-based incentive mechanism for LTE over unlicensed channels,” *IEEE Trans. Inf. Forensics Security*, vol. 67, pp. 6257–6440, 2019.

[16] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, “Consortium blockchain for secure energy trading in industrial Internet of Things,” *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.

[17] F. Ye, Y. Qian, and R. Q. Hu, “A security protocol for advanced metering infrastructure in smart grid,” in *Proc. IEEE GLOBECOM*. Austin, TX, USA, Feb. 2014, pp. 649–654.

[18] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, “Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study,” *IEEE Syst. J.*, vol. 9, no. 1, pp. 31–44, Mar. 2015.

[19] Y. Yan, R. Q. Hu, S. K. Das, H. Sharif, and Y. Qian, “An efficient security protocol for advanced metering infrastructure in smart grid,” *IEEE Netw.*, vol. 27, no. 4, pp. 64–71, Jul./Aug. 2013.

[20] M. Ammar, M. R. M. Rizk, A. Abdel-Hamid, and A. K. Aboul-Seoud, “A framework for security enhancement in SDN-based datacenters,” in *Proc. 8th IFIP Int. Conf. New Technol. Mobility Security (NTMS)*, Larnaca, Cyprus, Nov. 2016, pp. 1–4.

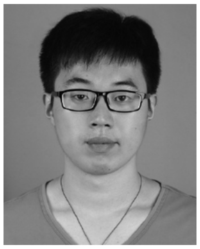
[21] W. Tian *et al.*, “Honeypot game-theoretical model for defending against APT attacks with limited resources in cyber-physical systems,” *ETRI J.*, vol. 41, no. 5, pp. 585–598, 2019.

[22] J. Li, S. Chu, F. Shu, J. Wu, and D. N. K. Jayakody, “Contract-based small-cell caching for data disseminations in ultra-dense cellular networks,” *IEEE Trans. Mobile Comput.*, vol. 18, no. 5, pp. 1042–1053, May 2019.

[23] Y. Zhang, L. Song, W. Saad, Z. Dawy, and Z. Han, “Contract-based incentive mechanisms for device-to-device communications in cellular networks,” *IEEE J. Sel. Areas Commun.*, vol. 33, no. 10, pp. 2144–2155, Oct. 2015.

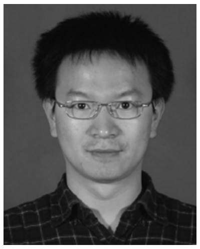
[24] Z. Chen, T. Ni, H. Zhong, S. Zhang, and J. Cui, “Differentially private double spectrum auction with approximate social welfare maximization,” *IEEE Trans. Inf. Forensics Security*, vol. 14, pp. 2805–2818, 2019.

[25] H. Jin, G. Sun, X. Wang, and Q. Zhang, “Spectrum trading with insurance in cognitive radio networks,” in *Proc. 31st IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Orlando, FL, USA, Mar. 2012, pp. 2041–2049.

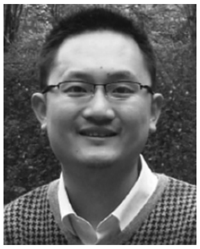


Wen Tian (Graduate Student Member, IEEE) received the B.S. degree in physics from the Changsha University of Science and Technology, Changsha, China, in 2014, and the M.S. degree in control theory and control engineering from the Jiangsu University of Science and Technology, Zhenjiang, China, in 2017. He is currently the Ph.D. degree with the Nanjing University of Science and Technology, Nanjing, China. His research interests include cyber–physical systems and network security.

Miao Du is currently pursuing the Ph.D. degree with the School of Computer Science and Engineering, Southeast University, Nanjing, China. He is also a Research Assistant with the College of Internet of Things, Nanjing University of Posts and Telecommunications, China. His current research interests include wireless sensor network, social networks, security, game theory, smart grid communications, and cyber–physical systems.



Xiaopeng Ji (Member, IEEE) received the B.S. degree in electronics and information engineering and the Ph.D. degree in control science and engineering from the Nanjing University of Science and Technology, Nanjing, China, in 2005 and 2010, respectively. From 2010 to 2016, he was a Senior Research, a Development Engineer, and a Technical Manager in microgrid and active distribution systems with Beijing Sifang Automation Company, Ltd. From 2016 to 2019, he was a Lecturer with the School of Automation, Nanjing University of Science and Technology. He is currently a Senior Engineer with the School of Electronic and Information Engineering, Nanjing University of Information Science and Technology. His research interests include smart grids, cyber–physical systems, and cyber-security dynamics.



Guangjie Liu received the B.S. degree in electrical and computer engineering and the Ph.D. degree in control science and engineering from the Nanjing University of Science and Technology, Nanjing, in 2002 and 2007, respectively, where he is currently a Professor with the School of Electronic and Information Engineering. His research interests are multimedia systems and deep learning.

Yuewei Dai received the B.S. and M.S. degrees in system engineering from the East China Institute of Technology, Nanjing, China, in 1984 and 1987, respectively, and the Ph.D. degree in control science and engineering from the Nanjing University of Science and Technology, in 2002, where he is currently a Professor with the School of Electronic and Information Engineering. His research interests are in multimedia security, system engineering theory, and network security.

Zhu Han (Fellow, IEEE) received the B.S. degree in electronic engineering from Tsinghua University, in 1997, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, in 1999 and 2003, respectively. From 2000 to 2002, he was an Research and Development Engineer with JDSU, Germantown, Maryland. From 2003 to 2006, he was a Research Associate with the University of Maryland. From 2006 to 2008, he was an Assistant Professor with Boise State University, Idaho. He is currently a John and Rebecca Moores Professor with the Electrical and Computer Engineering Department as well as with the Computer Science Department, University of Houston, Houston, TX, USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul, South Korea. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, big data analysis, security, and smart grid. He received an NSF Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for the Journal on Advances in Signal Processing in 2015, the IEEE Leonard G. Abraham Prize in the field of Communications Systems (Best Paper Award in IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS) in 2016, and several best paper awards in IEEE conferences. He is also the Winner of 2021 IEEE Kiyo Tomiyasu Award, for outstanding early to mid-career contributions to technologies holding the promise of innovative applications, with the following citation: "For Contributions to Game Theory and Distributed Management of Autonomous Communication Networks." Since 2017, he has been 1% highly cited researcher according to Web of Science. He was an IEEE Communications Society Distinguished Lecturer from 2015 to 2018, and since 2019, he has been an AAAS Fellow and an ACM Distinguished Member.