Hidden Electricity Theft by Exploiting Multiple-Pricing Scheme in Smart Grids

Yang Liu, Ting Liu, *Member, IEEE*, Hong Sun, Kehuan Zhang, *Member, IEEE*, and Pengfei Liu

***Abstract*— With the development of demand response technologies, the pricing scheme in smart grids is moving from flat pricing to multiple pricing (MP), which facilitates the energy saving at the consumer side. However, the flexible pricing policy may be exploited for the stealthy reduction of utility bills. In this paper, we present a hidden electricity theft (HET) attack by exploiting the emerging MP scheme. The basic idea is that attackers can tamper with smart meters to cheat the utility that some electricity is consumed under a lower price. To construct the HET attack, we propose an optimization problem aiming at maximizing the attack profits while evading current detection methods, and design two algorithms to conduct the attack on smart meters. Moreover, we disclose and exploit several new vulnerabilities of smart meters to demonstrate the feasibility of HET attacks. To protect smart grids against HET attacks, we propose several defense and detection countermeasures, including selective protection on smart meters, limiting the attack cycle, and updating the billing mechanism. Extensive experiments on a real data set demonstrate that the attack could cause high economic losses, and the proposed countermeasures could effectively mitigate the attack's impact at a low cost.**

***Index Terms*— Smart grids, security, hidden electricity theft, multiple pricing, countermeasures.**

I. Introduction

INCREASING integration of intermittent renewable energy resources is expected to deteriorate the operational security and reliability in the emerging smart grid. Various demand response (DR) techniques have been applied to emphasize these challenges. As one of the most promising technologies, multiple-pricing (MP) scheme (e.g., time-of-use, step tariff, and critical-peak pricing) can shift peak load and encourage energy saving via price incentive [1]. The MP scheme adopts multiple rates under spatial and temporal dependent electricity attributes, such as power quality, level of reliability, volume of usage, and maximum demand [2]. A pilot project in the state of Washington, which ran from March 2006 to March 2007, indicates that scheduling appliances based on the MP scheme can reduce electricity bills by 10% for consumers [3].

Although the evolution from the flat-pricing (FP) scheme to MP scheme will bring significant benefits, its security risks on electricity theft have been mostly ignored. Under the traditional FP scheme, any manipulation on the electricity consumption data will be directly reflected on the final bills, which makes the electricity theft behaviors easy to detect. However, the situation under the MP scheme becomes much more complicated. Attackers could cheat utility companies that the electricity is consumed under periods with lower prices, and take over the benefit provided for real price-sensitive consumers. This kind of electricity theft is quite different from traditional electricity theft behaviors and is harder to detect by existing electricity theft detection (ETD) methods. In this paper, we will show that with exquisite design, attackers could reduce their bills under the MP scheme while evading most of the existing ETD methods.

Besides ETD methods, an alternative approach to defense electricity theft is to protect the smart meters, whose security problem has attracted lots of concern [4]. As summarized in [5], smart meters' typical security vulnerabilities include measurement interruption, password extraction, meter storage tampering, communication interception, and communication tampering. Moreover, the data privacy problem of smart meters should also be noticed [6]–[8]. With the fine-grained electricity consumption data from smart meters, users' power usage pattern could be studied well [9], [10]. Until now, there are already lots of research on protecting smart meters' security and privacy. For example, to limit large-scale attacks on smart meters, McLaughlin et al. leveraged diversity techniques on smart meter's firmware [11]. To secure the communication between smart meters and utility companies, Tsai and Lo proposed a new anonymous key distribution scheme [12]. To protect data privacy, Giaconi et al. utilized renewable energy sources and rechargeable batteries to partially hide the consumer's energy consumption behavior [13]. However, few methods have been deployed in the real world due to the high cost of updating a system with millions of widely distributed meters. Thus, in the real case, smart meters are still susceptible to the attack and could be leveraged by electricity thieves.

Manuscript received March 31, 2019; revised August 9, 2019 and December 26, 2019; accepted December 26, 2019. Date of publication January 9, 2020; date of current version February 6, 2020. This work was supported in part by the National Key Research and Development Program of China under Grant 2018YFB0803501, in part by the National Natural Science Foundation of China under Grant 61772408, Grant U1766215, Grant U1736205, Grant 61721002, and Grant 61632015, in part by the Fundamental Research Funds for the Central Universities, and in part by the Hong Kong SAR Research Grants Council (RGC) General Research Fund (GRF) under Grant 14208019 and Grant 14208818. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Walid Saad. *(Corresponding author: Ting Liu.)*

Yang Liu, Ting Liu, Hong Sun, and Pengfei Liu are with the Ministry of Education Key Lab for Intelligent Networks and Network Security, School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an 710049, China (e-mail: yliu@sei.xjtu.edu.cn; tingliu@mail.xjtu.edu.cn; hsun@sei.xjtu.edu.cn; lpf9456@stu.xjtu.edu.cn).

Kehuan Zhang is with the Department of Information Engineering, The Chinese University of Hong Kong, Hong Kong (e-mail: khzhang@ie.cuhk.edu.hk).

Digital Object Identifier 10.1109/TIFS.2020.2965276

In this paper, we present a hidden electricity theft (HET) attack and discuss its defense strategies. First, we introduce a generalized billing model to present existing pricing schemes in electricity markets. Second, based on this model, we theoretically prove that previous ETD methods may fail under emerging MP schemes. Third, we propose an HET model to maximize attackers' profits, and provide two algorithms for conducting the attack. Fourth, we propose several countermeasures to defense or detect the HET attack at a low cost. Finally, we study the HET attack and its countermeasures through simulations on a real-world data set. Simulation results show that the HET attack may cause significant economic losses to utility companies, and the proposed countermeasures could effectively mitigate its impact.

The remainder of this paper is organized as follows: Section II reviews related work. Section III gives a minimal working example for the proposed attack. Section IV analyzes different pricing schemes under a generalized billing model and shows that the MP scheme is still vulnerable to electricity theft attacks. Section V constructs the HET attack model, proposes algorithms for conducting HET attacks, and demonstrates the attack's feasibility on a smart meter testbed. Section VI designs countermeasures for defensing and detecting HET attacks. Section VII analyzes the impact of HET attacks and the performance of countermeasures through simulation. Section VIII concludes the paper.

II. Related Works

As a major reason for non-technical losses (NTL) during electricity transmission and distribution [14], electricity theft problem has drawn lots of attention. McLaughlin et al. analyzed the strategies for electricity theft in advanced metering infrastructure (AMI) and found that a fully digitized metering system is inherently more dangerous than analog electricity meters [5]. Smith estimated the extent of electricity theft in a sample of 102 countries and showed that electricity theft is increasing in most regions of the world [15]. Depuru et al. overviewed the methods of stealing electricity, including tapping electricity directly from the distribution feeder, tampering smart meters, exchanging the position of breaking wires, isolating the neutral and disturbing the electronic reference point, etc. [16].

Concerning the electricity theft problem, various countermeasures have been proposed. One major approach is to prevent the attack by enhancing the metering system's information security. For example, Xiao et al. presented a mutual inspection strategy with additional sensors to enable non-repudiation on meter readings for smart grids [17]. McLaughlin et al. presented an AMI intrusion detection system (AMIDS) that merges different information to gather a sufficient amount of evidence about an on-going attack before marking an activity as a malicious electricity theft [18]. Fanibhare et al. ameliorated the AMIDS by merging the meters' log files from physical and cyber events and implement the elliptical curve digital signature algorithm (ECDSA) to secure AMIDS [19]. This approach can effectively block the electricity theft behaviors. However, the deployment cost of all these additional devices on all metered nodes is too high.

Another major approach is to detect electricity theft from collected data. Various works have been done on the ETD problem. Anas et al. summarized many types of electricity thefts and proposed several mathematical methods to detect electricity theft [20]. Czechowski and Kosek gave a more detailed review of electricity theft techniques and proposed some security mechanisms and means to detect them [21]. Among all these ETD methods, most of them can be classified into two broad categories, i.e., data-driven methods and consistency-based methods.

A. Data-Driven Methods

Data-driven methods leverage various data mining and machine learning technologies to train a classifier model which captures the electricity consumption pattern based on consumption data. Then the classifier model will be used to detect fraudulent consumers. For example, Nizar et al. detected irregularities in consumption based on an extreme learning machine (ELM) method [22]. Nagi et al. trained a support vector machine (SVM) classifier using historical consumption data to detect abrupt changes in load profile [22]. By combining decision tree (DT) and SVM classifiers, Jindal et al. proposed a comprehensive top-down scheme, which could detect and locate real-time electricity theft at every level in power transmission and distribution (T&D) [23].

B. Consistency-Based Methods

Consistency-based methods leverage physical laws, redundant devices, or additional measurements to detect data inconsistency in the power system. Typical physical laws include Kirchhoff's Law, Ohm's Law and the law of conservation of energy, etc. For example, Kadurek et al. detected electricity tampering based on power balance (the law of conservation of energy) as well as the relationship between power measurements, voltage measurements, and current measurements [24]. Xia et al. located the malicious users based on power balance, and adopted the binary search method and group testing method to shorten the detection time [25]. Moreover, they assessed the suspicions that users steal electricity at first, and then used the assessment to optimize the inspection order [26].

Unfortunately, there exist both merits and defects in current ETD methods. Data-driven methods can conduct the detection very quickly after model training. However, a large amount of training data and long training period are required. Moreover, when the condition changes, the trained model is often not suitable and needs retraining. For example, when some residents move in/out or some electrical appliances change, the electricity usage pattern changes and could not be presented by the original trained model. In addition, supervised learning methods need large amounts of theft samples, which rarely exist in the real case. By contrast, consistency-based methods can conduct the detection with high accuracy when enough data are provided. However, there are also some drawbacks. First, this method is sensitive to data completeness. Once some critical data are missing, the detection may fail. Second, the detection time would be long if there are a

TABLE I
MULTIPLE-PRICING SCHEME IN SHANGHAI, CHINA

Stage #	Consumption (kWh/Year)	Time	Unit Price (CNY/kWh)
I	0-3120	Peak	0.617
		Off-Peak	0.307
II	3120-4800	Peak	0.677
		Off-Peak	0.337
III	>4800	Peak	0.977
		Off-Peak	0.487

considerable number of meters in a distribution network with a complicated network topology. Finally, the cost of deploying redundant devices and transmitting additional measurements should be carefully considered. To reach better detection performance, some researchers have tried to combine data-driven methods and consistency-based methods. For example, in [27], the power balance law is used at first to narrow down the theft detection range, then a multi-class SVM is used to detect the abnormal electricity usage pattern. In [28], the power imbalance is calculated to generate the data set for further training and analysis.

It is worth noticing that there is a conceal assumption for most of the current ETD methods. That is, if the amount of electricity usage is unchanged, the revenue of utility companies will not be affected. This is true under the traditional FP scheme since the electricity bill is linear to the amount of electricity usage. However, the electricity price could vary at different periods or different locations under the MP scheme. Thus, by pretending that some electricity is consumed at a lower price, attackers could gain benefits while keeping the total amount of electricity usage unchanged. Based on this idea, we will develop a novel electricity theft attack called the HET attack in the following sections, which could gain benefits while escaping from most of the current ETD methods.

III. MINIMAL WORKING EXAMPLE

A minimal working example is applied here to show how HET attackers could reduce electricity bills while avoiding detected by ETD methods. State Grid Corporation of China had implemented the latest MP scheme for residential customers in Shanghai, China since 2012. As shown in Table I, there is a three-stage pricing based on annual total electricity consumption. Within each stage, the rates are divided into two parts based on time of use, i.e., peak hours from 6:00 am to 10:00 pm with higher rates and off-peak hours with lower rates. The electricity unit is kWh, and the billing unit is Chinese Yuan (CNY). As shown in Table II, two attack cases for two users (user A and user B) are analyzed under this MP scheme. For the sake of simplicity, we assume that the utility company collect the electricity usage data and calculate the bills once per year. Then attackers should tamper with smart meters once before data are collected.[1]

[1]In reality, utility companies in Shanghai read residential consumers' electricity usage records once per month, and then use these data to detect electricity theft and calculate the bills.

Before Attack: Assume that user A and user B consumed 2000 kWh and 7600 kWh in this year, respectively, and 50% energy consumption had been used during peak hours. The details of electricity consumption and cost could be calculated as *Before Attack* in Table II. The bills of user A and B are 924 CNY and 4342.8 CNY, respectively. The total energy consumption is 9600 kWh, and the revenue of the utility company is 5266.8 CNY.

Attack I: In this case, user A and user B are two collusive attackers, and their goal is to reduce their total bill as much as possible. Meanwhile, they should keep the total electricity consumption unchanged so that this attack would not be detected easily by utility companies' energy consistency-based detection. Then, they can modify electricity consumption data as *Attack I* in Table II. Table II shows two noticeable facts: 1) The overall electricity consumption has not been changed (still 9600 kWh in total), thus the utility company would believe that the coins of every watt have been paid; 2) By shifting some electricity consumption from user B to user A artificially, the total bill for both users is reduced from 5266.8 CNY to 4586.4 CNY (reduced by 12.92 %).

Attack II: In this case, user B is the only malicious attacker, and his goal is to reduce his own bill while keeping the total electricity consumption and user A's bill unchanged, so that his attack would not be noticed by both the utility company and user A. Meanwhile, the attacker also requires that the malicious manipulation on user A's data would not be detected easily by data-driven ETD methods, which means that the range of modification on user A's consumption data should be limited. In this example, user A's modified consumption data should be 50% to 150% of the original consumption data. Then, the attacker can modify the electricity consumption data as *Attack II* in Table II. Table II shows four noticeable facts: 1) The overall energy consumption has not been changed (still 9600 kWh in total), thus the utility company would believe that the coins of every watt have been paid. However, its real revenue is reduced to 5070 CNY (reduced by 3.74%); 2) The bill for user A has been slightly reduced, which would be ignored by most users since the bill is less than the real one; 3) To reduce the risk of being detected by data-driven ETD of user A, the attacker only decreased 250 kWh peak consumption and increased 500 kWh off-peak consumption of user A; 4) The bill for the attacker (i.e., user B) has decreased dramatically from 4342.8 CNY to 4146.75 CNY (reduced by 4.51%).

These two cases demonstrate that attackers can gain economic benefits from utility companies by manipulating meters' electricity consumption data. Meanwhile, attackers' behaviors can evade the detection of current data-driven and consistency-based methods. Hence, although utility companies may notice the revenue's reduction, they may regard it as a consequence of adopting the MP scheme, since more consumers are expected to respond to the flexible electricity prices. From the view of utility companies, attackers in this example are just normal DR participators. Even if utility companies have noticed the revenue's abnormal reduction, they cannot separate attackers from real DR participators by off-the-shelf ETD methods.

TABLE II
ELECTRICITY CONSUMPTION AND BILLS IN THE HET ATTACK EXAMPLE

Stage #	Time	Before Attack (kWh)		Attack I (kWh)		Attack II (kWh)	
		user A	user B	user A	user B	user A	user B
I	Peak	1000	1560	1560	1560	750	2320
	Off-Peak	1000	1560	1560	1560	1500	800
II	Peak	0	840	840	840	0	1240
	Off-Peak	0	840	840	840	0	440
III	Peak	0	1400	0	0	0	490
	Off-Peak	0	1400	0	0	0	2060
Electricity consumption (kWh)		2000	7600	4800	4800	2250	7350
Bills (CNY)		924	4342.8	2293.2	2293.2	923.25	4146.75
Total electricity consumption (kWh)		9600		9600		9600	
Total bills (CNY)		5266.8		4586.4		5070	

IV. SECURITY ANALYSIS OF DIFFERENT PRICING SCHEMES

In this section, we first present a generalized electricity billing model for different pricing schemes. Then, we introduce the attack assumptions under an electricity metering system. At last, we analyze two major ETD methods under different pricing schemes and show that attackers could make profits without being detected under the MP scheme.

A. Generalized Electricity Billing Model

To encourage more consumers to participate in the demand-side management program via financial incentives, utility companies are changing their pricing strategies from the FP scheme to the MP scheme, in which service or product suppliers adjust prices based on the market demands. There are several different MP mechanisms available, such as time-of-use (ToU) pricing, step tariff (a.k.a. the tiered pricing), real-time pricing (RTP), critical-peak pricing (CCP). Specifically, under the RTP scheme, the retail price changes from time to time according to the relationship between power supplies and demands. Under the step tariff scheme, the retail price varies according to the level of consumption during the period specified in the tariff [29]. ToU divides time into different segments, for example, peak hours and off-peak hours, and then charge at different tariffs for each segment. CPP model is an extension of ToU by adding a floating time window called *critical peak hours* for special cases when the imbalance between supplies and demands may affect normal grid operation [30]. Utility companies select one scheme or combine several schemes to generate their tariff systems. For example, the MP of Horizon Power (Australia) is step tariff [31]. The MP of Shanghai (China) in Sec. III is a combination of ToU and step tariff. The MP of Sacramento Municipal Utility District (U.S.) is a combination of ToU, step tariff and CPP [32].

To analyze both FP and MP schemes in a unified framework, we present a generalized electricity billing model here. Assume that there are $m\,(m \geq 1)$ prices in a billing system in the form of $P = [p^1\ p^2 \cdots p^m]^\top$. Under the FP scheme, the electricity price is static and the same for all users, i.e. $m = 1$. Under the MP scheme, the electricity price changes in different cases, i.e., $m > 1$. For simplicity, it is assumed that $p^1 > p^2 > \cdots > p^m$ when $m > 1$. The cumulative electricity consumption vector of user i for all pricing segments at time t can be written as $U_i(t) = [u_i^1(t)\ u_i^2(t) \cdots u_i^m(t)]^\top$ where $u_i^k(t)$ represents the cumulative electricity consumption of user i for price p^k from time 0 up to time t. Then, in a billing cycle which starts from time t and ends at time $t+T$, the electricity bills of user i can be defined as follows:

$$c_i^k = p^k \cdot w_i^k = p^k \cdot \left(u_i^k(t+T) - u_i^k(t)\right)$$

where $w_i^k = u_i^k(t+T) - u_i^k(t)$ and c_i^k are the electricity usage and bill of user i corresponding to price p^k in this billing cycle, respectively.[2] To make the expression compact, we define the following notations:

$$W_i = [w_i^1\ w_i^2\ \cdots\ w_i^m]^\top$$
$$W = [W_1\ W_2 \cdots W_n]$$

where W_i is a vector denoting user i's electricity usage for different prices in this billing cycle, and $\hat{W}$ is a stacked matrix denoting the electricity usage for all n users. Thus, the electricity cost for user i in this billing cycle is

$$c_i^M = P^\top W_i = \sum_{j=1}^{m} (p^j \cdot w_i^j) \tag{1}$$

where $\cdot$ represents the product operation. The total electricity cost for all the n users in this billing cycle is

$$C^M = P^\top W \mathbf{1} = \sum_{i=1}^{n} \sum_{j=1}^{m} (p^j \cdot w_i^j) \tag{2}$$

where $\mathbf{1}$ is a n-dimensional column vector whose elements are all one.

B. Attack Assumption

As shown in Fig. 1, utility companies supply electric power to end consumers via the power distribution grid, which usually has a radial topology [33]. For accurate calculation of electricity bills, smart meters are deployed for every consumer to measure and record their energy consumption. Besides, one gateway meter is installed at the supply side to measure the overall delivered electricity. Suppose that a utility company serves n_0 consumers as in Fig. 1. To build the attack model, we propose the following assumptions.

First of all, it is assumed that among all n_0 consumers, $n\,(n \leq n_0)$ consumers' meters have been compromised

[2]For traditional residential users, w_i^k and c_i^k are always non-negative. However, if there are renewable resources such as PV panels and batteries, w_i^k and c_i^k may be negative.

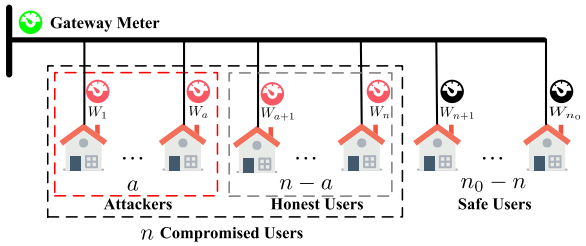


Fig. 1. A metering system for n_0 consumers where n of them are compromised. Among n compromised consumers, there are a attackers and $n-a$ honest users.

(i.e., the consumers in the black dashed box in Fig. 1). Besides, among n consumers, a consumers are the malicious users (attackers) who will launch the attacks, and the other $n-a$ consumers are honest users who are victims. In this paper, n compromised users are denoted by set Ψ. Within Ψ, a malicious users (attackers) are denoted by set Ψ_a, and $n-a$ honest users are denoted by set Ψ_{na}. Note that attackers could hardly compromise all the consumers, so the rest n_0-n consumers in Fig. 1 are safe. However, in the subsequent section, we will show that the terms denoting the consumption data of these safe consumers can be eliminated in the ETD model. Thus, attackers could launch the HET attack successfully with n compromised meters only.

Secondly, it is assumed that the measurement data of compromised smart meters can be manipulated. This seems to be a strong assumption, but it is totally realistic. As will be introduced in Sec. V-C, we have evaluated several off-the-shelf smart meters from well-known vendors and found that all of them are vulnerable to data manipulation attack. Reports from previous researches also confirmed our findings [34]–[36]. Those vulnerabilities are caused by various reasons, such as trivial bugs in codes, legacy protocols and devices, and engineering trade-offs due to operational constraints.

At last, it is assumed that attackers' ultimate goal is to obtain economic gain by paying less money for the same amount of used energy, but try to avoid detection at the same time. This can also be regarded as the definition of the HET attack.

C. Electricity Theft Detection Based on Consistency-Based Methods

Based on the consistency-based detection methods described in Sec. II, utility companies could detect the electricity theft attack with an extra isolated gateway meter attached at the supply side to measure the total supplied electricity. Moreover, honest users may also check their electricity bills to catch any abnormal changes, especially when their bills increase. Based on these detection methods, the following detection constraints need to be satisfied:

$$|w_0 - \sum_{j=1}^{m}\sum_{i=1}^{n}\hat{w}_i^j - \sum_{j=1}^{m}\sum_{i=n+1}^{n_0} w_i^j| \le \theta \cdot w_0 \tag{3a}$$

$$-\sigma_i^{\downarrow}\cdot c_i^M \le \hat{c}_i^M - c_i^M \le \sigma_i^{\uparrow}\cdot c_i^M, \quad \forall i \in \Psi_{na} \tag{3b}$$

where w_0 denotes the total supplied electricity of n_0 users, and θ represents the error factor reflecting the measurement error and power line losses. $\hat{w}_i^j$ $(1 \le i \le n)$ is the reported electricity consumption of compromised user i corresponding to price segment p^j, which might be manipulated by attackers. w_i^j $(n+1 \le i \le n_0)$ is the electricity consumption of safe user i, which could not be accessed and manipulated by attackers. $\hat{c}_i^M$ is the calculated electricity cost based on $\hat{w}_i^j$, i.e. $\hat{c}_i^M = \sum_{j=1}^{m}(p^j \cdot \hat{w}_i^j)$. $\sigma_i^{\downarrow}$ and $\sigma_i^{\uparrow}$ are sensitive factors of honest user i, which are inversely proportional to user i's sensitivity to the bill. Since users with higher bills may be more sensitive, we can infer that $\sigma_i^{\downarrow} > \sigma_i^{\uparrow} > 0$, and both $\sigma_i^{\downarrow}$ and $\sigma_i^{\uparrow}$ are negatively correlated to c_i^M with high probability.

Regarding the above consistency-based ETD procedures, constraint (3a) indicates that the total amount of technical losses (i.e., the difference between overall electricity supply and the total amount of electricity consumption reported by smart meters) should be small and roughly equal to the sum of power line losses and measurement error. Constraint (3b) indicates that the variation of each honest user's bill should be smaller than a certain threshold. Otherwise, it may trigger alarms. Actually, in a real system without attack, technical losses and the variation of each honest user's bill are very limited. Thus θ, $\sigma_i^{\downarrow}$ and $\sigma_i^{\uparrow}$ should be small. If we set θ to zero (i.e., no technical losses in the ideal situation), constraints (3a) can be rewritten as

$$w_0 - \sum_{j=1}^{m}\sum_{i=n+1}^{n_0} w_i^j = \sum_{j=1}^{m}\sum_{i=1}^{n}\hat{w}_i^j \tag{4}$$

In Eq. (4), both terms on the left-hand side are unavailable for attackers. However, according to the law of conservation of energy, we have

$$w_{tot} = \sum_{j=1}^{m}\sum_{i=1}^{n} w_i^j = w_0 - \sum_{j=1}^{m}\sum_{i=n+1}^{n_0} w_i^j \tag{5}$$

where w_{tot} denotes the total supplied electricity of n compromised users. With this substitution, all unknown terms in Eq. (4) are eliminated, and we can focus on n compromised meters for further analysis. The total calculated electricity cost for all compromised users after attack is defined as

$$\hat{C}^M = \sum_{i=1}^{n}\hat{c}_i^M = \sum_{i=1}^{n}\sum_{j=1}^{m}(p^j \cdot \hat{w}_i^j) \tag{6}$$

Note that smaller θ, $\sigma_i^{\downarrow}$ and $\sigma_i^{\uparrow}$ in constraints (3) indicate a stricter consistency-based detector, where less technical losses and bills' variation are allowed. Considering the extreme condition which maximizes the detection capability, we set θ, $\sigma_i^{\downarrow}$ and $\sigma_i^{\uparrow}$ to zero. Thus, constraints (3a) and (3b) can be tightened as

$$w_{tot} = \sum_{j=1}^{m}\sum_{i=1}^{n}\hat{w}_i^j \tag{7a}$$

$$\sum_{j=1}^{m}(p^j \cdot w_i^j) = \sum_{j=1}^{m}(p^j \cdot \hat{w}_i^j), \quad \forall i \in \Psi_{na} \tag{7b}$$

Eqs. (7) are a set of algebraic equations denoting the detection rules of the consistency-based ETD model with maximum detection capability. If attackers want to evade the detection with high probability, the manipulated electricity consumption data should be a solution of Eqs. (7). Otherwise, it may be detected by this ETD method.

After analyzing the ETD model in Eqs. (7), we have the following two propositions.

Proposition 1: Given the electricity theft detection model in Eqs. (7)*, there exists an unique solution if and only if* $a = 1$ *and* $m = 1$.

Proof: In Eqs. (7), the total number of equality constraints is $(n - a + 1)$. Since any electricity usage $\hat{w}_i^j$ for each compromised user and each price may be manipulated, there are $n \cdot m$ variables in total under these constraints. Also, there exists at least one solution for Eqs. (7), i.e. the data without any manipulation in the real case. Thus, the necessary and sufficient condition of unique solution for Eqs. (7) is $(n - a + 1) = n \cdot m$. Since $m \geq 1$, this condition can be met if and only if $a = 1$ and $m = 1$. □

From Proposition 1, we know that all the reported electricity usages cannot be manipulated if and only if there is only one attacker ($a = 1$) under the FP scheme ($m = 1$). Otherwise, if there are multiple collusive attackers ($a > 1$) or the case is under MP scheme ($m > 1$), there may exist multiple solutions for Eqs. (7), which indicates that attackers may manipulate some electricity consumption data without being detected by the detection methods here.

Proposition 2: Given the electricity theft detection model in Eqs. (7)*, the total calculated electricity cost for n compromised users could not be changed by attackers if* $m = 1$.

Proof: After substituting $m = 1$ and Eq. (7a) into Eq. (6), we can obtain that

$$\hat{C}^M = \sum_{i=1}^{n} (p^1 \cdot \hat{w}_i^1) = p^1 \sum_{i=1}^{n} \hat{w}_i^1 = p^1 \ w_{tot}$$

Since w_{tot} cannot be manipulated by attackers, $\hat{C}^M$ could not be changed by attackers. □

From constraint (7b), we know that each honest user's bill is fixed. Thus, combining Proposition 2, we can conclude that under the FP scheme ($m = 1$), attackers could not gain any profits by tampering with the electricity consumption data without being detected. However, attackers may seek profits under the MP scheme ($m > 1$), which can be demonstrated by two simple examples as below.

Example 1 (One User Under the ToU Pricing Scheme): In this example, there is one compromised user with two different prices (i.e., $a = 1, m = 2, p^1 > p^2, \Psi_a = \Psi, \Psi_{na} = \Phi$), where p^1 and p^2 are the peak hour price and off-peak hour price, respectively. As shown in Fig. 2, constraint (7a) is denoted by the black solid line, and constraint (7b) is ignorable since $\Psi_{na} = \Phi$. Point D, E, and F are three examples of feasible solutions. Three dashed lines denote three possible electricity costs C_1, C_2 and C_3, which can be met when the solution is at point D, E, and F, respectively. Combining the assumption $p^1 > p^2$, we can easily know that $C_3 > C_2 > C_1$. Suppose that point E denotes the real consumption data before attack. To reduce the final bill from C_2 to C_1, the attacker should move the reported consumption data from point E to point D. In other words, the attacker should claim that he or she has shifted some load from peak hours (i.e., hours with the higher price p^1) to off-peak hours (i.e., hours with the lower price p^2).

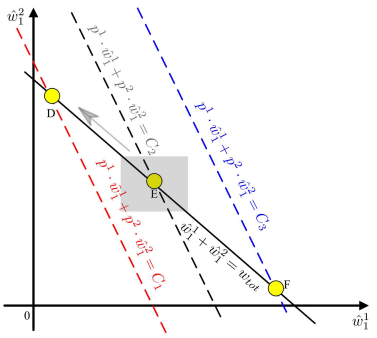


Fig. 2. Example 1 (one user under a ToU pricing scheme).

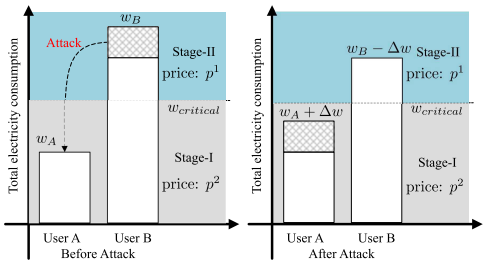


Fig. 3. Example 2 (two users under a tiered pricing scheme).

Example 2 (Two Users Under the Tiered Pricing Scheme): In this example, there are two compromised users with two different prices (i.e., $a = 2, m = 2, p^1 > p^2, \Psi_a = \Psi, \Psi_{na} = \Phi$). When the total electricity consumption is less than $p_{critical}$, the electricity price is p^2 as in stage I. When the total electricity consumption exceeds $w_{critical}$, the electricity price for the excess is p^1 as in stage II. As shown in Fig. 3, the attack is performed by shifting some electricity consumption Δw from user B to user A. Then the total bill for two users is reduced by $(p^1 - p^2)\Delta w$. Meanwhile, Constraint (7a) is met since the total electricity consumption is still $w_A + w_B$, and constraint (7b) is ignorable here since $\Psi_{na} = \Phi$. Thus, for reducing the final bill, big consumers should claim that they have cut down their electricity consumption to a lower stage.

From the above analysis, we can conclude that under the MP scheme, attackers could seek profits by manipulating metering data while bypassing the consistency-based electricity theft detection methods. Indeed, the original intention of the MP scheme is to stimulate users to shift their demand by economic benefits. Thus, attackers can pretend to shift their demand to steal the reward prepared for real DR participators. This is the essence of the proposed HET attack.

Remark 1 (A Win-Win Strategy for Multiple Attackers): In Example 2, if user B manipulates its electricity consumption from w_B *to* $w_B - \Delta w$ *alone, the attack behavior would be detected by consistency-based detection methods according to constraint* (7a)*. Moreover, user A cannot reduce its bill by shifting some electricity consumption to others since its electricity price is the lowest. Thus, user A and user B must cooperate to reduce the final bill without being detected. More generally, if there are multiple attackers, they should collaborate as far as possible to maximize the total attack benefits. Thus, the cooperation strategy is a win-win strategy*

for all attackers, and we will adopt it in the HET attack model.

To avoid unfairness, attackers should share their profits appropriately. One reasonable approach is to distribute the profits proportionally to the attack cost, which could be quantized by multiple factors, including the attack techniques, the attack times, the risk of being detected, etc.

D. Electricity Theft Detection Based on Data-Driven Methods

As discussed in Sec. II, data-driven methods are another type of widely used ETD methods. First, a classifier is trained by normal consumption data samples. Then, when the consumption pattern deviates far from the original pattern, the classifier could detect the anomalies and raise alarms. However, the electricity consumption of a single consumer is usually highly uncertain and hard to predict [37]. To decrease the false alarm rate, the classifier would not regard consumption patterns as attacks if they are closely similar to the original pattern. Thus, attackers could evade the data-driven detection methods by restricting data modification within a reasonable range. The manipulated consumption data of user i in any billing cycle will be limited as

$$\delta_{low} w_i^j \leq \hat{w}_i^j \leq \delta_{high} w_i^j, \quad \forall w_i^j \geq 0 \tag{8a}$$

$$\delta_{high} w_i^j \leq \hat{w}_i^j \leq \delta_{low} w_i^j, \quad \forall w_i^j < 0 \tag{8b}$$

where the attack range $[\delta_{low}, \delta_{high}]$ is defined to restrict the meter's data manipulation in the attack, and $0 < \delta_{low} \leq 1 \leq \delta_{high}$. Constraint (8a) is applied on traditional users without renewable resources, while constraints (8a) and (8b) are both applied on users with renewable resources. Regarding the attack example in Fig. 2, these constraints are denoted by the grey rectangular region near point E. As the attack range narrows down, the attack is harder to detect. Meanwhile, the attack profits may also decrease. The impact of different attack ranges on the attack performance will be evaluated in Sec. VII-A3.

V. Hidden Electricity Theft Attack

In this section, we first propose the HET attack model under the MP scheme based on the analysis in Sec. IV. Then, we propose two algorithms for conducting viable attacks on smart meters. At last, we demonstrate the HET attack's feasibility by analyzing smart meters' security issues on a real testbed.

A. Hidden Electricity Theft Attack Model

As discussed in Sec. IV-B, the ultimate goal for the HET attack is to pay less money for the same amount of consumed electricity without being detected under the MP scheme. Regarding an HET attack starting from time t and ending at time $t + \Delta t$, the attack construction problem can be regarded as an optimization problem as follows:

$$\min_{\hat{w}_i^j} \hat{C}^M \tag{9a}$$

$$\text{s.t.} \quad w_{tot} = \sum_{j=1}^{m} \sum_{i=1}^{n} w_i^j \tag{9b}$$

$$(6), (7), (8) \tag{9c}$$

where w_i^j and $\hat{w}_i^j$ denote the reported electricity usage for user i and price p^j from time t to time $t + \Delta t$ before and after attack, respectively. The total electricity consumption for all n users is calculated by Eq. (9b), which should be consistent with the measurements on the supply side. Eq. (6) defines the objective function $\hat{C}^M$, i.e., the total calculated electricity cost for all compromised users after attack. By introducing constraints (7) and (8), attackers can bypass the ETD methods discussed in Sec. IV. Eq. (7b) guarantees that the bills of non-attackers (i.e., honest users) are unchanged. Thus, seeking the minimal total electricity cost for n compromised users here is equivalent to seeking the minimal electricity cost for a attackers.

Problem (9) represents the general model for constructing the HET attack. It is worth mentioning that there are some implicit constraints in this model. That is, the manipulated consumption data $\hat{w}_i^j$ should follow the pricing scheme. For example, regarding the MP scheme in Table I, the annual accumulated electricity consumption data for stage I should not exceed 3120 kWh.

These implicit constraints are applied when solving problem (9). Specifically, $\hat{w}_i^{peak}$ and $\hat{w}_i^{offpeak}$ are introduced as the decision variables, which denote the total electricity consumption for user i within an attack cycle at peak hours and off-peak hours, respectively. Then, any $\hat{w}_i^j$ in (9) can be expressed by $\hat{w}_i^{peak}$ and $\hat{w}_i^{offpeak}$ according to the pricing scheme in Table I. With this substitution, all implicit constraints for this pricing scheme are satisfied.

Note that under the MP scheme in Table II, utility companies could obtain the total amount of supplied electricity during peak hours and off-peak hours easily. These data may be used for electricity detection. In this case, two additional constraints are added to problem (9) as below [3]

$$\sum_{i=1}^{n} \hat{w}_i^{peak} = \sum_{i=1}^{n} w_i^{peak} \tag{10a}$$

$$\sum_{i=1}^{n} \hat{w}_i^{offpeak} = \sum_{i=1}^{n} w_i^{offpeak} \tag{10b}$$

where w_i^{peak} and $w_i^{offpeak}$ denote the total amount of real supplied electricity during peak hours and off-peak hours, respectively. In this paper, when we study the attack under the MP scheme in Table II, we will add constraints (10) to the attack model by default. For example, in the example in Sec. III, the total amount of supplied electricity during peak hours and off-peak hours are unchanged after the attack.

With these implicit constraints and specific constraints, problem (9) is still a linear programming (LP) problem, which

[3]Constraints (10) are specific constraints and will be applied only for the ToU pricing mechanism.

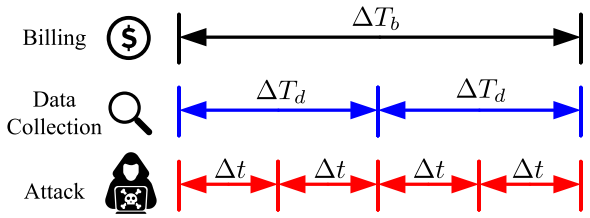


Fig. 4. A schematic diagram of the relationship among the billing cycle, the detection cycle and the attack cycle.

can be solved efficiently by solvers like Gurobi and CPLEX. Note that W, which denotes the original consumption data, is a solution to problem (9) since it can meet all the constraints in problem (9). The corresponding objective is C^M. Thus, problem (9) is always feasible.

After solving the problem, attackers will manipulate all compromised meters' electricity consumption data accordingly. The optimization and data manipulation procedures are conducted online periodically to follow the demand changes within each attack cycle.

Remark 2 (Relaxed Constraints for Total Supplied Electricity During Peak Hours and Off-Peak Hours): After adopting the emerging MP scheme, it is reasonable to assume that not all utility companies will leverage the total amount of supplied electricity during peak hours and off-peak hours to enhance the consistency-based detection. In this scenario, attackers could seek more benefits by relaxing constraints (10) *as*

$$|\sum_{i=1}^{n} \hat{w}_i^{peak} - \sum_{i=1}^{n} w_i^{peak}| \leq \gamma^{peak} \cdot \sum_{i=1}^{n} w_i^{peak} \tag{11a}$$

$$|\sum_{i=1}^{n} \hat{w}_i^{offpeak} - \sum_{i=1}^{n} w_i^{offpeak}| \leq \gamma^{offpeak} \cdot \sum_{i=1}^{n} w_i^{offpeak} \tag{11b}$$

where γ^{peak} and $\gamma^{offpeak}$ denote the error factors for total supplied electricity during peak hours and off-peak hours, respectively.

Remark 3 (Relationship Among the Attack Cycle, the Data Collection Cycle and the Billing Cycle:) As shown in Fig. 4, there are three different cycles in the HET attack model, i.e., the billing cycle ΔT_b, the data collection cycle ΔT_d, and the attack cycle Δt. The billing cycle is the time interval that utility companies calculate the bills, which is usually one month. The data collection cycle refers to the time interval that utility companies collect data from smart meters. Traditionally, the data collection cycle is usually the same as the billing cycle due to the limitation of metering systems. Currently, as smart meters are widely deployed, the data collection cycle becomes much shorter (e.g., one day, an hour, 30 minutes, or 15 minutes). The attack cycle is the time interval between two attacks. If the attack could be finished within each data collection cycle, the collected data could be manipulated successfully without any inconsistency. Thus, we can conclude the relationship among the above cycles as

$$\Delta T_b = N_1 \Delta T_d \tag{12a}$$

$$\Delta T_d = N_2 \Delta t \tag{12b}$$

where N_1 and N_2 are two integers and $N_1 \geq 1, N_2 \geq 1$. Eq. (12a) *is always satisfied since the bills are calculated based on the collected data. Eq.* (12b) *is the necessary condition to guarantee that all the collected data are consistent after the HET attack.*

Note that the data collection cycle could be different from the recorded data's period. For example, some smart meters store the daily consumption data, and the utility company collects all these daily consumption data once per month. In this case, we assume that attackers could change all the relevant daily data before they are collected, which could eliminate all the inconsistencies in the collected data.

B. Algorithms for Conducting HET Attacks

To conduct the proposed HET attack in a real system, attackers need to manipulate the recorded data in compromised smart meters. There are several different methods available. For example, one method is to tamper with the electricity consumption data stored in smart meters directly, or jam-and-inject false data by attacking the communication channels and protocols. Another method is to change some critical parameters in smart meters to change the measurements indirectly. Considering these two approaches, we will present relevant algorithms to launch the HET attack. For simplicity, we define the following notations:

$$\hat{W}_i = [\hat{w}_i^1 \ \hat{w}_i^2 \dots \hat{w}_i^m]^\top, \quad \forall i = 1, 2, \dots, n$$
$$\hat{W} = [\hat{W}_1 \ \hat{W}_2 \dots \hat{W}_n]$$

where $\hat{W}_i$ is the stacked vector denoting the manipulated electricity usage for user i under all price segments, $\hat{W}$ is the stacked matrix denoting the electricity usage for all n users under all price segments after attack, respectively.

1) Algorithm for Tampering With Measurements: As shown in Algorithm 1, the HET attack is launched by tampering with metering measurements directly. At the end of each attack cycle (time $t + \Delta t$), the target electricity consumption W_a is determined from line 3 to line 14. First, the real consumption within this attack cycle (W) is acquired at line 2, and the target of manipulated electricity consumption W_a is initially set as W at line 3. Then if there exist multiple prices in current billing cycle, attackers will try to minimize the total electricity cost by solving the optimization problem (9) at line 6. If the new cost $\hat{m}$ is smaller, which means that attackers indeed could gain some financial rewards by tampering with consumption data from W to $\hat{W}$, then $\hat{W}$ will be set as the target for tampering with electricity consumption at line 9. Otherwise, there is no chance to reduce the overall cost, then the original electricity usage W will be used, and no real tampering operation will be performed. The above procedures are repeated until the end of this attack.

2) Algorithm for Tampering With Parameters: Two of the most common and essential parameters related to metering are the ratio settings for Current Transformer (CT) and Potential Transformer (PT). CT/PT is employed to measure the *current/voltage* and scale the *current/voltage* signal to match the signal input rating of the smart meter [16]. The scale factor of CT/PT can be called the CT/PT ratio. Under different metering environments, the CT/PT ratio in the smart meter should be tuned to meet different CT/PT hardware installed by the grid

Algorithm 1 HET Attack via Tampering With Electricity Consumption Measurements

Input: P, t, Δt
Output: W_a
1: **for** each attack cycle at end time $t + \Delta t$ **do**
2: Acquire W (from time t to time $t + \Delta t$);
3: $W_a = W$;
4: $p_{min} \leftarrow locateMin(P)$, $p_{max} \leftarrow locateMax(P)$;
5: **if** $p_{min} \neq p_{max}$ **then**
6: $\hat{W} \leftarrow$ Solve optimization problem (9);
7: $m \leftarrow P^\top W\mathbf{1}$, $\hat{m} \leftarrow P^\top \hat{W}\mathbf{1}$;
8: **if** $\hat{m} < m$ **then**
9: $W_a = \hat{W}$;
10: **end if**
11: **end if**
12: **end for**

operators. Thus, attackers may tamper with the CT/PT ratio to change the *current*/*voltage* measurements, which can finally change the electricity consumption measurements. With this method, attackers can bypass some complicated consistency-based detection, such as the relationship between *current* and power when the *voltage* is almost fixed.

Since the *voltage* level for a residential consumer is almost fixed and cannot be changed easily without being detected, we will tamper with the CT ratio here. Suppose that the CT ratio for user i at time t before and after attack are $CT_i(t)$ and $CT_i'(t)$, respectively. Then the scaling ratio of the *current* measurement for user i at time t can be defined as

$$\lambda_i(t) = \frac{CT_i'(t)}{CT_i(t)} \tag{13}$$

Combining the relationship between CT ratio and the metered *current*, we can obtain

$$\hat{I}_i(t) = \lambda_i(t) I_i(t) = \frac{CT_i'(t)}{CT_i(t)} I_i(t) \tag{14}$$

where $I_i(t)$ and $\hat{I}_i(t)$ represent the *current* measurement of user i at time t before and after attack, respectively.

Let $\Lambda = [\lambda_1(t)\ \lambda_2(t) \cdots \lambda_n(t)]^\top$ denote the scaling ratio vector for all n consumers, then the manipulated electricity consumption within this attack cycle can be written as

$$\hat{W} = diag(\Lambda) W \tag{15}$$

where $diag(\Lambda)$ is a diagonal matrix whose elements along the diagonal are $\lambda_i(t)$.

However, different from the attack based on tampering with electricity consumption measurements directly, this attack is more difficult to launch. This is mainly because these metering parameters will impact future electrical energy measurements. In particular, within an attack cycle from time t to time $t + \Delta t$, manipulation on CT ratio at time t will change all the *current* measurements, and thus change all the measured energy consumption from time t to time $t + \Delta t$. Since the real electricity consumption cannot be predicted perfectly, it is inevitable to introduce some error between real consumption data and the manipulated data after this attack. To evade the detection, attackers should control the error within a limited range.

From Eq. (14), we know that there is a correlation between $\lambda_i(t)$ and $\hat{I}_i(t)$. If there is no attack, then $\lambda_i(t) = 1$, $\hat{I}_i(t) = I_i(t)$. Therefore, there is also a correlation between $\lambda_i(t) - 1$ and the measurement error within each attack cycle. Therefore, we can restrict the variation range of $\lambda_i(t)$ to limit the error indirectly. Here the variation range of $\lambda_i(t)$ is set as

$$\lambda_{\min} \leq \lambda_i(t) \leq \lambda_{\max}, \quad \forall i = 1, 2, \ldots, n \tag{16}$$

where $\lambda_{\min}$ $(0 < \lambda_{\min} < 1)$ and $\lambda_{\max}$ $(\lambda_{\max} > 1)$ denote the lower bound and upper bound for the variation range of $\lambda_i(t)$, respectively.

After tampering with the parameters, the relative error between the manipulated electricity consumption and the real electricity consumption within the current attack cycle can be defined as

$$\begin{aligned} e &= (\mathbf{1}^\top \hat{W}\mathbf{1} - \mathbf{1}^\top W\mathbf{1})/(\mathbf{1}^\top W\mathbf{1}) \\ &= (\hat{w}_{tot} - w_{tot})/w_{tot} \end{aligned} \tag{17}$$

where $w_{tot} = \mathbf{1}^\top W\mathbf{1}$ and $\hat{w}_{tot} = \mathbf{1}^\top \hat{W}\mathbf{1}$ denote the summation of all users' electricity consumption before and after the parameter manipulation attack, respectively. Borrowing insights from automatic control, a negative feedback loop is introduced to reduce the relative error within each attack cycle, which will be illustrated in the following proposed algorithm. Accordingly, constraint (16) is adapted temporarily as

$$\lambda_{\min} \leq \lambda_i(t)(1 + e) \leq \lambda_{\max}, \quad \forall i = 1, 2, \ldots, n \tag{18}$$

Algorithm 2 HET Attack via Tampering With Meter Parameters

Input: P, t, Δt
Output: Λ
1: **for** each attack cycle at start time t **do**
2: Calculate e for last attack cycle using Eq. (17);
3: Estimate real consumption data W in this attack cycle (from time t to time $t + \Delta t$);
4: $p_{min} \leftarrow locateMin(P)$, $p_{max} \leftarrow locateMax(P)$;
5: **if** $p_{min} \neq p_{max}$ **then**
6: $(\hat{W}, \Lambda) \leftarrow$ Solve optimization problem (9) with additional constraints (15) and (18);
7: **end if**
8: $\Lambda = \Lambda * (1 + e)$;
9: Output: Λ;
10: **end for**

As described in Algorithm 2, the target attack vector Λ is determined at the beginning of each attack cycle (time t). First, the relative error e for the last attack cycle is calculated at line 2 (zero for the first time to launch attacks). Then, the real consumption data W within this attack cycle is estimated based on historical consumption data at line 3. Afterwards, if there exist multiple prices in current billing cycle, attackers will try to minimize the total electricity cost by solving the optimization problem (from line 5 to line 7). By introducing the term $1+e$ into constraint (16) as (18), the error can provide a negative feedback on all the manipulated ratios $\lambda_i(t)$. For example, when the relative error e increases, the term $1 + e$ in (18) drives $\lambda_i(t)$ to decrease by narrowing down $\lambda_i(t)$'s variation range, which in turn decrease the error. At line 8,

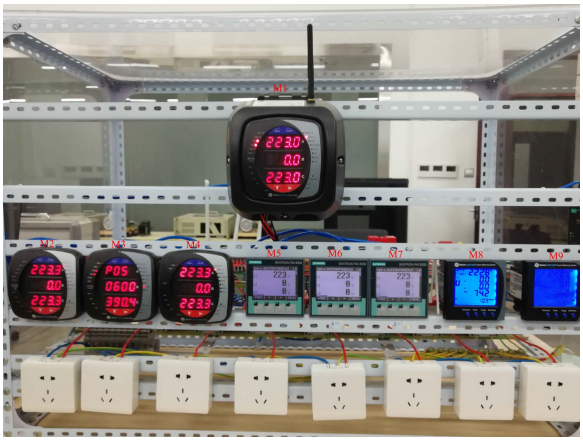


Fig. 5. A smart meter testbed consisting of nine smart meters, i.e., M1 (GE EPM7100), M2 (GE EPM7000), M3 (GE EPM6000), M4 (GE EPM2200), M5-7 (Siemens PAC420) and M8-9 (GE EPM5500P).

the output Λ is scaled by $1+e$ so that the final output Λ can meet constraint (16). Above procedures will be performed repeatedly until the end of this attack.

3) Analytical Analysis of Proposed Algorithms: For both Algorithm 1 and Algorithm 2, the key procedure is to solve optimization problem (9). As discussed in Sec. V-A, problem (9) is an LP problem. Moreover, it is still an LP problem after adding linear constraints (15) and (18). Thus, both proposed algorithms could be solved with high efficiency.

Regarding an attack cycle from time t to time $t+\Delta t$, adversaries in Algorithm 1 would collect the total consumption data W at the end of this attack cycle (i.e., time $t+\Delta t$), and then construct the attack and change meters' measurements directly. In contrast, adversaries in Algorithm 2 need to predict the consumption data $\hat{W}$ within this attack cycle at the beginning of this attack cycle (i.e., time t), and then construct the attack and change meters' CT parameters to impact measurements indirectly. Due to the existence of prediction error between $\hat{W}$ and W, Algorithm 2's solution is biased from the optimum in the real case. Moreover, although constraint (18) could help reducing the error between $\hat{w}_{tot}$ and w_{tot}, it will limit the range of manipulated electricity consumption. Thus, Algorithm 2's attack profits are usually less than that of Algorithm 1.

C. Feasibility Analysis on Smart Meter Testbed

As shown in Fig. 5, we have analyzed the security issues of smart meters on a real testbed to demonstrate the feasibility of conducting HET Attacks. Since the Modbus protocol is supported by all the smart meters in our testbed, we choose it to communicate for convenience. First, we introduce how to conduct attacks based on tampering with meters' measurements and parameters, respectively. Then, we briefly introduce two unpublished vulnerabilities to demonstrate that some smart meters can be fully compromised.

1) Meter Attack via Tampering With Measurements: To launch the attack in Sec. V-B1, we should tamper with smart meters' consumption data. After investigation, we have found that the energy consumption data could be manipulated in some meters. For example, Table III lists four Modbus registers of the energy consumption in the smart meter called GE EPM5500P. The first column represents register's name, in which the *import energy* is the accumulated electrical energy flowing from the power grid to the consumer, the *export energy* is the accumulated electrical energy flowing from the consumer to the power grid, and the *net energy* is the difference between them. The second column represents the register's access address in the Modbus protocol. The third column represents the value range of these registers. The last column represents the accessibility, and R/W means readable and writable with permission.

TABLE III
ELECTRICITY CONSUMPTION REGISTERS IN GE EPM5500P

Name	Address	Range	Access
Import Energy	0x0156	0 to 99,999,999.9	R/W
Export Energy	0x0158	0 to 99,999,999.9	R/W
Net Energy	0x0160	0 to 99,999,999.9	R/W

TABLE IV
REGISTERS RELATED TO CT AND PT IN SIEMENS PAC4200

Name	Address	Range	Access
Primary Voltage	0xC355	1 to 999,999	R/W
Secondary Voltage	0xC357	1 to 690	R/W
Primary Current	0xC35B	1 to 999,999	R/W
Secondary Current	0xC35D	1 or 5	R/W

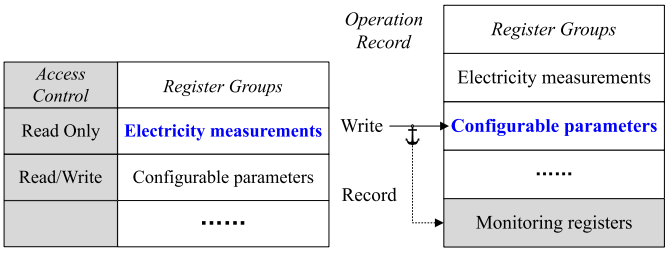
The EPM5500P meter uses four digits password to verify operator' legal identity. Thus, it is easy to guess the password through brute force attack, which has been verified in the real case. After passing the simple password validation mechanism, attackers can tamper with these data in Table III arbitrarily.

However, many smart meters may set the accessibility of these critical registers to read-only (RO). Therefore, the direct tampering of electricity consumption may not work on all smart meters easily. On our testbed, this kind of attack can be conducted on GE EPM5500P and Siemens PAC4200.

2) Meter Attack via Tampering With Parameters: To launch the attack in Sec. V-B2, we should tamper with parameters of smart meters' CT/PT ratios. Specific configurable parameters, such as the CT numerator and the CT denominator, are designed for the CT ratio in smart meters. Likewise, similar configurable parameters are designed for the PT ratio. For example, as shown in Table IV, the Modbus registers related to the CT and PT in the Siemens PAC4200 meter are R/W.

Attackers can tamper with the *current* measurements by changing the values of the CT numerator and the CT denominator (corresponding to the *primary current* and the *secondary current* in Table IV), which will change the electricity consumption data indirectly. This meter also uses a four-digit password to ensure the security of writing action, which could be cracked easily.

3) Two Unpublished Vulnerabilities: After investigation on the mechanism of smart meters in our testbed, we have found two vulnerabilities (design deficiencies or bugs) that can be leveraged by attackers to compromise smart meters: a) the programmable settings (PS) update mode in GE smart meters, where the attacker can fully control this meter when a legal



(a) Patch on access control. (b) Patch on writing operation record.

Fig. 6. Protect against the HET attack by patching smart meters' firmware.

user has been authenticated within one minute; b) the firmware update process of Siemens PAC4200 meter, where the attacker can publish a malicious firmware to users and bypass the firmware integrity check on this meter. We have reported them to smart meters' manufacturers.

VI. Countermeasures

As discussed in Sec. II, defense and detection are two major approaches against the electricity theft attack. In this section, we propose some novel defense and detection countermeasures to mitigate the impact of the HET attack at a low cost. First, we protect a group of smart meters from the HET attack via firmware patches under limited protection resources. Then, we propose two strategies to improve current ETD methods for better detection performance.

A. Selective Protection on Smart Meters

As discussed in Sec. V-B, HET attacks could be conducted by tampering with electricity measurements or configurable parameters. Accordingly, we apply two patches on smart meter's register groups to protect against the HET attack.

1) Patch on Access Control: As shown in Fig. 6a, regarding the attack by tampering with electricity measurements directly, the first patch is to enhance the access control by designing the registers storing the electricity consumption data as read-only registers. With this patch, the metering data could not be easily modified even if attackers can access smart meters through remote network communication.

2) Patch on Writing Operation Record: Different from electricity measurements, smart meters' parameters need to be tuned according to different deployment scenarios, which cannot be designed as read-only registers. Thus, regarding the parameter manipulation attack, the second patch is to add a group of independent and read-only monitoring registers. As shown in Fig. 6b, each writing operation on a critical parameter will increase the value of relevant monitoring registers by one. Moreover, the timestamp for the last writing operation is also recorded. Therefore, the utility company can record its modification operations and detect the illegal operations via these monitoring registers.

With these patches, attackers cannot launch HET attacks easily through tampering with smart meters' electricity measurements or configurable parameters. The only approach left for attackers is to fully control the smart meter and recompile its firmware. However, since smart meters are widely distributed with various brands, configurations, and firmware versions, patches for all smart meters are not practical. Assume that utility companies already know the set Ψ, i.e. all the n deficient smart meters that may be compromised by the attackers in Fig. 1. Then, the optimal defense strategy under limited resources is to select out a group of smart meters to protect, which could minimize the loss caused by any potential HET attacks. The selection strategy could be modeled as follows:

$$\min_{\Psi_p} \max_{\hat{w}_i^j} C^M - \hat{C}^M \tag{19a}$$

$$\text{s.t.} \quad \Psi_p \subset \Psi, \ |\Psi_p|_0 \le n_p \tag{19b}$$

$$\hat{w}_i^j = w_i^j, \quad \forall i \in \Psi_p, \ j = 1, 2, \ldots, m \tag{19c}$$

$$(9b), (9c) \tag{19d}$$

where Ψ_p is the set of protected smart meters, and $|\Psi_p|_0$ is its cardinality. n_p is the maximum number of smart meters protected by utility companies. The objective function minimizes the economic loss $C^M - \hat{C}^M$ caused by any possible HET attacks. Constraint (19b) indicates that utility companies could protect at most n_p smart meters from being compromised. Constraint (19c) indicates that attackers could not manipulate these protected smart meters. Constraints (19d) denote the known constraints when constructing the HET attack.

Problem (19) is a combinatorial optimization problem, and it will degenerate to problem (9) if Ψ_p is fixed. When the number of combinations $\binom{n}{n_p}$ is small, the optimal set could be found efficiently by the exhaustive search method. When $\binom{n}{n_p}$ is large, a suboptimal set could be found by heuristic algorithms like the greedy algorithm, the genetic algorithm, etc. Due to the limitation of space, we will focus on the effectiveness of the selective protection strategy, and the efficient solutions to problem (19) when $\binom{n}{n_p}$ is significantly large will be left as our future work.

B. Enhancement on Electricity Theft Detection

Based on the characters of the HET attack, we propose two strategies to enhance current ETD methods. One strategy is to reduce the attack cycle by random consistency checking; another strategy is to draw innocent users' attention to their consumption behaviors by introducing the charging-rebating model into the current billing system.

1) Detection Based on Random Consistency Checking: As discussed in Remark 3, the attack cycle should be strictly equal to or shorter than the data collection cycle to bypass the detection of current ETD methods. One direct option for improving the performance of ETD methods is to shorten the data collection cycle directly. However, the data collection cycle is limited by the cost of communication, storage, and computation. Inspired by the random checking algorithm in cloud computing, we suggest utility companies adopt the random consistency checking strategy on the electricity data, which is briefly described here. Besides the periodical data collection time, utility companies should randomly select some time, and then collect the data and check the consistency at these additional time within each hour. This strategy needs few additional resources and can cover most of the attack time.

2) Detection Under Charging-Rebating Model: One fundamental assumption for HET attacks is that innocent users (i.e., honest users with compromised smart meters) only care about their electricity bills but ignore the details of electricity consumption. Thus, we can encourage users to focus on their consumption behaviors by changing the billing mechanism from the charging-only model to the charging-rebating model, which can be described as

$$Pay(i) = \sum_{j=1}^{m} w_i^j \cdot p^{high} \tag{20}$$

$$Back(i) = \sum_{j=1}^{m} w_i^j \cdot \left(p^{high} - p^j\right) \tag{21}$$

where user i should firstly pay their bills $Pay(i)$ under the highest price p^{high}, and the utility company will return the balance $Back(i)$ as the rebate. This mechanism can be easily implemented on existing billing systems through software upgrading.

Under this new mechanism, users would care about both the payment and the rebate on their bills. Assume that innocent user i would ignore the bill's change if the following constraint is satisfied

$$-\mu_i^{\downarrow} \leq \frac{\widehat{Pay}(i) - Pay(i)}{Pay(i)} \leq \mu_i^{\uparrow}, \quad \forall i \in \Psi_{na} \tag{22}$$

where $\mu_i^{\downarrow}$ and $\mu_i^{\uparrow}$ denote user i's sensitive factors to the payment $Pay(i)$. Similar to the definition of $\sigma_i^{\downarrow}$ and $\sigma_i^{\uparrow}$ in Eq. (3b), $\mu_i^{\downarrow}$ and $\mu_i^{\uparrow}$ have negative correlation with user i's payment and $\mu_i^{\downarrow} > \mu_i^{\uparrow} > 0$. $\widehat{Pay}(i)$ denotes user i's payment after attack, which could be calculated as

$$\widehat{Pay}(i) = \sum_{j=1}^{m} \hat{w}_i^j \cdot p^{high} \tag{23}$$

By substituting (20) and (23) into (22), we can get

$$-\mu_i^{\downarrow} \leq \frac{\sum_{j=1}^{m} (\hat{w}_i^j - w_i^j)}{\sum_{j=1}^{m} w_i^j} \leq \mu_i^{\uparrow}, \quad \forall i \in \Psi_{na} \tag{24}$$

The above analysis indicates that attackers need to satisfy constraint (24) to evade innocent users' detection. Hence, after the charging-rebating model is adopted, innocent user i's electricity consumption data could not be easily manipulated without being exposed.

VII. Simulation and Analysis

In this section, we study the HET attack algorithms in Sec. V-B and the proposed countermeasures in Sec. VI through simulation on a real-world energy usage data set. First, we analyze the performance of the attack via tampering with measurements, and study the impact of different attack parameters. Then, we study the performance of the attack via tampering with parameters. Lastly, we demonstrate the effectiveness of the proposed countermeasures through simulation.

The data set is obtained from the electricity consumption benchmarks project of Australia [38], which contains the energy consumption of 25 Victorian householders from 2012/4/1 to 2014/3/31. In the simulation, the annual data of 17 general householders from 2013/1/1 to 2013/12/31 are adopted for further analysis. The electricity bills are calculated under Shanghai's MP scheme in Table I. As shown in Table V, the original electricity consumption data range from 1198.25 kWh to 8009.25 kWh, and the total consumption is 68471.25 kWh. Meanwhile, the bills vary from 646.24 CNY to 5606.87 CNY, and the total income of the utility company is 41074.21 CNY.

According to the real settings in Shanghai, both the billing cycle and detection cycle are set as one month in the simulation. Moreover, the attack cycle is also set as one month by default, and it will be changed when we study the impact of different attack cycles.

A. Attack via Tampering With Measurements

The HET attack via tampering with measurements is evaluated in this subsection. First, two critical attack scenarios are investigated: 1) *collusive attack*, where all users are attackers and share the attack profits; 2) *non-collusive attack*, where only one user is the attacker, and the other users are honest users with compromised meters. Then, the impact of the attack range on attack performance is studied. At last, the attack scenario in Remark 2 is analyzed.

1) Collusive HET Attack: In the collusive attack scenario, all users are attackers and share the profits. We simulate three groups of collusive HET attack (attack 1, attack 2 and attack 3) with different attack range (i.e., $[\delta_{low}, \delta_{high}]$ defined in Sec. IV-D), and the changes of energy and bills after attack are shown in Table V. Take attack 1 for example. When the attack range is set as $[0, +\infty)$, attackers can reduce the total electricity bills as high as 2691 CNY. We further analyze the bills of each user and find that HET attack will dramatically reduce the unit electricity prices of big consumers but slightly increase the small consumers. For example, user 7 could save 3108.56 CNY by removing 3710.87 kWh to others, whose unit electricity price is reduced from 0.700 CNY/kWh to 0.581 CNY/kWh. However, user 16 needs to pay extra 1221.93 CNY for additional 2244.36 kWh electricity, whose unit electricity price is increased from 0.539 CNY/kWh to 0.543 CNY/kWh.

As shown in Table V, the loss caused by attack 1 could be as high as 6.5%. It is higher than the profit rate of most utility companies around the world in 2018, such as State Grid Corporation of China (2.7%), Electricite de France (4.6%), ENEL in Italy (5.1%), Tokyo Electric Power (5.4%, Japan), Korea Electric Power (2.2%), and Scottish & Southern Energy (2.6%, Britain). [4] Meanwhile, it is much higher than non-profit Regional Transmission Organizations whose profit rate is less than 1%, such as PJM, NYISO, and MISO in the US. Thus, the HET attack would threaten the profitability of these companies and cause severe problems to the whole power grid.

2) Non-collusive HET Attack: In the non-collusive attack scenario, there is only one attacker. The HET attack simulation procedures are conducted for each user, and the final attack profits are shown in Table VI. As discussed in Sec. V-A, the bills of non-attackers (honest users) would be unchanged. Thus, we only list each attacker's profit, which

[4] These data come from http://fortune.com/fortune500/.

TABLE V

ENERGY AND BILLS BEFORE AND AFTER COLLUSIVE HET ATTACK (ELECTRICAL ENERGY UNIT: KWH, BILLING UNIT: CNY)

User	Original Data		Data Variation after Attack 1 Attack Range: $[0, +\infty)$		Data Variation after Attack 2 Attack Range: $[0.4, 3]$		Data Variation after Attack 3 Attack Range: $[0.8, 1.2]$	
	Energy	Bill	Energy	Bill	Energy	Bill	Energy	Bill
1	2680.84	1547.82	1547.70	845.09	1141.35	626.22	244.13	161.34
2	6683.14	4272.36	-2062.26	-1712.65	-2068.13	-1914.29	-702.36	-720.64
3	4170.32	2392.83	-66.60	-39.19	-62.42	-152.21	234.18	155.34
4	3782.69	1950.45	-64.72	17.74	198.41	115.12	190.18	121.88
5	2854.32	1522.90	1823.16	1050.70	1326.25	1789.85	196.99	235.7
6	2609.16	1487.81	1286.58	668.40	1230.92	698.04	268.55	174.85
7	8009.25	5606.87	-3710.87	-3108.56	-2821.79	-2771.22	-943.57	-929.12
8	4047.20	2106.16	-221.70	4.80	-2.49	16.31	235.73	146.33
9	3550.78	2000.79	210.91	135.53	907.51	468.71	309.32	207.27
10	2510.72	1448.68	1283.87	652.30	1230.06	721.25	275.74	176.33
11	2125.78	1168.43	1637.68	886.17	1401.84	795.41	223.34	135.65
12	4354.37	2453.02	-464.07	-265.97	-368.14	-261.52	57.06	41.32
13	2047.04	1164.68	1783.19	958.42	1330.11	770.01	203.58	129.57
14	4565.71	2425.29	-794.15	-298.46	-794.9	-446.82	107.71	81.96
15	7490.31	5227.63	-3019.89	-2583.62	-2190.05	-2361.46	-729.57	-774.19
16	1198.25	646.23	2244.36	1221.93	2122.45	560.13	130.28	79.46
17	5791.37	3652.26	-1413.19	-1123.58	-1301.33	-1259.37	-301.29	-372.57
Total	68471.25	41074.21	0	-2690.95	0	-2605.84	0	-949.52

TABLE VI

PROFITS OF THE NON-COLLUSIVE HET ATTACK (UNIT: CNY)

User #	Profit	User #	Profit	User #	Profit
1	135.36	7	221.94	13	135.2
2	221.11	8	142.57	14	149.29
3	151.83	9	141.14	15	233.63
4	145.86	10	135.27	16	114.51
5	135.33	11	135.55	17	219.19
6	135.20	12	150.75		

is almost equal to the loss of the utility company. As shown in Table VI, attackers' profits range from 114.51 CNY (user 16) to 233.63 CNY (user 15). Specifically, user 16 gain the least profit from HET attack, who consumes the least electricity among all users. User 2, 7, and 15 could gain the most profit, who are the top three energy consumers. Thus, the non-collusive attack would cause much less loss to the utility company than the collusive attack.

3) Analysis of Attack Range: As indicated in Table V, narrowing the attack range would decrease the profits of HET attacks. Specifically, when the attack range is reduced from $[0, +\infty)$ to $[0.4, 3]$ and $[0.8, 1.2]$, the total saved bill decreases from 2690.95 CNY (saved by 6.55%) to 2605.84 CNY (saved by 6.34%) and 949.52 CNY (saved by 2.3%). However, smaller attack range is preferred to bypass the data-driven theft detection, since the manipulated data would not trigger the abnormal detection alarms when the manipulated data are similar to the real data. To describe the similarity between the manipulated data and the original data for user i, we use the cosine similarity between $\hat{W}_i$ and W_i, which can be calculated as $(W_i^\top \hat{W}_i)/(||W_i|| \cdot ||\hat{W}_i||)$. As shown in Fig. 7, when the attack range narrows from $[0, +\infty)$ to $[0.8, 1.2]$, the average cosine similarity increases from 0.882 to 0.997. Moreover, the minimum cosine similarities under three attack ranges are 0.778, 0.863, and 0.994, respectively. Therefore, the attacker should optimize the attack range to make a trade-off between the attack profits and the risk of being detected.

4) Analysis of Relaxed Constraints for Total Supplied Electricity During Peak Hours and Off-Peak Hours: As discussed

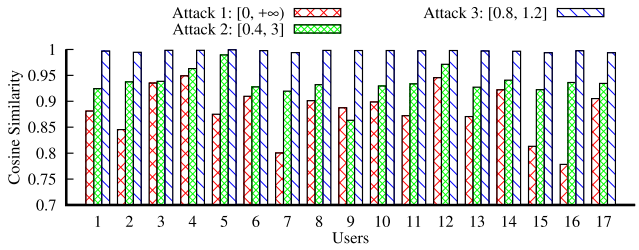


Fig. 7. Cosine similarities between manipulated data and original data under different attack ranges.

in Remark 2, if utility companies do not leverage the total amount of supplied electricity during peak hours and off-peak hours for detection, attackers may seek more benefits. For comparison, we select attack 2 in Sec. VII-A1 (i.e., the collusive HET attack with an attack range of $[0.4, 3]$) as the benchmark. In these new attacks, all the settings are the same as attack 2 except that constraints (10) are replaced by (11). Besides, $\gamma^{offpeak}$ is set the same as γ^{peak} for simplicity.

Fig. 8 shows the error bars of all 17 users' cosine similarity, and the percentage of the total saved bill under different γ^{peak}. From the figure, all users' cosine similarities always keep at a high level as γ^{peak} increases, which ensures that the manipulated data are still similar to the original data. This is because the variation of data is limited by the attack range $[0.4, 3]$. Thus, these new attacks are still safe from being detected by data-driven based methods. Meanwhile, the total saved bill increases almost linearly as γ^{peak} increases. As γ^{peak} increases from 0 to 0.05, the percentage of the total saved bill increases from 6.34% to 7.88%. The result in Fig. 8 suggests that, to reduce economic losses caused by HET attacks, utility companies should always leverage the total supplied electricity data during peak hours and off-peak hours for electricity theft detection.

B. Attack via Tampering With Parameters

In this subsection, we assume that all users are colluded to launch the HET attack by manipulating the meter parameters

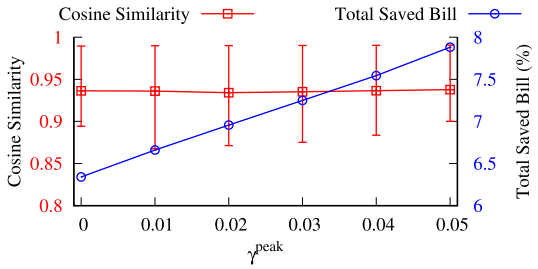


Fig. 8. All users' cosine similarity and the percentage of the total saved bill vs. γ^{peak} for the case discussed in Remark 2.

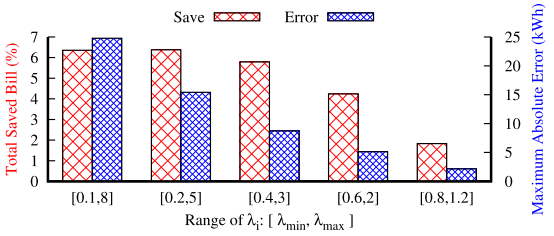


Fig. 9. Attack's maximum absolute error and the percentage of the total saved bill with different ranges of λ_i.

using Algorithm 2. Simulations are conducted on different variation ranges of λ_i (i,e., $[\lambda_{min}, \lambda_{max}]$ as defined in (16)). As discussed in Sec. V-B2, the error between the manipulated data and real consumption data is inevitable due to the estimation error. In fact, there is a positive and tight correlation between the error and the risk of being detected. Therefore, we calculate the absolute error $\left|\hat{w}_{tot} - w_{tot}\right|$ within each hour in a whole year, and find the maximum one with different $[\lambda_{min}, \lambda_{max}]$. Meanwhile, the percentage of the total saved bill is calculated.

As shown in Fig. 9, there is a close correlation between the absolute error and $[\lambda_{min}, \lambda_{max}]$. Furthermore, it can be concluded that the total saved bill after attack directly depends on $[\lambda_{min}, \lambda_{max}]$. When $[\lambda_{min}, \lambda_{max}]$ is narrow, the attacker's ability to manipulate the electricity consumption is limited, which leads to a low reduction ratio of the total electricity bill; when $[\lambda_{min}, \lambda_{max}]$ is wide enough, the percentage of total saved bill can approach the result of HET attack based on tampering with the electricity consumption directly. Therefore, it is necessary to find a trade-off between the attack profits and the risk of being detected. For instance, from the view of attackers, it is a good choice to set the variation range $[\lambda_{min}, \lambda_{max}]$ as $[0.4, 3]$.

C. Selective Protection on Smart Meters

In this subsection, we choose the collusive attack scenario in Sec. VII-A1 as the benchmark and test the selective smart meter protection strategy in Sec. VI-A. Since $\binom{n}{n_p}$ is not very large, we will find out the optimal protection set Ψ_p in problem (19) by the exhaustive search method.

The minimal economic losses under different numbers of protected smart meters are shown in Fig. 10. From the figure, the economic losses decrease quickly when the number of protected smart meters increases. Among all the 17 smart meters, if four meters are protected away from attacks, the economic

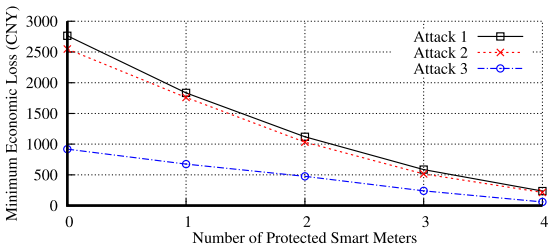


Fig. 10. Minimal economic loss v.s. number of protected smart meters in the collusive attack scenario.

TABLE VII
BILLS AND RELEVANT ECONOMIC LOSS RATES UNDER DIFFERENT ATTACK CYCLES (ORIGINAL TOTAL BILL: 41074.21 CNY)

Attack Cycle	Bills after Attack (CNY)	Loss Rate
1 month	38383.26	6.551%
1 day	38409.20	6.488%
1 hour	38413.11	6.479%
15 minutes	38419.23	6.464%

losses caused by three attacks (i.e., attack 1, attack 2 and attack 3) could be reduced from 2690.95 CNY, 2605.84 CNY and 949.52 CNY to 237.05 CNY, 213.82 CNY and 59.38 CNY, respectively. In other words, more than 90% of the economic losses could be cut down via protecting about 23.5% of all the deficient meters. Hence, by protecting a group of critical smart meters, utility companies could effectively mitigate the impact of HET attacks at a low cost.

D. Enhancement on Electricity Theft Detection

Two strategies proposed in Sec. VI-B is evaluated in this subsection.

1) Detection Based on Random Consistency Checking: We take attack 1 in Sec. VII-A1 as the benchmark, and conduct three new simulations under different attack cycles, including one day, one hour, and 15 minutes. As shown in Table VII, the attack profits may decrease when the attack cycle becomes shorter. For example, the economic loss rate after attack slightly decreases from 6.551% to 6.464% when the attack cycle shortens from one month to 15 minutes. Note that the total amount of supplied electricity during peak hours and off-peak hours has been leveraged for detection, so the principal cause for the bills' variation is that when some user's consumption exceeds the price steps as the attack cycle becomes longer, the optimized attack strategy could be slightly different.

As indicated in Table VII, it is not cost-efficient to shorten the attack cycle by shortening the data collection cycle directly, since it could only cut down a few economic losses. However, shorter attacker cycle means more frequent attack operation, which costs more and increases the risk of being detected by the intrusion detection system. Thus, the random consistency checking strategy is valuable for attack detection since it could shorten the attack cycle at a low cost. For example, utility companies could collect the data and check the consistency randomly once per hour. Accordingly, the only approach for evading the random detection strategy is to shorten the attack

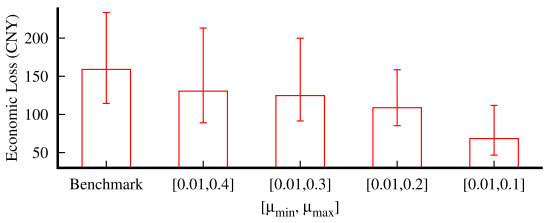


Fig. 11. Economic loss caused by the non-collusive HET attack vs. different range of $\mu_i^{\downarrow}$ ($[2\mu_{min}, 2\mu_{max}]$) and $\mu_i^{\uparrow}$ ($[\mu_{min}, \mu_{max}]$). The first benchmark denotes the same scenario as in Sec. VII-A2. The other bars denote the scenarios with the charging-rebating model, where constraint (24) is applied.

cycle or reduce the attack times, which would increase the attack cost or decrease the attack profits.

2) Detection Under Charging-Rebating Model: To demonstrate the effectiveness of the charging-rebating model, we select the non-collusive HET attack in Sec. VII-A2 as the benchmark and conduct the attack for each user again with additional constraint (24). For simplicity, we assume that $\mu_i^{\downarrow}$ and $\mu_i^{\uparrow}$ are negatively linear to $Pay(i)$, and the range of $\mu_i^{\downarrow}$ and $\mu_i^{\uparrow}$ are set as $[2\mu_{min}, 2\mu_{max}]$ and $[\mu_{min}, \mu_{max}]$, respectively.

Fig. 11 shows the error bars for the economic losses caused by all the non-collusive HET attackers under different $[\mu_{min}, \mu_{max}]$. From the figure, the economic losses decrease a lot when users are more sensitive to the payment in the charging-rebating model (i.e., μ_{max} is smaller). Thus, with the charging-rebating model, the economic losses caused by HET attacks could be effectively cut down if innocent users care more about their payment and rebate on their bills.

VIII. Conclusion and Future Work

This paper revealed a new security threat, called the hidden electricity theft, under emerging multiple-pricing schemes in smart grids. First, we analyzed the security on both flat-pricing and multiple-pricing schemes and find out that current electricity theft detection methods may fail under the multiple-pricing scheme. Based on this idea, we proposed the HET attack model to maximize the economic profits while evading most of the current electricity theft detection methods. We also designed two algorithms to conduct the HET attack on real smart meters and demonstrated the feasibility on the smart meter testbed. Then, we provided some novel countermeasures to protect the multiple-pricing scheme from HET attacks. Lastly, we studied the HET attack and its countermeasures through extensive simulations on a real data set. Simulation results demonstrated that the attack could cause significant economic losses, and the proposed countermeasures could effectively mitigate the impact of this attack.

In the future, we plan to extend our work in three directions. First, we will consider some up-to-date operation and business schemes in the power system, such as distributed generation (i.e., consumers transit the power they generated or stored to the grid) and capacity selling (i.e., consumers commit to reducing loads at times). With these new schemes, the metering and billing system would be much more complicated and vulnerable to the HET attack. Second, we will investigate similar attacks in other physical systems with similar multiple-pricing schemes, such as the water system, the transportation system, the parking system, etc. For these systems, the threats of HET-similar attacks might exist, when the following conditions are satisfied: 1) the structure is few-supplier versus multi-consumer; 2) the billed objects in the system could only be measured but hard to be traced, so that the bill's calculation depends on the meter readings on the demand side; 3) consumers' consumption patterns are hard to predict. Third, we will improve current countermeasures to prevent the HET attack with better performance. For example, we need to find an efficient way to determine the set of protected smart meters for the combinatorial optimization problem (19) when the number of combinations is significantly large.

References

[1] U.S. Department of Energy. (2006). *Benefits of Demand Response in Electricity Markets and Recommendations for Achieving Them*. Accessed: Jan. 18, 2020. [Online]. Available: https://www.energy.gov/oe/downloads/benefits-demand-response-electricity-markets-and-recommendations-achieving-them-report

[2] C. Woo, P. Sreedharan, J. Hargreaves, F. Kahrl, J. Wang, and I. Horowitz, "A review of electricity product differentiation," *Appl. Energy*, vol. 114, pp. 262–272, Feb. 2014.

[3] E. Marris, "Upgrading the grid," *Nature*, vol. 454, no. 7204, pp. 570–573, 2008.

[4] F. M. Cleveland, "Cyber security issues for advanced metering infrastructure (AMI)," in *Proc. IEEE Power Energy Soc. Gen. Meeting-Convers. Del. Electr. Energy 21st Century*, Jul. 2008, pp. 1–5.

[5] S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy theft in the advanced metering infrastructure," in *Proc. Int. Workshop Critical Inf. Infrastruct. Secur.* Berlin, Germany: Springer, 2009, pp. 176–187.

[6] M. R. Asghar, G. Dan, D. Miorandi, and I. Chlamtac, "Smart meter data privacy: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2820–2835, 4th Quart., 2017.

[7] Y. Hong, W. M. Liu, and L. Wang, "Privacy preserving smart meter streaming against information leakage of appliance status," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 9, pp. 2227–2241, Sep. 2017.

[8] P. Kumar, A. Braeken, A. Gurtov, J. Iinatti, and P. H. Ha, "Anonymous secure framework in connected smart home environments," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 4, pp. 968–979, Apr. 2017.

[9] F. Mcloughlin, A. Duffy, and M. Conlon, "A clustering approach to domestic electricity load profile characterisation using smart metering data," *Appl. Energy*, vol. 141, pp. 190–199, Mar. 2015.

[10] A. Al-Wakeel, J. Wu, and N. Jenkins, "K-means based load estimation of domestic smart meter measurements," *Appl. Energy*, vol. 194, pp. 333–342, May 2017.

[11] S. McLaughlin, D. Podkuiko, A. Delozier, S. Miadzvezhanka, and P. McDaniel, "Embedded firmware diversity for smart electric meters," in *Proc. 5th USENIX Conf. Hot Topics Secur. (HotSec)*, 2010, pp. 1–8. Accessed: Jan. 18, 2020. [Online]. Available: http://dl.acm.org/citation.cfm?id=1924931.1924937

[12] J.-L. Tsai and N.-W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 906–914, Mar. 2016.

[13] G. Giaconi, D. Gunduz, and H. V. Poor, "Smart meter privacy with renewable energy and an energy storage device," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 129–142, Jan. 2018.

[14] R. F. Ghajar and J. Khalife, "Cost/benefit analysis of an AMR system to reduce electricity theft and maximize revenues for Électricité du Liban," *Appl. Energy*, vol. 76, nos. 1–3, pp. 25–37, Sep. 2003.

[15] T. B. Smith, "Electricity theft: A comparative analysis," *Energy Policy*, vol. 32, no. 18, pp. 2067–2076, Dec. 2004.

[16] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft," *Energy Policy*, vol. 39, no. 2, pp. 1007–1015, Feb. 2011.

[17] Z. Xiao, Y. Xiao, and D. H.-C. Du, "Non-repudiation in neighborhood area networks for smart grid," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 18–26, Jan. 2013.

[18] S. Mclaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, "A multi-sensor energy theft detection framework for advanced metering infrastructures," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1319–1330, Jul. 2013.

[19] V. Fanibhare, V. Dahake, and S. Duttagupta, "Energy theft detection using AMIDS and cryptographic protection in smart grids," in *Proc. Int. Conf. Internet Things Appl. (IOTA)*, Jan. 2016, pp. 131–136.

[20] M. Anas, N. Javaid, A. Mahmood, S. Raza, U. Qasim, and Z. Khan, "Minimizing electricity theft using smart meters in AMI," in *Proc. 7th Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput.*, Nov. 2012, pp. 176–182.

[21] R. Czechowski and A. M. Kosek, "The most frequent energy theft techniques and hazards in present power energy consumption," in *Proc. Joint Workshop Cyber-Phys. Secur. Resilience Smart Grids (CPSR-SG)*, Apr. 2016, pp. 1–7.

[22] A. H. Nizar, Z. Y. Dong, and Y. Wang, "Power utility nontechnical loss analysis with extreme learning machine method," *IEEE Trans. Power Syst.*, vol. 23, no. 3, pp. 946–955, Aug. 2008.

[23] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar, and S. Mishra, "Decision tree and SVM-based data analytics for theft detection in smart grid," *IEEE Trans. Ind. Informat.*, vol. 12, no. 3, pp. 1005–1016, Jun. 2016.

[24] P. Kadurek, J. Blom, J. F. G. Cobben, and W. L. Kling, "Theft detection and smart metering practices and expectations in The Netherlands," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. Eur. (ISGT Eur.)*, Oct. 2010, pp. 1–6.

[25] X. Xia, Y. Xiao, and W. Liang, "ABSI: An adaptive binary splitting algorithm for malicious meter inspection in smart grid," *IEEE Trans. Forensics Security*, vol. 14, no. 2, pp. 445–458, Feb. 2019.

[26] X. Xia, Y. Xiao, and W. Liang, "SAI: A suspicion assessment-based inspection algorithm to detect malicious users in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 361–374, 2020.

[27] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity theft detection in AMI using customers' consumption patterns," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 216–226, Jan. 2016.

[28] M. Zanetti, E. Jamhour, M. Pellenz, M. Penna, V. Zambenedetti, and I. Chueiri, "A tunable fraud detection system for advanced metering infrastructure using short-lived patterns," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 830–840, Jan. 2019.

[29] International Electrotechnical Commission. (1973). *Tariffs Classed According to Structure*. Accessed: Jan. 18, 2020. [Online]. Available: http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=691-05-12

[30] S. Borenstein, M. Jaske, and A. Rosenfeld, "Dynamic pricing, advanced metering, and demand response in electricity markets," Center Study Energy Markets, CA, USA, Tech. Rep. CSEM-WP-105, 2002.

[31] Horizon Power. *Horizon Power: Western Australia's Regional Electricity Power*. Accessed: Jan. 18, 2020. [Online]. Available: https://horizonpower.com.au

[32] SMUD. *Rate Information*. Accessed: Jan. 18, 2020. [Online]. Available: https://www.smud.org/en/Rate-Information

[33] Y. Liu *et al.*, "Coordinating the operations of smart buildings in smart grids," *Appl. Energy*, vol. 228, pp. 2510–2525, Oct. 2018.

[34] C. Matthew. (2008). *Hacking AMI*. Accessed: Jan. 18, 2020. [Online]. Available: https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1493830240.pdf

[35] N. Lawson. (2010). *Reverse-Engineering a Smart Meter*. Accessed: Jan. 18, 2020. [Online]. Available: https://rdist.root.org/2010/02/15/reverse-engineering-a-smart-meter/

[36] ppcasm. (2012). *Itron Centron C1SR Meter Reverse Engineering*. Accessed: Jan. 18, 2020. [Online]. Available: http://ppcasm.blogspot.hk/2012/10/itron-centron-c1sr-meter-reverse.html

[37] R. Sevlian and R. Rajagopal, "Short term electricity load forecasting on varying levels of aggregation," 2014, *arXiv:1404.0058*.

[38] Department of Industry, Innovation and Science, Australia. (Apr. 2015). *Electricity Consumption Benchmarks*. Accessed: Jan. 18, 2020. [Online]. Available: http://data.gov.au/dataset/0f3d60db-bd63-419e-9cd9-0a663f3abbc9

Yang Liu received the B.S. degree in automation and the Ph.D. degree in cyber security from the School of Electronic and Information, Xi'an Jiaotong University, in 2012 and 2019, respectively. From September 2015 to April 2017, he was a Visiting Scholar with the Department of Electrical and Computer Engineering, University of California at Riverside, Riverside. His research interests include smart grid security, demand response, and cyber-physical systems.

Ting Liu (Member, IEEE) received the B.S. degree in information engineering and the Ph.D. degree in systems engineering from the School of Electronic and Information, Xi'an Jiaotong University, China, in 2003 and 2010, respectively. He was a Visiting Professor with Cornell University from 2016 to 2017. He is currently a Professor with Xi'an Jiaotong University. His research interests include software engineering and cyber-physical systems.

Hong Sun received the B.S. degree in automation and the M.Eng. degree in control engineering from the School of Electronic and Information, Xi'an Jiaotong University, in 2014 and 2017, respectively. He was a Research Assistant with the Department of Information Engineering, The Chinese University of Hong Kong, from September 2016 to January 2017. His current research focuses on security of cyber-physical systems.

Kehuan Zhang (Member, IEEE) received the Ph.D. degree in informatics from Indiana University Bloomington, Bloomington, in 2012. He is currently an Associate Professor with the Department of Information Engineering, The Chinese University of Hong Kong. His research focuses on system and software security, including mobile computing security, cloud computing, and the Internet of Things (IoT) security. He is a member of ACM.

Pengfei Liu received the B.S. degree in automation from the School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China, in 2016, where he is currently pursuing the Ph.D. degree with the School of Cyber Science and Engineering. His research interests include intrusion detection and security of ICSs.