Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid

Kun Wang, *Member, IEEE*, Miao Du, Sabita Maharjan, *Member, IEEE*, and Yanfei Sun

***Abstract*—Advanced metering infrastructure (AMI) is an important component for a smart grid system to measure, collect, store, analyze, and operate users consumption data. The need of communication and data transmission between consumers (smart meters) and utilities make AMI vulnerable to various attacks. In this paper, we focus on distributed denial of service attack in the AMI network. We introduce honeypots into the AMI network as a decoy system to detect and gather attack information. We analyze the interactions between the attackers and the defenders, and derive optimal strategies for both sides. We further prove the existence of several Bayesian-Nash equilibriums in the honeypot game. Finally, we evaluate our proposals on an AMI testbed in the smart grid, and the results show that our proposed strategy is effective in improving the efficiency of defense with the deployment of honeypots.**

***Index Terms*—Honeypot, game theory, advanced metering infrastructure, distributed denial of service attack, smart grid.**

I. Introduction

ADVANCED Metering Infrastructure (AMI) is an integration of many technologies that provide apt interactions between client terminals and third party systems. AMI is a crucial component for consumers to obtain near-real time price information, which helps them optimize their power usage. Moreover, AMI makes it possible for the grid to timely receive valuable information about consumers [1], e.g., their power consumption, aiming at ensuring and enhancing the reliability of the power system. Nonetheless, the two-way communications between the grid and the users may also increase the vulnerability of an AMI network to malicious attacks.

Manuscript received August 31, 2016; revised November 22, 2016 and January 7, 2017; accepted February 5, 2017. Date of publication February 16, 2017; date of current version August 21, 2017. This work was supported in part by the NSFC under Grant 61572262, Grant 61533010, Grant 61373135, Grant 61571233, and Grant 61532013, in part by the National China 973 Project under Grant 2015CB352401, in part by the NSF of Jiangsu Province under Grant BK20141427, in part by the Open Research Fund of the Key Laboratory of Broadband Wireless Communication and Sensor Network Technology (NUPT), the Ministry of Education under Grant NYKL201507, and in part by the Qinlan Project of Jiangsu Province. *(Corresponding author: Yanfei Sun.)* Paper no. TSG-01182-2016.

K. Wang, M. Du, and Y. Sun are with the Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mail: kwang@njupt.edu.cn; dumiao0118@163.com; sunyanfei@njupt.edu.cn).

S. Maharjan is with Simula Research Laboratory, 1325 Fornebu, Norway, and also with the University of Oslo, 1325 Oslo, Norway (e-mail: sabita@simula.no).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2017.2670144

Security issues in networks can be summarized in terms of three main objectives: confidentiality, integrity and availability [2]. Among various types of threats in the smart grid, distributed denial-of-service (DDoS) is a typical attack that severely threatens availability of the communication network resources. DDoS attack refers to any event that can reduce or eliminate the proper execution of the network [3], by making the resources inaccessible for legitimate users.

Honeypot based approach is one of the attractive alternatives to counter DDoS attacks as it can protect the network while also consuming less resources. Honeypots are security resources that help attract, detect, and gather attack information. By pretending to be normal servers to attract the attackers, honeypots can consume attackers' resources and time. They can also influence and interfere with the choice of intruders, and further detect the intruders' attack intention. Other than production systems, the main system can monitor any suspicious intrusion to honeypots.

However, the existing work using honeypots mainly addresses static defense, which is insufficient to deal with dynamic attacks [4]. Dynamic attack is a persistent attempt to introduce invalid data into a system, and/or to damage or destroy data already stored in it. In addition, as a rational attacker, it is typical that the attackers generally understand the defense systems in the network by sniffing beforehand. Anti-honeypot is used by attackers to identify and detect the defense systems. The attacker can first utilize an anti-honeypot to detect the honeypot proxy server in the target network by transmitting initiative packets. Once the honeypot server determines, the attacker can bypass the honeypot, and access to the target network through other channels. If the attackers use anti-honeypots to detect the defense systems in the network successfully, they can still find the optimal attack strategies.

In this paper, we study DDoS attacks in AMI networks and introduce a Bayesian honeypot game model. We derive and prove that the equilibrium conditions can be achieved between legitimate users and attackers, for the strategies of honeypots and anti-honeypots, respectively. As a result, we can deploy honeypots reasonably in the AMI networks to consolidate the defense systems according to the equilibriums. Our proposed model does not only improve the detection rate but also helps reduce energy consumption.

To this end, our main contributions are listed as follows:

- We introduce the idea of deploying honeypots into an AMI network for designing secure communications between the operators and the consumers in the smart grid.

- We present a honeypot game to address DDoS attacks in an AMI network and analyse groups of strategies to achieve an optimal equilibrium between legitimate users and attackers.
- We conduct experiments on an AMI testbed to evaluate the performance of our strategy.

The rest of the paper is organized as follows. We propose the system model in Section II. First, we introduce the AMI structure. Then we design the honeypot game model, and prove the existence of Nash equilibriums. The optimal strategies in the honeypot game model are analyzed in Section III. Experimental results are presented in Section IV. A summary of related work is provided in Section V. Finally, in Section VI, we draw the conclusion.

II. System Model

In this section, we describe the AMI structure in the smart grid. Then, we introduce the honeypot game model, define the payoff functions, and derive the Bayesian Nash equilibrium (BNE).

A. AMI Structure

AMI is an advanced form of automated meter reading (AMR). There is one-way communication facilitated for reading meters in the traditional AMR. However, AMI enables two-way communications between the utility company and meters. AMI consists of smart meters, data aggregators, central system (AMI headend), meter data management system (MDMS), and the communication networks and enabling communication technologies [5]. The headend is the intermediate agent between AMI networks and utility applications.

Smart meters are the key components in terms of AMI networks in the smart grid. Apart from measuring power consumption, smart meters can also monitor statistical data, and report to the consumers. Each smart meter connects to an aggregator and periodically forwards the power usage data to it. An aggregator receives data from a batch of meters and forwards them to the headend. Also, control commands sent by the headend is transmitted to meters via aggregators. A meter can directly reach a connection to an aggregator, or through another meter. In virtue of a unique third party network, plenty of aggregators are connected to a headend. A lot of firewalls are deployed in the network to make restrictions on communications between the energy provider's network and AMI.

Fig. 1 demonstrates the AMI structure. We abstract the AMI network into a tree structure. The top node is the headend. Below it are aggregators. Connected to the aggregators are large numbers of smart meters. DDoS attack happens when service users cannot achieve normal service by Internet service provider (ISP) anymore, due to the depletion of network or system resources. In this example, we consider DDoS attacks that target a critical server (e.g., a FTP server or a Web server) in an AMI network. The attacker acquires a number of bots to send DDoS attack traffic to server [6]. First, nodes along the path will quickly become exhausted. Second, the downstream nodes along the main path cannot communicate with the base station properly, due to the tree-structured topology of an AMI. Thus, DDoS attacks may further lead to network paralysis, power shortages, and power overload in the smart grid, or even a major accident [7]. A DDoS attack against an AMI network can be targeted at any node in this tree structure, i.e., either at a smart meter, at an aggregator or at the headend. In this paper, we consider the first two types of attacks where honeypots can be set at the other side of the firewall away from the energy provider. They serve as decoys for the two types of nodes to lure attackers and then detect attacks by permitting themselves to be sniffed, detected or intruded.

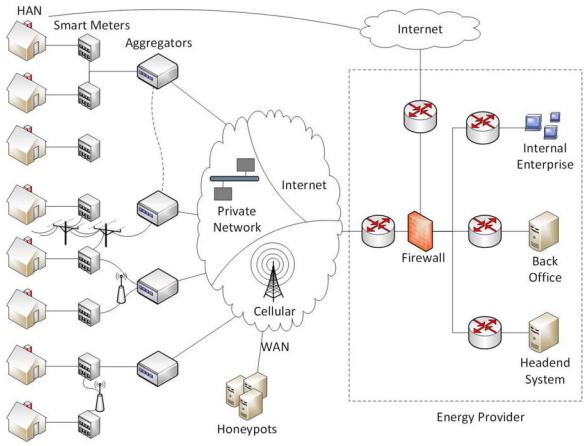


Fig. 1. AMI network infrastructure with honeypot deployment.

Honeypots are designed to be attacked by hackers, they can collect evidence and help hide the real servers. In AMI networks, if the server security measures are not enough, the entire servers are exposed to the attackers. If we embed honeypots into the real servers, the real servers can serve as an internal network on the honeypots' network port mapping, which can increase the safety ratio of the real servers. Even if the attackers penetrate the external "servers", they cannot obtain any valuable information, as they attack honeypots instead [8]. However, if the attackers sniff the deployment of honeypots, and further identify the types of honeypots in AMI networks by deploying anti-honeypots. The attackers can bypass the honeypots to attack the real servers. To address this issue, we propose a honeypot game model, and analyze the interactions between attackers and defenders to derive optimal strategies for honeypots deployment in the AMI networks.

B. Honeypot Game Strategy

As shown in Fig. 2, we define the honeypot game $\mathcal{G}_1$ as $\mathcal{G}_1 \triangleq \{\{\mathcal{Z}, \mathcal{W}\}, \{\mathcal{F}_\mathcal{Z}, \mathcal{F}_\mathcal{W}\}, \{\mathcal{J}_\mathcal{Z}, \mathcal{J}_\mathcal{W}\}\}$. Here, we regard the smart grid system as a service provider (SP). $\{\mathcal{Z}, \mathcal{W}\}$ is the finite collection of players where $\mathcal{Z} \triangleq \{Z_1, Z_2, Z_3\}$, represents different services: real communications, honeypot service, and anti-honeypot service, provided by the SP respectively. $\mathcal{W} \triangleq \{W_1, W_2\}$, represents the set of different visitors: legitimate users and attackers, respectively. $\{\mathcal{F}_\mathcal{Z}, \mathcal{F}_\mathcal{W}\}$ is the set of strategies of the attackers and that of the honeypots, respectively. $\mathcal{F}_\mathcal{Z} \triangleq \{\Omega_1, \Omega_2\}$ is a binary variable, where Ω_1 indicates providing service. $\mathcal{F}_\mathcal{W} \triangleq \{\Lambda_1, \Lambda_2\}$ is also a binary

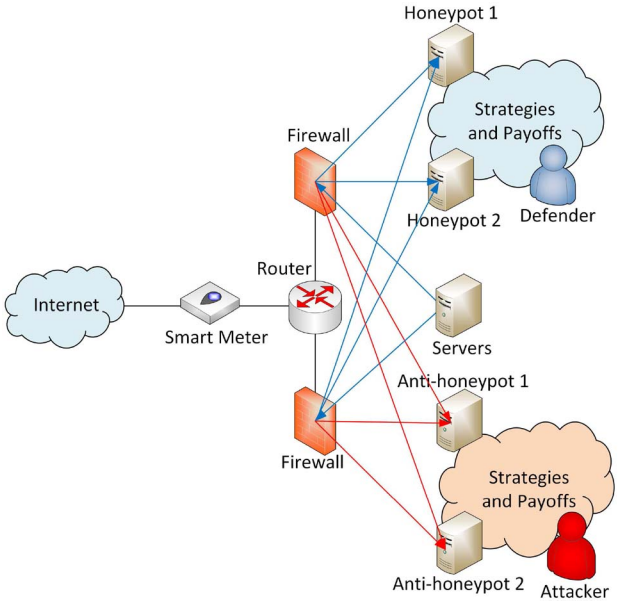


Fig. 2. Honeypot game.

TABLE I
LIST OF SYMBOLS IN THE PAPER

Symbols	Descriptions
Z_1	real communications
Z_2	honeypot service
Z_3	anti-honeypot service
W_1	legitimate users
W_2	attackers
F_Z	strategies of different services
F_W	strategies of different visitors
λ	legitimate users' payoff
ς	attackers' payoff
φ	attack damage factor
δ	honeypot decoy factor
σ	detection probability
Ω_1	SP provides service
Ω_2	SP does not provide service
Λ_1	visitors access
Λ_2	visitors do not access

variable, where Λ_1 indicates providing access. $\{\mathcal{J}_\mathcal{Z}, \mathcal{J}_\mathcal{W}\}$ denotes payoff of the players, where $\mathcal{J}_\mathcal{Z}$ and $\mathcal{J}_\mathcal{W}$ represent the payoffs of the real servers and the visitors, respectively. The detailed list of notations is provided in Table I.

The payoffs are discussed for three different cases as follows.

- **CASE 1:** Real smart grid communication is provided by the SP. If the legitimate users get the service, the payoff is $\lambda(\lambda > 0)$ for legitimate users and attackers, otherwise it is $-\lambda$ for both sides. If the attackers get the service, the service performance will deteriorate, the service-side payoff is $-\varphi\lambda$, the attackers' payoff is $\varphi\lambda$ ($\varphi \geq 1$ represents the attack damage factor, which reflects the degree of damage due to different attacks.), or else service-side's payoff is 0 and attackers' payoff is 0.
- **CASE 2:** Honeypot service is provided by the SP. Honeypot is regarded as the trap to lure attackers. Thus for legitimate users, no matter whether the service-side provides honeypot service or not, they are unable to obtain normal service. Thus the payoff for the legitimate users is $-\lambda$. If the SP provides effective honeypot service to decoy attackers successfully, the payoff for the legitimate users is $\delta\varsigma$ ($\varsigma > 0$, δ represents decoy factor, which reflects the degree of decoy for attackers and $\delta \geq 1$), the attackers' payoff is $-\delta\varsigma$.
- **CASE 3:** Anti-honeypot service is provided by the SP. Anti-honeypot is used by attackers to identify and detect the defense systems. Thus for legitimate users, irrespective of whether the SP provides anti-honeypot service or not, they are unable to obtain normal service. Thus the payoff is $-\lambda$. If the anti-honeypot service is effective/successful, i.e., if it can help the attackers identify the defense systems, the attackers' payoff is $\sigma\varsigma$ ($\varsigma > 0$, σ represents detection probability, which reflects the performance of detecting the defense systems, $\sigma \geq 1$), the legitimate users' payoff is $-\sigma\varsigma$.

In our model, the SP does not know the type of the visitors in advance, but it has a priori information about certain statistical metrics regarding the visitors, for instance, the distribution of the type of visitors. We assume $\{P(W_1) = 1-\theta, P(W_2) = \theta\}$. Similarly, we consider that the visitors also know the probability distributions of the type of services provided, where $\{P(Z_1) = 1-\varpi-\omega, P(Z_2) = \varpi, P(Z_3) = \omega\}$. Since the players are conscious of the strategies of the adversaries, we utilize Bayesian rules to obtain the posterior probability of the players in the game and calculate the expected maximum payoffs for all the players. Clearly, the SP can apply four sets of strategies: $\{(\Omega_1, \Omega_1), (\Omega_1, \Omega_2), (\Omega_2, \Omega_1), (\Omega_2, \Omega_2)\}$, which represents the strategies of both real communications and honeypots. Analogously, $\{(\Lambda_1, \Lambda_1), (\Lambda_1, \Lambda_2), (\Lambda_2, \Lambda_1), (\Lambda_2, \Lambda_2)\}$ represent the strategies of the legitimate users and the attackers, respectively. The payoff of the real services for the strategy Ω_1 is denoted as $J_{Z_1}(\Omega_1)$ where

$$\begin{aligned} J_{Z_1}(\Omega_1) &= P(W_1 \mid \Lambda_1) * (-\varphi\lambda) + P(W_2 \mid \Lambda_1) * (\lambda) \\ &= (-\varphi + \theta\varphi + \theta)\lambda. \end{aligned} \tag{1}$$

Similarly, the payoff of the real services for the strategy Ω_2 can be computed as

$$\begin{aligned} J_{Z_1}(\Omega_2) &= P(W_1 \mid \Lambda_1) * 0 + P(W_2 \mid \Lambda_1) * (-\lambda) \\ &= -\theta\lambda. \end{aligned} \tag{2}$$

Thus, for honeypot services, strategy Ω_1 is the strictly dominant strategy. Consequently, the honeypot services invariably select strategy Ω_1 for any visitor. However, for real services, they can make a choice between strategy Ω_1 and Ω_2. The payoff obtained with strategy Λ_1 of legitimate users is given by

$$\begin{aligned} J_{W_1}(\Lambda_1) &= P(Z_1 \mid \Omega_1) * (-\lambda) + P(Z_2 \mid \Omega_1) * (\lambda) \\ &\quad + P(Z_3 \mid \Omega_1) * (-\lambda) \\ &= (2\varpi - 1)\lambda. \end{aligned} \tag{3}$$

The payoff obtained with legitimate users' strategy Λ_2 can be computed as $J_{W_1}(\Lambda_2) = P(Z_1 \mid \Omega_1) * 0 + P(Z_2 \mid \Omega_1) * 0 + P(Z_3 \mid \Omega_1) * 0 = 0$.
The payoff of attackers with strategy (Λ_1) is

$$\begin{aligned} J_{W_2}(\Lambda_1) &= P(Z_1 \mid \Omega_1) * (-\delta\varsigma) + P(Z_2 \mid \Omega_1) * \varphi\lambda \\ &\quad + P(Z_3 \mid \Omega_1) * \sigma\varsigma \\ &= \varpi(\delta\varsigma + \varphi\lambda) + \omega(\delta + \sigma)\varsigma - \delta\varsigma. \end{aligned} \tag{4}$$

Similarly the payoff of attackers with strategy (Λ_2) can be computed as $J_{W_2}(\Lambda_2) = P(Z_1 \mid \Omega_1) * 0 + P(Z_2 \mid \Omega_1) * 0 + P(Z_3 \mid \Omega_1) * 0 = 0$.

Theorem 1: A BNE strategy $\{(\Omega_1, \Omega_1), (\Lambda_1, \Lambda_1)\}$ exists in the honeypot game model provided

$$\theta < \frac{\varphi}{2+\varphi},\ \varpi < \frac{1}{2},\ \omega < \frac{\varphi\lambda - \delta\varsigma}{2(\delta+\sigma)}.$$

Proof: We first assume that $J_{Z_1}(\Omega_1) = J_{Z_1}(\Omega_2)$. Then, we have

$$\theta = \frac{\varphi}{2+\varphi}. \tag{5}$$

From the perspective of the service-side, according to (5), when the visitors are attackers if $\theta < \varphi/(2+\varphi)$, Ω_1 would be the dominant strategy for the SP. In that case, the SP will provide the real service. Otherwise, if $\theta > \varphi/(2+\varphi)$, Ω_2 would be the dominant strategy. Considering that the players in this game should choose the dominant strategies, we can obtain the dominant strategy $\{(\Omega_1, \Omega_1)\}$ for visitors, which is their strategy $\{(\Lambda_1, \Lambda_1)\}$ under the condition $\theta < \varphi/(2+\varphi)$, if $\theta > \varphi/(2+\varphi)$, the dominant strategy is $\{(\Omega_2, \Omega_1)\}$.

We explain and prove the dominant strategy of the SP when the visitors use strategy $\{(\Lambda_1, \Lambda_1)\}$. Then, we need to evaluate whether the strategy $\{(\Lambda_1, \Lambda_1)\}$ is the dominant strategy or not from the perspective of the visitors. Assuming that $J_{W_1}(\Lambda_1) = J_{W_1}(\Lambda_2)$ and $J_{W_2}(\Lambda_1) = J_{W_2}(\Lambda_2)$, we have

$$\varpi = \frac{1}{2} \tag{6}$$

$$\varpi = \frac{\delta\varsigma - \omega(\delta+\sigma)}{\varphi\lambda + \delta\varsigma}, \tag{7}$$

Solving (6) and (7) simultaneously, we obtain

$$\frac{\delta\varsigma - \omega(\delta+\sigma)}{\varphi\lambda + \delta\varsigma} = \frac{1}{2}, \tag{8}$$

which further yields

$$\omega = \frac{\varphi\lambda - \delta\varsigma}{2(\delta+\sigma)}, \tag{9}$$

$$\theta < \frac{\varphi}{2+\varphi},\ \varpi < \frac{1}{2},\ \omega < \frac{\varphi\lambda - \delta\varsigma}{2(\delta+\sigma)}. \tag{10}$$

Consider the case when $\theta < \varphi/(2+\varphi)$. In this case, according to (6), if the probability of honeypot service is $\varpi < 1/2$, the legitimate users' strategy Λ_1 will be the dominant strategy for SP's strategy $\{(\Omega_1, \Omega_1)\}$. Similarly, according to (7), if the attacker uses strategy Λ_1, the dominant strategy for the SP will be $\{(\Omega_1, \Omega_1)\}$ when $\omega < (\varphi\lambda - \delta\varsigma)/2(\delta+\sigma)$. Thus, from (8) and (9), we can obtain a Bayesian-Nash Equilibrium (BNE) strategy $\{(\Omega_1, \Omega_1), (\Lambda_1, \Lambda_1)\}$ for the game when (10) is true.

When $\theta > \varphi/(2+\varphi)$, the dominant strategy of services is $\{(\Omega_2, \Omega_1)\}$. In this case, the strategy $\{(\Omega_1, \Omega_1), (\Lambda_1, \Lambda_1)\}$ cannot result a BNE in the game according to (7), (8), (9) and (10). ■

Analogously, two other BNE strategies $\{(\Omega_1, \Omega_1), (\Lambda_1, \Lambda_2)\}$ and $\{(\Omega_2, \Omega_1), (\Lambda_2, \Lambda_2)\}$ exist in the game under conditions (11) and (12), respectively.

$$\theta < \frac{\varphi}{2+\varphi},\ \varpi < \frac{1}{2},\ \omega > \frac{\varphi\lambda - \delta\varsigma}{2(\delta+\sigma)}. \tag{11}$$

$$\theta > \frac{\varphi}{2+\varphi},\ \varpi > \frac{1}{2},\ \omega > \frac{\varphi\lambda - \delta\varsigma}{2(\delta+\sigma)}. \tag{12}$$

In the next section, we will analyze the optimal strategies for legitimate users and attackers according to the BNEs.

Algorithm 1: Optimal Strategies for Honeypot Game Model

Input: θ, φ, ϖ, ω, λ, δ and ς
Output: Optimal strategies $\{(\Omega_{ii}, \Omega_{jj}), (\Lambda_{ii}, \Lambda_{jj})\}$
/* Initialize the strategies, $\{\Omega_i, \Omega_j\}$ */
/* Find the stable state */
if $\theta < \varphi/2 + \varphi$ **then**
  if $\omega < (\varphi\lambda - \delta\varsigma)/2(\delta+\sigma) \wedge \varpi < 1/2$ **then**
    choose optimal strategy $\{(\Omega_1, \Omega_1), (\Lambda_1, \Lambda_1)\}$.
  end
  else
    cannot achieve a BNE.
  end
  if $\omega > (\varphi\lambda - \delta\varsigma)/2(\delta+\sigma) \wedge \varpi < 1/2$ **then**
    choose optimal strategy $\{(\Omega_1, \Omega_1), (\Lambda_1, \Lambda_2)\}$.
  end
  else
    cannot achieve a BNE.
  end
end
else
  if $\omega > (\varphi\lambda - \delta\varsigma)/2(\delta+\sigma) \wedge \varpi > 1/2$ **then**
    choose optimal strategy $\{(\Omega_2, \Omega_1), (\Lambda_2, \Lambda_2)\}$.;
  end
  else
    cannot achieve a BNE.
  end
end

III. Optimal Strategies

We first analyze the BNEs in the honeypot game model compared to the traditional game in terms of equilibrium strategies. We, then, analyse the payoffs of legitimate users and attackers via game trees.

A. Nash Equilibrium Analysis in Honeypot Game Model

The honeypot game model is considerably different than the traditional game model in terms of the equilibrium conditions. In a traditional Bayesian game, strategy $\{\Omega_1, (\Lambda_1, \Lambda_2)\}$

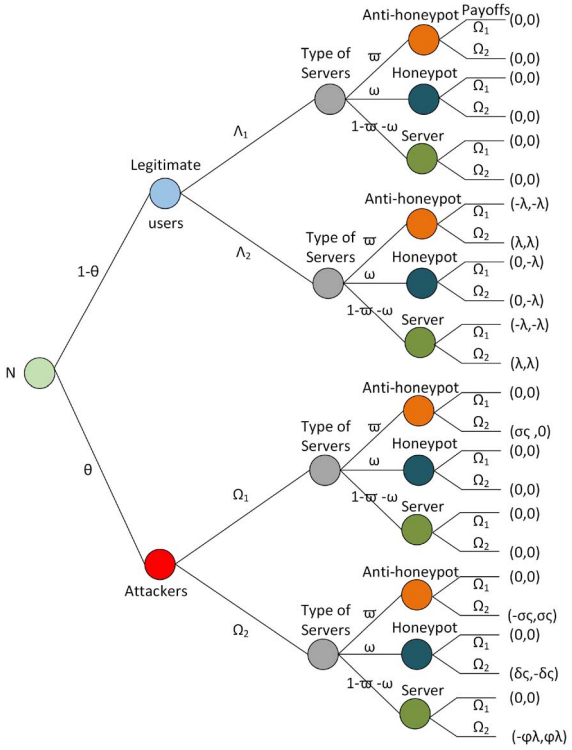


Fig. 3. The game tree from legitimate users' perspective.

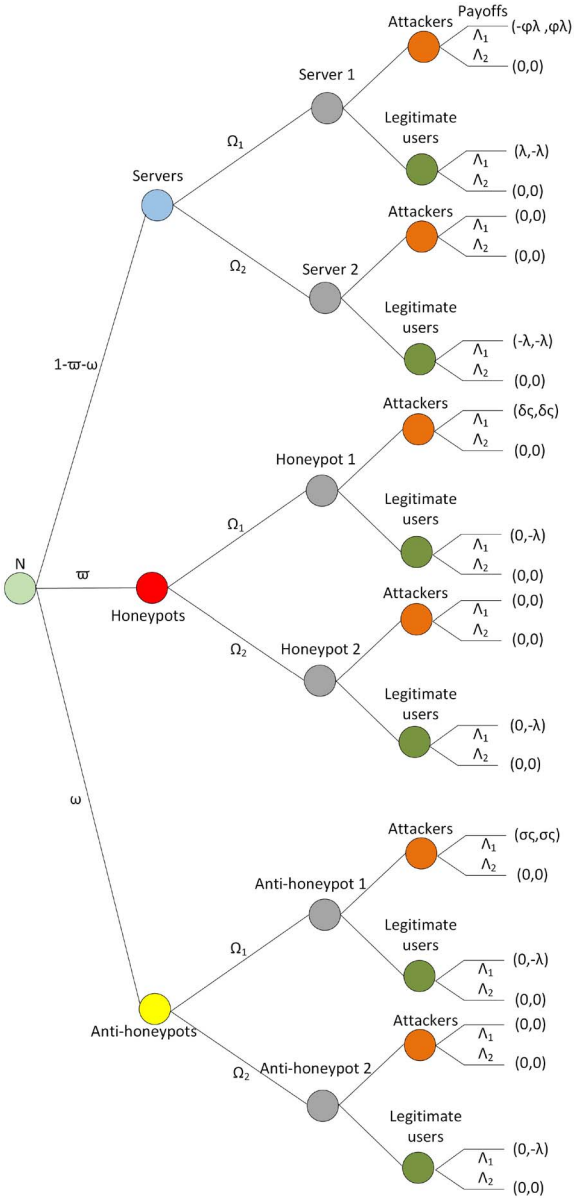


Fig. 4. The game tree from attackers' perspective.

achieves equilibrium only when $\theta < \varphi/(2+\varphi)$, consequently the BNE is only affected by the attackers' probability θ and attack factor φ, which implies that the services can easily suffer attacks. However, in the honeypot game, $\theta < 2/(2+\varphi)$ is only one of the conditions for the equilibrium to exist, and it is also affected by ϖ and ω, the probability of the honeypots and anti-honeypots, attack factor φ, decoy factor δ and detection probability σ, which makes the defense mechanism more active. We present the algorithm to reach the optimal strategies for the honeypot game model in Algorithm 1.

Figs. 3 and 4 are the game trees from the legitimate users' perspective and from the attackers' perspective, respectively. θ is related to the attack damage factor φ, according to (9), ω is related to $(\varphi\lambda - \delta\varsigma)/2(\delta+\sigma)$. Therefore, the BNE conditions are de facto influenced by the value of ϖ, φ, δ, and σ. Considering that attack factor φ is a concrete value, we can improve the degree of decoy factor δ appropriately, and deploy the probability of honeypot ϖ reasonably to achieve optimal defense strategy. On the other hand, the anti-honeypot service is to help attackers identify the defense systems. Attackers can find their optimal strategies according to $\omega = (\varphi\lambda - \delta\varsigma)/2(\delta+\sigma)$. The term 'optimal' is a relative one. A Nash equilibrium is not always the pareto optimal solution but is essentially the best response for given strategies of other players. In a general context, more efficient solutions such as a correlated equilibrium or a social welfare based equilibrium, can exist. However, reaching these equilibriums require extra signaling and/or cooperation among the users. In a scenario with rational players, such 'more efficient' solutions, although, desirable, can not be reached. The 'optimal' was based on the fact that, Nash equilibrium is normally the best possible solution when the players are selfish, and when they do not/are not willing to communicate/cooperate.

More importantly, in a dynamic network, ω should be as small as possible to increase δ. But the higher is δ, the easier it becomes for the attackers to detect the honeypots. Thus the attackers may not carry on the attacks, and the deployment of the honeypots may consume more resources. Similarly, the lower is δ, the defense systems consume fewer resources. But the detection rate is lower. Thus the probability of a successful attack will increase. In addition, we consider that when we deploy too many honeypots in the network, the defense system cannot improve their detection performance, but waste large amount of cyber resources. As a result, we need to reduce the value of ω, and increase the value of the decoy factor δ reasonably in a dynamic environment, in order to find out the dynamic balance between detection rate and energy consumptions.

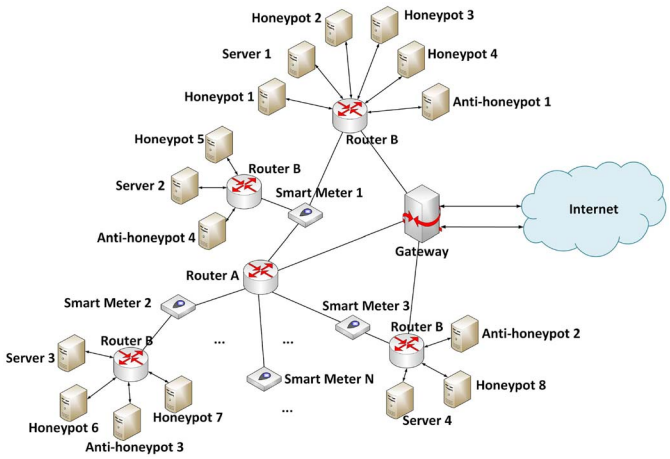


Fig. 5. AMI network testbed.

TABLE II
SIMULATION SETTINGS

Parameters	Parameter Values
Network scale	$400m \times 400m$
Number of nodes	500
Simulation duration	10 minutes
Nodes placement strategy	Random placement
Smart Meters-to-Router B	0.64 Mbps
Router B-to-Smart Meters	0.4 Mbps
Servers-to-Router B	5 Mbps
Router B-to-Gateway	80 Mbps
Gateway-to-Router A	0.5 Gbps
Demand length	1000 bytes
Demand per period	6 s
Time between demands	8 s
Answer length	1000 bytes
Time between periods	12 s
Response time	5 ms
Compared model	CH monitor model, All Monitor model

To this end, we may infer that when we adjust the value of the decoy factor δ appropriately, the HG model can reach a dynamic balance between detection rate and energy consumptions, and effectively solve the DDoS attacks in AMI networks. Then, the proposed model can achieve the optimal strategies for both defenders and attackers when the performance of energy consumption and detection rate reaches a dynamic balance.

IV. PERFORMANCE EVALUATIONS

In this section, we construct an AMI network testbed to evaluate the performance of our scheme. The experiment settings are explained first, followed by detailed experimental results.

A. Experiment Settings

As shown in Fig. 5, we conduct various simulations to explore the appropriate deployment of honeypots to adress DDoS attacks in AMI networks. The constructed topology consists of routers, honeypots, anti-honeypots, smart meters, and normal servers using OPNET simulation environment. Normal servers are viewed as the victims of the attack, which are equivalent to the central servers of an AMI network, and dispatch data to smart meters. Since the central server is one of the most important components in an AMI network, we deploy honeypots, disguised as real servers to lure the attacks and protect the real servers.

We construct a small-scale testbed consisting of 4 servers, 10 honeypots and 2 anti-honeypots. The specific simulation and the Web traffic parameters are shown in Table II. In our experiments, we take two interdependent honeypot services into consideration:

- Anti-honeypot service: we assume that attackers and defenders may have their own strategies in the AMI network. We design the anti-honeypot service to help attackers identify and detect the honeypots in the defense systems.
- Honeypot service: we design the honeypot service to decoy the attackers, in order to protect the normal servers. We can reasonably deploy honeypots in AMI network, and add the decoy performance to improve the effectiveness of defense.

We consider the following combinations of energy consumption and detection rate: $\{\varpi, \omega\} = \{(0.2, 0.6), (0.4, 0.4), (0.6, 0.2)\}$. Under these circumstances, the performance comparisons are between the existing Cluster Head (CH) model [9], All Monitor (AM) model [10], and our honeypot game (HG) model.

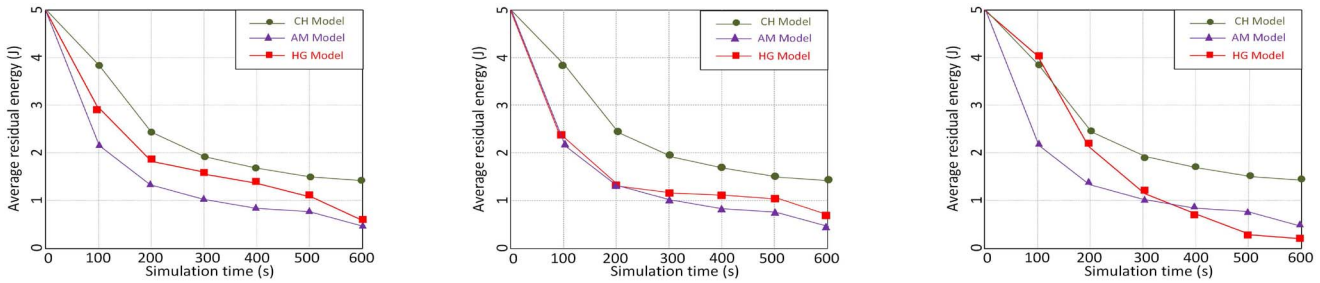
B. Experiment Results

Through these comparisons of the different probabilities, we will get different results for energy consumption and detection rate, which can help us find out the reasonable deployment of honeypots and anti-honeypots in the AMI network.

As shown in Fig. 6, the slope of the energy consumption curves of the HG model in AMI network are relatively smooth, which means the energy consumption is relatively slow. However, The energy consumption rate of the AM model shows substantial variation. AM model's energy consumption far outweighs that of HG model. In addition, different $\{\varpi, \omega\} = \{(0.2, 0.6), (0.4, 0.4), (0.6, 0.2)\}$, result in different energy consumption in HG model.

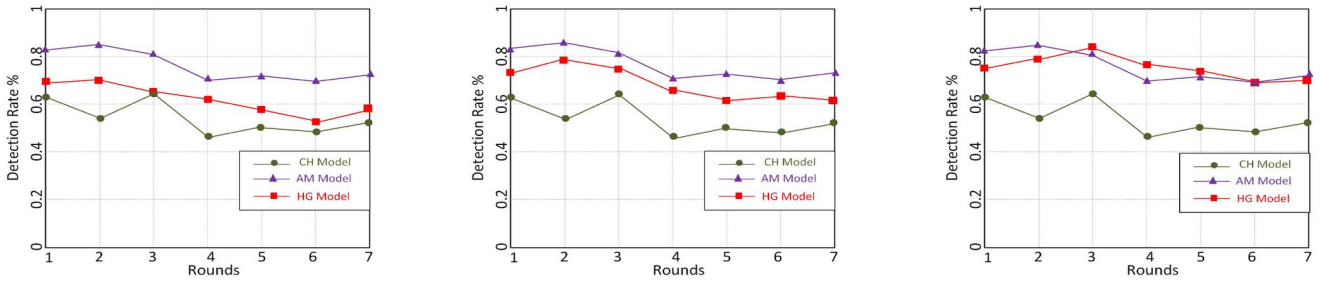
Fig. 7 shows that the CH monitor model's detection rate is between 40% and 60%. On average, the detection rate is about 50%, which means the performance of detection rate is unstable and highly random. In contrast, when $\{\varpi, \omega\} = \{(0.2, 0.6)\}$, the game model's detection rate is between 50% and 70%. When $\{\varpi, \omega\} = \{(0.4, 0.4)\}$, the game model's detection rate is between 60% and 80%, and when $\{\varpi, \omega\} = \{(0.6, 0.2)\}$, the game model's detection rate is between 70% and 85%. These results indicate that increasing the number of honeypots in the AMI network can significantly reduce the anti-honeypot accounts for the proportion of the total number of servers. This can help the normal servers to avoid being the victims of the attacks to a considerable extent.

In addition, when $\{\varpi, \omega\} = \{(0.4, 0.4)\}$, the energy consumption of the HG model is more than in the CH model, but the detection rate is also better than in the CH model.



(a) $\{\varpi,\omega\} = \{(0.2,0.6)\}$ (b) $\{\varpi,\omega\} = \{(0.4,0.4)\}$ (c) $\{\varpi,\omega\} = \{(0.6,0.2)\}$

Fig. 6. Performance for energy consumptions.



(a) $\{\varpi,\omega\} = \{(0.2,0.6)\}$ (b) $\{\varpi,\omega\} = \{(0.4,0.4)\}$ (c) $\{\varpi,\omega\} = \{(0.6,0.2)\}$

Fig. 7. Performance for detection rate.

Similarly, while the energy consumption is slightly less than in the AM model, the detection rate is close to what the AM model can provide. When $\{\varpi, \omega\} = \{(0.6, 0.2)\}$, the energy consumption is close to what the AM model incurs, but the detection rate is higher than in the AM model. When we continue to increase ϖ and decrease ω, which means we need to deploy more honeypots in the networks. However, we find that the energy consumption and the detection rate of these two performances are worse than in the AM model. In other words, along with the change in $\{\varpi, \omega\}$, the energy consumption and the detection rate are also changing. By varying $\{\varpi, \omega\}$, we can find the appropriate value to obtain dynamic balance between energy consumption and detection rate. As a result, we can conclude that

1)In this testbed, $\{\varpi, \omega\} = \{(0.6, 0.2)\}$ can achieve the optimal performance in terms of energy consumption and detection rate. Therefore, we can deploy about 10 honeypots and 3 anti-honeypots in this AMI network testbed.

2)In a dynamic network, more honeypots deployed in the network do not necessarily mean that the defense performance is more effective.

3)When the performance of energy consumption and detection rate reaches a dynamic balance (e.g., $\{\varpi, \omega\} = \{(0.55, 0.25)\}$, the system model will achieve the optimal strategies for both the attackers and the defenders.

V. Related Work

In this section, we propose a brief summary of the state of the art literature on security issues in AMI, honeypot for DDoS attacks, and the use of game theory for modeling DDoS attacks.

A. Security Issues in AMI

Security issues for AMI in the smart grid has been widely studied. Some work focused on intrusion detection. For instance, Faisal *et al.* [11] presented an Intrusion Detection System (IDS) architecture using data stream for AMI in the smart grid, and analysed the performance of existing data stream mining algorithms with an IDS data set. Wang *et al.* [12] introduced a framework of cost-model for evaluating the architectures of IDS. Pivotal management to strengthen the smart grid security includes a significant amount of work. For instance, Ye *et al.* [13] presented a novel protocol called Integrated Authentication and Confidentiality (IAC) to ensure the security in AMI communication. Liu *et al.* [14] presented a novel management model for large number of devices.

In addition, we can list several possible threats related to the development of smart grid as follows: a) high complexity is likely to cause the network to be much easily attacked, as well as lead to some unknown errors. b) some new types of attacks are emerged due to the interactions between different networks, and further cause the collapse of the defense system. c) multiple interfaces in the network may increase the possibility of a DDoS attack. d) multiple nodes in the network are potential threats, since they are very vulnerable to the attackers. e) a large number of data collection and two-way transmission may cause the consumer privacy and data confidentiality to be attacked [15].

B. Honeypot for DDoS

Honeypot is one of the security resources, which is used as a trap to lure the attacker. The concept of honeypots has long

been used to improve security in different systems [16]–[18]. Provos [19] presented 'honeyd', which is a honeypot software package to monitor large-scale honeynet. Dagon *et al.* [20] presented the 'honeyStat' system to utilize honeypots to detect worm attacks in the networks. Jiang and Xu [21] presented a virtual honeynet system with a distributed presence and centralized operation. Wang *et al.* [22] presented a hybrid and distributed honeypot architecture to capture attack traffic. Vrable *et al.* [23] designed large-scale honeynet systems to obtain high-fidelity attack data. Tang and Chen [24] presented a novel 'double-honeypot' detection system which can effectively detect worm attacks.

Some previous studies pointed out the idea that honeypots can be deployed in the smart grid to attract, detect, and gather attack information [25]. Through the use of Virtual Manufacturing (VM) monitors, honeypots are reasonably deployed in the network [24], in order to monitor attacker activities [3], [26], [27]. Hastings *et al.* [28] set a low-interaction honeypot in the smart grid and recorded the attack data for 6 months. Shadow honeypot [29] is a new hybrid detection method, which verifies the abnormal prognosis and improves the algorithm of hybrid detection via feedback mechanism.

C. Game Theory for Modeling DDoS

Game theory has been widely used to analyze the security of critical systems. Mirkovic and Reiher [30] presented a classification of DDoS attacks and defense mechanisms. Peng *et al.* [31] proposed a review of defense mechanisms and DDoS attacks based on networks. Jiang *et al.* [32] introduced a two-person zero-sum game to deal with DDoS traffic injection. Xu and Lee [33] proposed a game-theoretic model to solve DDoS attacks and analyzed the performance of the defense system. Yan and Eidenbenz [34] presented a novel mechanism, providing ISPs to address DDoS attacks in a non-cooperative game. Mohi *et al.* [35] proposed a Bayesian game model to defend against DDoS attacks in wireless sensor networks. Zang *et al.* [36] utilized a Bayesian game model to deal with the DDoS attack. Chai *et al.* [37] proposed the game model in a continuous setting, and the Nash equilibrium can be computed to address attack detection problems.

Nevertheless, to the best of our knowledge, there is little work towards the deployment of honeypots for enhancing security in the smart grid, particularly, focusing the analytical models. Our proposed model can detect DDoS attacks by deploying honeypots in AMI networks with higher probability than traditional methods. We utilize a game theoretical approach to analyze and prove the added security level due to the honeypots while also capturing characteristic features of the attackers, legitimate users, and the service providers. Thus, our model is expected to be useful in deploying honeypots in a real AMI scenario.

VI. Conclusion

In this paper, we introduced honeypots into the AMI network in the smart grid to address DDoS attacks. In addition, we considered the anti-honeypot problem from the perspective of attackers. We presented a honeypot game strategy to analyze the strategic interactions between the attackers and the defenders. Simulation results showed that the energy consumption and the detection rate can be improved with the proposed model, which indicate that the honeypot game strategy can be applied to an AMI network to protect the data and to further ensure the security of AMI networks in the smart grid.

References

[1] F. Ye, Y. Qian, and R. Q. Hu, "A real-time information based demand-side management system in smart grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 2, pp. 329–339, Feb. 2016.

[2] Y. Zhang *et al.*, "Securing vehicle-to-grid communications in the smart grid," *IEEE Wireless Commun.*, vol. 20, no. 6, pp. 66–73, Dec. 2013.

[3] 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.

[4] N. Krawetz, "Anti-honeypot technology," *IEEE Security Privacy*, vol. 2, no. 1, pp. 76–79, Jan./Feb. 2004.

[5] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Başar, "Demand response management in the smart grid in a large population regime," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 189–199, Jan. 2016.

[6] K. Wang, X. Qi, L. Shu, D.-J. Deng, and J. J. P. C. Rodrigues, "Toward trustworthy crowdsourcing in the social Internet of Things," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 30–36, Oct. 2016.

[7] K. Wang, Y. Shao, L. Shu, C. Zhu, and Y. Zhang, "Mobile big data fault-tolerant processing for eHealth networks," *IEEE Netw.*, vol. 30, no. 1, pp. 36–42, Jan./Feb. 2016.

[8] Y. Zhang *et al.*, "Cognitive machine-to-machine communications: Visions and potentials for the smart grid," *IEEE Netw.*, vol. 26, no. 3, pp. 6–13, May/Jun. 2012.

[9] K. Wang *et al.*, "Game-theory-based active defense for intrusion detection in cyber-physical embedded systems," *ACM Trans. Embedded Comput. Syst.*, vol. 16, no. 1, 2016, Art. no. 18.

[10] H. Moosavi and F. M. Bui, "A game-theoretic framework for robust optimal intrusion detection in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 9, pp. 1367–1379, Sep. 2014.

[11] 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.

[12] 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.

[13] 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, 2014, pp. 649–654.

[14] N. Liu, J. Chen, L. Zhu, J. Zhang, and Y. He, "A key management scheme for secure communications of advanced metering infrastructure in smart grid," *IEEE Trans. Ind. Electron.*, vol. 60, no. 10, pp. 4746–4756, Oct. 2013.

[15] R. Yu *et al.*, "Cognitive radio based hierarchical communications infrastructure for smart grid," *IEEE Netw.*, vol. 25, no. 5, pp. 6–14, Sep./Oct. 2011.

[16] K. Wang, L. Yuan, T. Miyazhaki, S. Guo, and Y. Sun, "Anti-eavesdropping with selfish jamming in wireless networks: A Bertrand game approach," *IEEE Trans. Veh. Technol.*, to be published, doi: 10.1109/TVT.2016.2639827.

[17] C. K. Dimitriadis, "Improving mobile core network security with honeynets," *IEEE Security Privacy*, vol. 5, no. 4, pp. 40–47, Jul./Aug. 2007.

[18] K. Wang and M. Wu, "Nash equilibrium of node cooperation based on metamodel for MANETs," *J. Inf. Sci. Eng.*, vol. 28, no. 2, pp. 317–333, 2012.

[19] N. Provos, "A virtual honeypot framework," in *Proc. 13th USENIX Security Symp.*, San Diego, CA, USA, 2004, p. 1.

[20] D. Dagon *et al.*, "HoneyStat: Local worm detection using honeypots," in *Proc. 7th Int. Symp. RAID*, 2004, pp. 39–58.

[21] X. Jiang and D. Xu, "Collapsar: A VM-based architecture for network attack detention center," in *Proc. 13th USENIX Security Symp.*, San Diego, CA, USA, 2004, p. 2.

[22] K. Wang, M. Du, Y. Sun, A. Vinel, and Y. Zhang, "Attack detection and distributed forensics in machine-to-machine networks," *IEEE Netw.*, vol. 30, no. 6, pp. 49–55, Nov./Dec. 2016.

[23] M. Vrable *et al.*, "Scalability, fidelity and containment in the Potemkin virtual honeyfarm," in *Proc. ACM Symp. SOSP*, Brighton, U.K., 2005, pp. 148–162.
[24] Y. Tang and S. Chen, "Defending against Internet worms: A signature-based approach," in *Proc. IEEE INFOCOM*, Miami, FL, USA, 2005, pp. 1384–1394.
[25] T. Flick and J. Morehouse, *Securing the Smart Grid: Next Generation Power Grid Security*. Rockland, MA, USA: Syngress, 2010.
[26] H. A. Lagar-Cavilla *et al.*, "SnowFlock: Rapid virtual machine cloning for cloud computing," in *Proc. ACM Eur. Conf. Comput. Syst.*, Nuremberg, Germany, 2009, pp. 1–12.
[27] N. Provos and T. Holz, *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*. Upper Saddle River, NJ, USA: Addison-Wesley, 2007, pp. 201–211.
[28] J. Hastings, D. M. Laverty, and D. J. Morrow, "Tracking smart grid hackers," in *Proc. 49th Int. Univ. Power Eng. Conf. (UPEC)*, Cluj-Napoca, Romania, 2014, pp. 1–5.
[29] K. G. Anagnostakis *et al.*, "Shadow honeypots," *Int. J. Comput. Netw. Security*, vol. 2, no. 9, pp. 1–15, 2010.
[30] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," in *Proc. ACM SIGCOM*, Portland, OR, USA, 2004, pp. 39–53.
[31] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," *ACM Comput. Surveys*, vol. 39, no. 1, pp. 60–67, 2007.
[32] H. Jiang, K. Wang, Y. Wang, M. Gao, and Y. Zhang, "Energy big data: A survey," *IEEE Access*, vol. 4, pp. 3844–3861, 2016.
[33] J. Xu and W. Lee, "Sustaining availability of Web services under distributed denial of service attacks," *IEEE Trans. Comput.*, vol. 52, no. 2, pp. 195–208, Feb. 2003.
[34] G. Yan and S. Eidenbenz, "DDoS mitigation in non-cooperative environments," in *Proc. Int. Conf. Netw.*, Singapore, 2008, pp. 599–611.
[35] M. Mohi, A. Movaghar, and P. M. Zadeh, "A Bayesian game approach for preventing DoS attacks in wireless sensor networks," in *Proc. Int. Conf. Commun. Mobile Comput.*, Kunming, China, 2009, pp. 507–511.
[36] W. Zang, P. Liu, and M. Yu, "How resilient is the Internet against DDoS attacks?—A game theoretic analysis of signature-based rate limiting," *Int. J. Intell. Control Syst.*, vol. 12, no. 4, pp. 307–316, 2007.
[37] B. Chai, J. Chen, Z. Yang, and Y. Zhang, "Demand response management with multiple utility companies: A two-level game approach," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 722–731, Mar. 2014.

Kun Wang (M'13) received the B.Eng. and Ph.D. degrees with the School of Computer, Nanjing University of Posts and Telecommunications, Nanjing, China, in 2004 and 2009. From 2013 to 2015, he was a Post-Doctoral Fellow with the Electrical Engineering Department, University of California at Los Angeles, CA, USA. In 2016, he was a Research Fellow with the School of Computer Science and Engineering, University of Aizu, Aizu-Wakamatsu City, Japan. He is currently an Associate Professor with the School of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing. He has published over 50 papers in referred international conferences and journals. His current research interests are mainly in the area of big data, wireless communications and networking, smart grid, energy Internet, and information security technologies. He was a recipient of the Best Paper Award at IEEE GLOBECOM'2016. He serves as an Associate Editor of the IEEE ACCESS, the *Journal of Network and Computer Applications*, and *EAI Transactions on Industrial Networks and Intelligent Systems* and an Editor of the *Journal of Internet Technology*. He was the Symposium Chair/Co-Chair of IEEE IECON16, IEEE EEEIC16, IEEE WCSP16, and IEEE CNCC17. He is a member of ACM.

Miao Du is currently pursuing the postgraduation degree in information network with the 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.

Sabita Maharjan received the M.Eng. degree in wireless communication from the Antenna and Propagation Laboratory, Tokyo Institute of Technology, Tokyo, Japan, in 2008, and the Ph.D. degree in network and distributed systems from the University of Oslo, Oslo, Norway, and the Simula Research Laboratory, Fornebu, Norway, in 2013, where she is currently a Post-Doctoral Fellow. Her current research interests include wireless networks, network optimization, security, game theory, smart grid communications, and cyber-physical systems.

Yanfei Sun received the Ph.D. degree in communication and information system from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2006, where he has been a Professor with the College of Telecommunication and Information Engineering, since 2006. His main research interests are in the areas of future network, industrial Internet, big data management, and analysis intelligent optimization and control.