TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 01/12 pp105-120
Volume 19, Number 2, April 2014

Energy-Theft Detection Issues for Advanced Metering Infrastructure in Smart Grid

Rong Jiang*, Rongxing Lu, Ye Wang, Jun Luo, Changxiang Shen, and Xuemin (Sherman) Shen

Abstract: With the proliferation of smart grid research, the Advanced Metering Infrastructure (AMI) has become the first ubiquitous and fixed computing platform. However, due to the unique characteristics of AMI, such as complex network structure, resource-constrained smart meter, and privacy-sensitive data, it is an especially challenging issue to make AMI secure. Energy theft is one of the most important concerns related to the smart grid implementation. It is estimated that utility companies lose more than $25 billion every year due to energy theft around the world. To address this challenge, in this paper, we discuss the background of AMI and identify major security requirements that AMI should meet. Specifically, an attack tree based threat model is first presented to illustrate the energy-theft behaviors in AMI. Then, we summarize the current AMI energy-theft detection schemes into three categories, i.e., classification-based, state estimation-based, and game theory-based ones, and make extensive comparisons and discussions on them. In order to provide a deep understanding of security vulnerabilities and solutions in AMI and shed light on future research directions, we also explore some open challenges and potential solutions for energy-theft detection.

Key words: smart grid; Advanced Metering Infrastructure (AMI); security; energy-theft detection

1 Introduction

The power grid has become a necessity in the modern society. Without a stable and reliable power grid, tens of millions of people's daily life will be degraded dramatically[1]. For instance, the India blackout in July 2012 affected more than 60 million people (about 9% of the world population) and plunged 20 of Indian 28 states into darkness[2]. Indeed, the traditional power grid, which is surprisingly still grounded on the design more than 100 years ago, can no longer be suitable for today's society[3]. With the development of information system and communication technology, many countries have been modernizing the aging power system into smart grid, which is featured with two-way transmission, high reliability, real-time demand response, self-healing, and security.

Within smart grid, Advanced Metering Infrastructure (AMI) plays a vital role and is associated with people's daily life most closely[4]. AMI modernizes the electricity metering system by replacing old mechanical meters with smart meters, which provide two-way communications between utility companies and energy customers. With the AMI, people can not only read the meter data remotely, but also do some customized control and implement fine-coarse demand

• Rong Jiang and Jun Luo are with School of Computer, National University of Defense Technology, Changsha 410073, China. E-mail: jiangrong@nudt.edu.cn; junluo@nudt.edu.cn.
• Rongxing Lu is with School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore. E-mail: rxlu@ntu.edu.sg.
• Ye Wang is with Communication Engineering Research Center, Harbin Institute of Technology Shenzhen Graduate School, Shenzhen 518055, China. E-mail: wangye.hitsz@gmail.com.
• Changxiang Shen is with Computing Technology Institute of China Navy, Beijing 100841, China. E-mail: shenchx@cae.cn.
• Rong Jiang and Xuemin (Sherman) Shen are with Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, N2L 3G1, Canada. E-mail: xshen@bbcr.uwaterloo.ca.
∗ To whom correspondence should be addressed.
Manuscript received: 2014-01-25; accepted: 2014-01-26

response[5]. In addition, the real-time data collected from the smart meters can improve the reliability of the distribution grid by avoiding line congestion and generation overloads[6]. The utility companies can also provide faster diagnosis of outage and dynamical electricity price thanks to the AMI. Hence, AMI has attracted great attention from many stakeholders, including utility companies, energy markets, regulators, etc. AMI technologies are rapidly overtaking the traditional meter reading technologies and millions of smart meters are equipped in the household all over the world. For example, there are already more than 4.7 million smart meters used for billing and other purposes in Ontario, Canada[7]. According to the American Institute for Electric Efficiency (IEE), approximately 36 million smart meters have been installed in the United State by May 2012, and additional 30 million smart meters will be deployed in the next three years[8].

However, rich information exchange and hierarchical semi-open network structure in AMI extend the attack surface for metering to entire public networks and introduce many vulnerabilities for cyber attacks[9, 10]. Among all the attacks to the AMI, energy theft in emerging economies has been a widespread practice, both in developing countries and developed countries. A World Bank report finds that up to 50% of electricity in developing countries is acquired via theft[11]. It is reported that each year over 6 billion dollars are lost due to the energy theft in the United States alone[12]. In 2009, the FBI reported a wide and organized energy-theft attempt that may have cost up to 400 million dollars annually to a utility following an AMI deployment[13]. In Canada, BC Hydro reports $100 million in losses every year[14]. Utility companies in India and Brazil incur losses around $4.5 billion and $5 billion due to electricity theft, respectively[15, 16]. There is even a video which shows how to crack the meter and cut the electricity bill in half in Youtube[17]. As a result, energy-theft issue becomes one of the most important concerns which prohibit the development of AMI.

Due to the nature of non-technical loss during transmission of electrical energy, it is very difficult for the utility companies to detect and fight the people responsible for energy theft. The unique challenges for energy theft in AMI call for the development of effective detection techniques. However, so far, few studies have elaborated what have been achieved and what should be done for these challenges. As a result, we are motivated to investigate energy-theft issue in AMI, which is of critical importance to the design of AMI information networks and has been considered as one of the highest priorities for the smart grid design. In this paper, we provide a state-of-the-art survey of existing energy-theft detection schemes in AMI.

2 System Model and Security Requirements

In this section, we present the system model and identify security requirements for AMI.

2.1 System model

The advanced metering infrastructure is a hierarchical structure. As shown in Fig. 1, AMI is comprised of a number of different networks communicating with each

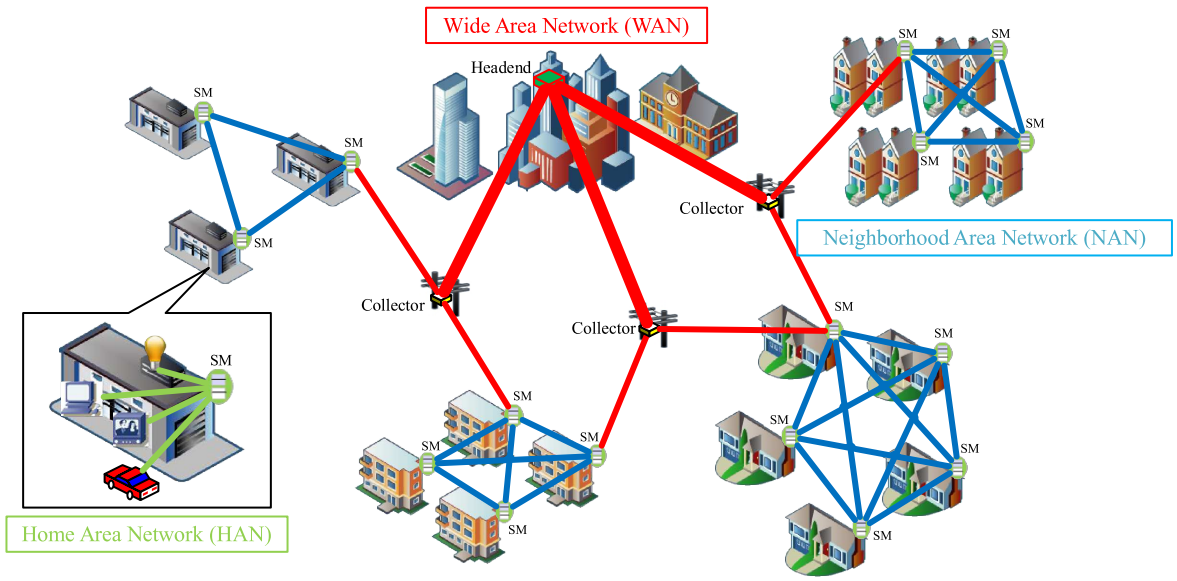

Fig. 1 A simple AMI architecture.

other, and these networks are described as follows:

- Home Area Network (HAN): The home area network is a kind of local area network with smart meter as its core. Household appliances can connect to the smart meter through wireless channel, e.g., ZigBee, which conveniently enables people to monitor and control the use of household appliances and make proper and economical usage plans.
- Neighborhood Area Network (NAN): The neighborhood area network is a network which is comprised of neighboring smart meters. A collector in NAN takes charge of the aggregation of metering data from smart meters, and the popular WiFi technology is suggested for NAN. Certainly, other technologies such as WiMAX and 3G/4G cellular can also be used for NAN communication.
- Wide Area Network (WAN): The wide area network serves as a connection of collectors in NAN and headends in the utility control center. Since millions of metering data are transferred in the WAN, the requirements of both bandwidth and reliability of the network are extremely high. As a result, the main communication technology suggested in WAN is optic fiber, although microwave and cellular are also considered for WAN as optional technologies.

The metering data continuously generated by smart meter can be used by various grid stakeholders to offer efficient services as follows:

- *Customers* can know exactly how much electricity they have consumed at any time and adjust their electricity consumption according to the dynamic electricity price;
- *Grid operators* can make smooth operation of the power system based on the real-time metering data;
- *Energy providers* can estimate the mid-term power consumption according the aggregated data;
- *Billing companies* need precise power consumption data to implement flexible electricity price model;
- *Third part value added services* can make electricity usage suggestion by analysing the customer's consumption profile;
- *Governmental agencies* need to access the data to make relevant laws.

2.2 Security requirements

Obviously, different stakeholders in AMI may have their own security requirements. For example, the customers care about their privacy information and regular electricity usage; while the utility companies aim to provide stable energy supply and prevent the customers from energy theft. In general, those sensitive objects that need to be protected in AMI can be classified as follows:

- Smart meter data: The data collected from the smart meters should not be accessed by any unauthorized entities;
- Control data: The control command should be received and implemented by the smart meters correctly and completely;
- Bill information: The electricity price and bill paid for the utility company should not be manipulated by unauthorized entities;
- Customer's personal information: The information includes customer's credit card information, daily electricity usage profile, and so on.

Based on the above sensitive objectives, security requirements for AMI can be classified as follows:

- *Confidentiality*: Sensitive information should only be accessed by authorized entities;
- *Integrity*: Data transmitted in the AMI must be authentic and correctly reflect the source data without any unauthorized manipulation;
- *Availability*: Data in AMI should be accessible by authorized entities whenever they need the data;
- *Non-repudiation*: The entities cannot deny receiving anything, such as renewed electricity price, that they have received; and cannot clarify that they have sent some data, e.g., electricity amount they have consumed, which they actually do not send;
- *Privacy*: The entities cannot infer any private information from the published metering data.

3 Threat Model

3.1 Attacker model

There are different kinds of attackers with various purposes to violate AMI. Analysis of the attackers provides better insights into their attack techniques. Generally speaking, attackers in AMI can be classified as follows:

- *Curious eavesdroppers*: These attackers are only interested in the activities of their neighbors;
- *Greedy customers*: These attackers want to crack the AMI in order to steal electricity;
- *Malicious eavesdroppers*: These attackers collect metering data for some vicious purposes such as house breaking;
- *Swanky attackers*: These attackers only want to show

off their ability and wisdom of attack techniques;

- *Active attackers*: These attackers aim to launch large-scale terrorist attacks by compromising the whole power system;
- *Intrusive data management agencies*: These attackers want to collect customers' private information for marketing or economic purposes.

Specifically, there are three types of attackers who are motivated to commit energy theft[18]:

- Customers: Traditionally, customers have been the primary adversaries aiming to steal power. The means and motivation to tamper with analog meters is very much individual in nature. In developing countries, people commit energy theft due to their poor infrastructure, poverty, and irregularities in metering and distribution systems. In developed countries, people, who cultivate marijuana illegally, steal electricity to hide their overall electricity consumption to avoid police inspection and prosecution.
- Organized crime: The motivation in the case of organized crime is the monetization of energy theft. Because of the extended computing and network capabilities of AMI, the task of creating software and hardware tools to compromise smart meters can be offloaded from customers to professional hackers. Members of this group will leverage certain design aspects of AMI systems, such as the widespread use of the same password set over many meters, to greatly amplify the profit from cracking a single smart meter.
- Utility company insiders: In most work, utility company insiders are implicitly trusted to be honest in the case of analog meters and the same model applies for AMI. However, in order to avoid mis-operation or being attacked by malicious employees in utility companies, it is preferable that utility side systems enforce proper customer and group management to provide properties such as separation of duties.

3.2 Attack tree based threat model

3.2.1 Definition and structure of attack tree

The attack tree approach, which provides a formal and methodical way to describe the security of systems based on varying attacks, is proposed by Schneier[19]. The attack tree enumerates all potential actions that an attacker could utilize to gain access to the target system and each branch in the tree represents a set of intermediate steps which the attacker must take prior to gaining access to the target system. The attack behaviors against a system are represented in a tree structure, with the final desired goal as the root node and different ways to achieve that goal as child nodes. Each child node of the root becomes a sub-goal, child nodes of which are ways to achieve that sub-goal. If one of those nodes cannot be divided further, it becomes the leaf node. Otherwise, those nodes are treated as sub-goals separately and will be decomposed continually until all the events become leaf nodes.

According to the logical relationship among the nodes, there are two kinds of logic gate, called OR-gate and AND-gate in attack tree. The OR-gates are used to represent alternative attack methods, while the AND-gates are used to represent different steps toward achieving the same goal. The nodes, which are linked with an OR-gate, are OR nodes. Those nodes linked an AND-gate are AND nodes. The presentation of OR node and AND node is shown in Fig. 2, where Goal_0 is an AND node and Goal_1 is an OR node. In order to achieve the Goal_0, both of the sub-goal Goal_{01} and Goal_{02} must be achieved first. While the Goal_1 can be achieved as long as either Goal_{11} or Goal_{12} is achieved.

3.2.2 Attack tree for energy theft in AMI

We perform a top-down, stepwise refinement, and heuristic strategy to construct the attack tree for energy theft[20]. "Energy theft" is set as the attacker's overall goal. The procedure of attack tree construction for energy theft in AMI is described as follows:

- Define the attacker's overall goal "G: Energy Theft" in AMI.
- Decompose the goal G into sub-goals: Interrupt Measurement, Tamper Stored Demand, and Modify in Network. The attacker's purpose can be achieved if any of the three components is reached. This list might be extensive and more sub-goals could be added.
- Continue the step-wise decomposition until the task cannot be divided into smaller ones. The completed diagram of attacks and sub-attacks is called an attack tree, as shown in Fig. 3.

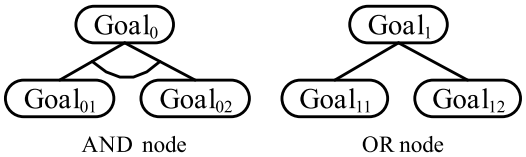

Fig. 2 AND node and OR node.

We go into the detail to illustrate the attack tree construction. There are three ways to achieve goal "energy theft" as shown in Fig. 3[18]:

- Interrupt measurement: This attack takes place before the smart meter makes a demand measurement and aims to prevent the smart meter from recording the consumed electricity. There are two ways, i.e., "disconnect meter" and "meter inversion", to commit this attack. In order not to be retrieved by the utility company, it is necessary to erase the logged events which indicate outage or reverse energy flow.
- Tamper stored demand: The attacker can also tamper the data stored in the smart meter to achieve energy theft, since the smart meter's behavior are controlled by these data (such as tariffs for TOU pricing, logs of both physical events and executed commands, recorded network command). The other way to tamper stored demand is erasing relevant records which are audit logs and the recorded total demand. These records can be accessed by administrative interfaces that need passwords.
- Modify in network: This attack directly injects the false data into communication between smart meters and utility company. The attacker needs to implement two steps to achieve this sub-goal: intercept communication and inject traffic. After successfully intercepting the links between smart meter and collector, a "man in the middle attack" or a "meter spoofing attack" can be used to send forged data and event logs.

Note that, the attack tree shown in Fig. 3 is only an example to capture the possible attacks launched by the attackers in AMI. As a general framework, an attack tree could accommodate more attack sub-tree by considering more attack strategies of the adversaries in practice. Recent research on the AMI security and privacy preservation[21-24] would also benefit the construction of the attack tree.

4 Techniques for Energy-Theft Detection

Different from other issues in smart grid, energy theft seems more intractable. This is partly because it involves human nature and economic considerations which are difficult to observe and control even by advanced measurement equipments. The detection and identification of frauds in power systems has been initially addressed with statistical techniques[25,26]. A variety of solutions to energy theft have been proposed recently due to the fast development of AMI in smart grid. In this section, we introduce our taxonomy of detection technique for energy theft in AMI. According to the detection strategies used in the literatures, we classify the exiting AMI energy-theft detection schemes into three categories, i.e., classification-based, state-based, and game theory-based ones, as shown in Fig. 4.

4.1 Classification-based detection technique

Among all the detection techniques for energy theft, classification-based detection technique, which is defined as the load profile classification of electricity consumption of a customer or a group of customers over a period of time, is one of the most widely used approaches. The basic procedure for classification-based energy-theft detection consists of seven parts: data acquisition, data preprocessing, feature extraction, classifier training and parameter optimization, classification, data postprocessing, and suspected customer list generation, as shown in Fig. 5. The main idea of this technique is to distinguish abnormal energy usage patterns from all energy usage patterns based on a testing dataset containing examples of the normal class and the attack class.

4.1.1 Classification-based schemes

Support Vector Machines (SVM) are widely utilized in the literatures[27-32] to classify the load profiles of customers for detection of energy-theft suspects. SVM

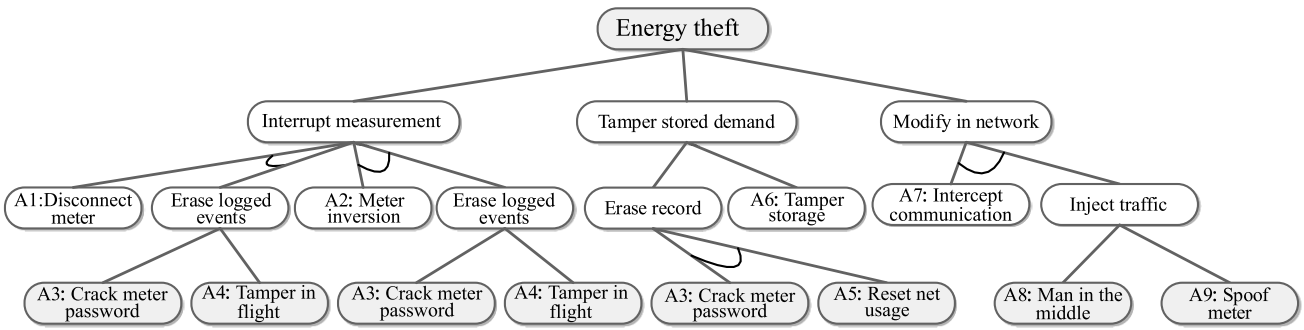

Fig. 3 Attack tree for energy theft.

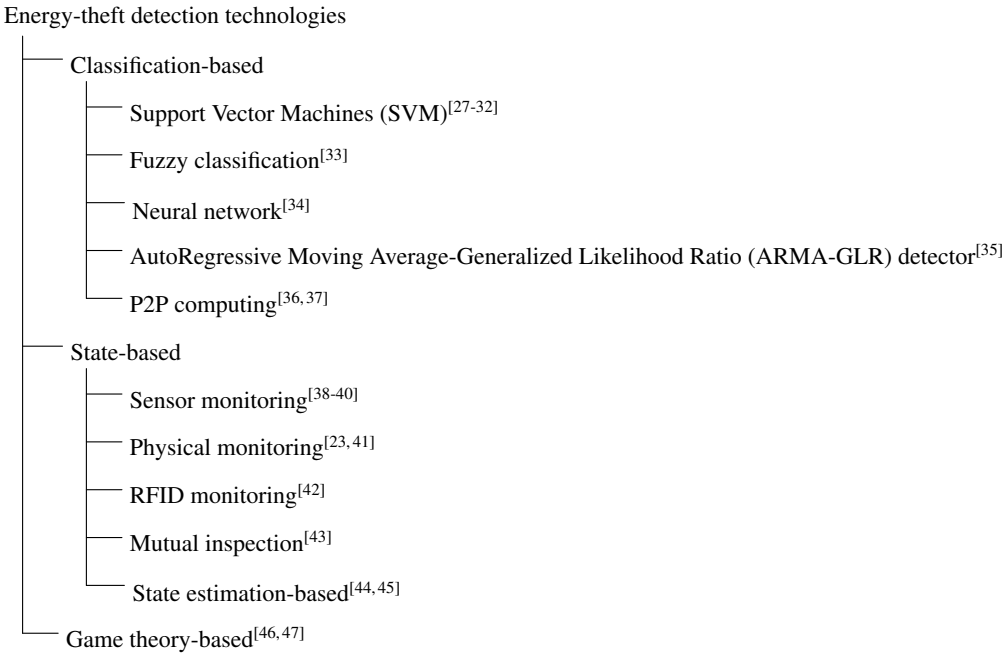

Fig. 4 Classification of energy-theft technique.

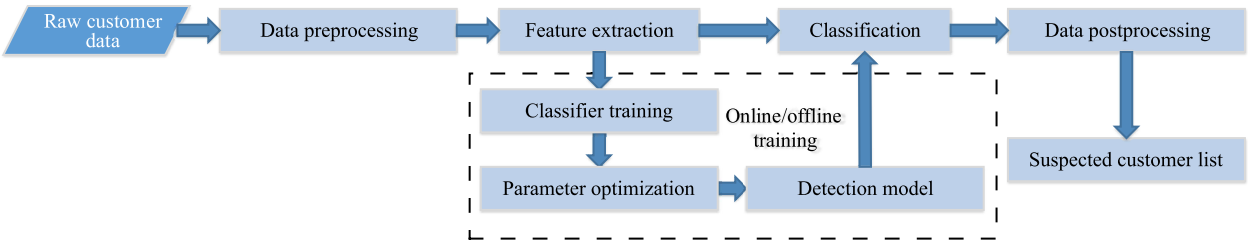

Fig. 5 Basic procedure for classification-based energy-theft detection.

was introduced by Vapnik in the late 1960s on the foundation of statistical learning theory[48, 49]. The main purpose of the (binary) SVM algorithm used for classification is to construct an optimal decision function $f(x)$ that accurately predicts unseen data into two classes, and minimizes the classification error using

$$f(x) = \mathrm{sgn}(g(x)) \tag{1}$$

where $g(x)$ is the decision boundary between the two classes. This is achieved by following the method of Structural Risk Minimization (SRM) principle[49]

$$R < \frac{t}{n} + \sqrt{\frac{h\left(\ln\left(\frac{2N}{h}\right)+1\right) - \ln(\eta/4)}{n}} \tag{2}$$

where R is the classification error expectation, t is the number of training errors, n is the number of training samples, and η is a confidence measure.

Specifically, Ref. [27] presents a hybrid approach towards Non-Technical Loss (NTL, most part of which is energy theft) analysis for electric utilities using Genetic Algorithm (GA) and SVM. The proposed approach uses customer load profile information to expose abnormal behavior that is known to be highly correlated with NTL activities. GA provides an increased convergence and globally optimized SVM hyper-parameters using a combination of random and prepopulated genomes.

Nagi et al. proposed an SVM-based approach[28] which uses customer load profile information and additional attributes to expose abnormal behavior that is known to be highly correlated with NTL activities. In order to improve the detection hitrate, they further present the inclusion of human knowledge and expertise into the SVM-based Fraud Detection Model (FDM) with the introduction of a Fuzzy Inference System (FIS), in the form of fuzzy *IF-THEN* rules[30].

Depuru et al. developed approximate energy consumption patterns of several customers based on customers' geographical location, load capacity, and their type[29]. A dataset representing the energy

consumption patterns of several customers is developed based on the historical data. In addition, they analyze the influence of energy theft on the power grid by comparing the electricity load on the grid with and without considering NTL in the analysis of consumption patterns. Then, the input training data is used to train the SVM model and the electricity consumption patterns of several customers are tested whenever needed. At last, this classification is done based on rules and the customers with suspicious energy consumption profiles are grouped and prosecuted.

In Ref. [31], a data encoding technique is proposed to reduce the complexity of the instantaneous energy consumption data for evaluation. After the encoding process, the data will be input to an SVM classification model that classifies customers into three categories: genuine customers, illegal consumers, and suspicious customers. Due to the huge amount of customers and high frequent data collection, how to efficiently detect the illegal customers from mass data is a big issue. In order to accelerate the processing speed, Depuru et al. investigated the possibility and role of High Performance Computing (HPC) algorithms in detection of illegal consumers[32]. An encoding procedure is designed and implemented to simplify and modify customer energy consumption data for quicker analysis without compromising the quality or uniqueness of the data. In addition, in Ref. [50] they implemented a Neural Network (NN) model and suggested a hierarchical model for enhanced estimation of the classification efficiency, if that data is classified using SVM.

Nizar et al. also investigated the efficiency of the SVM technique, Extreme Learning Machine (ELM) and its online sequential ELM (OS-ELM) variant for identification of abnormal load behavior indicating energy theft based on a load-profile evaluation[51-53].

Besides the SVM technique, many other classification methods, such as fuzzy classification[33] and neural networks[34], are utilized to detect energy theft. dos Angelos et al. proposed a fuzzy computational technique for the classification of electricity consumption profiles[33]. This methodology is comprised of two steps. In the first step, a C-means-based fuzzy clustering is performed to find customers with similar consumption profiles. Afterwards, a fuzzy classification is performed using a fuzzy membership matrix and the Euclidean distance to the cluster centers. At last, the distance measures are normalized and ordered, yielding a unitary index score. Among the index scores, the potential fraud or customers with irregular patterns of consumption can be found with the highest scores.

Muniz et al. presented an intelligent system, which intends to increase the level of accuracy in the identification of irregularities among low tension customers[34]. The intelligent system is composed of two neural network ensembles. The proposed methodology is formed by two basic modules, one for filtering the database and another for actual classification of a consumer. Each module is composed by a committee with five neural networks, where each network has an output that classifies customers into two categories: irregular customers and normal customers. The evaluated model provides very good performance for low tension customers, greatly improving current fraud detection rate.

With the development of attack techniques, the previous work may be evaded by an advanced attackers. In order to derive a new general way of evaluating classifiers in such developing adversarial environments, Mashima and Cárdenas argued that instead of using a set of attack samples for evaluating classifiers, they need to find the worst possible attack for each classifier and evaluate the classifier by considering the costs of this worst-case attack[35]. A new metric is introduced to evaluate the classification accuracy of anomaly detectors. This new metric takes into some consideration of the fundamental problems in anomaly detection when applied to security problems: (1) the fact that attack examples in a dataset might not be representative of future attacks; (2) in many cases it is hard to get attack data for academic studies. As a result, they can avoid training and evaluating classifiers with imbalanced and unrepresentative datasets. Based on the threat model and metric, an ARMA-GLR detector is developed to detect the energy-theft behaviors.

Although some schemes have been proposed for the utility companies to detect energy theft in AMI, they all require customers to send their private information, e.g., load profiles or meter readings at certain times, to the utility companies, which invades customers' privacy and raises serious concerns about privacy, safety, etc. In order to investigate the energy-theft detection problem without violating the customers' privacy, Salinas et al. proposed three P2P computing algorithms[36, 37], which can identify the customers who are committing energy theft in AMI while preserving all customers'

privacy. In their scheme, the customers can be classified by solving a Linear System of Equations (LSE) for customers' "honesty coefficients" k. The "honesty coefficients" k can be calculated as follows:

Assume that there are n customer smart meters and a collector smart meter in the neighborhood area network; Define a sampling period denoted by SP; Let energy consumption recorded by customer $j(1 \leqslant j \leqslant n)$ and energy consumption recorded by the collector at time t_i be $p_{t_i,j}$ and $\overline{\mathcal{P}}_{t_i}$, respectively; Let the honesty coefficient be k_j for each customer j, where $k_j > 0$. After every sampling period, all the $n+1$ smart meters will record their energy consumption in the past sampling period and $k_j \cdot p_{t_i,j}$ gives the real energy consumption of customer j from time instant $t_i - \mathrm{SP}$ to time instant t_i. Since the sum of all customers' real energy consumption in the past sampling period must be equal to the total energy consumption of the neighborhood measured at collector at time t_i, we have

$$k_1 p_{t_i,1} + k_2 p_{t_i,2} + \cdots + k_n p_{t_i,n} = \overline{\mathcal{P}}_{t_i} \tag{3}$$

The objective is to obtain all the k_j. Obviously, (1) if $k_j = 1$, then customer j is honest and did not steal energy; (2) if $k_j > 1$, then customer j records less energy than what he/she consumes and hence is an energy thief; (3) if $0 < k_j < 1$, then customer j records more than what he/she consumes, which means that his/her smart meter may be malfunctioning. In particular, with n linear equations, there is an LSE as follows:

$$\begin{cases} k_1 p_{t_1,1} + k_2 p_{t_1,2} + \cdots + k_n p_{t_1,n} = \overline{\mathcal{P}}_{t_1}; \\ \vdots \\ k_1 p_{t_n,1} + k_2 p_{t_n,2} + \cdots + k_n p_{t_n,n} = \overline{\mathcal{P}}_{t_n} \end{cases} \tag{4}$$

which can also be formulated in matrix form:

$$\boldsymbol{Pk} = \overline{\boldsymbol{\mathcal{P}}} \tag{5}$$

Three P2P computing based algorithms, i.e., LU decomposition based approach, LUD with partial pivoting (LUDP) approach, and QR decomposition approach, are proposed to solve the linear system of equations presented in Eq. (5) while preserving the customers' privacy. Each smart meter can find its own honesty coefficient without knowing any of the other smart meters' recorded energy consumption data. The customers who commit energy theft can be detected with honesty coefficient $k > 1$.

4.1.2 Comparison of classification-based schemes

Table 1 shows the comparison results of classification-based energy-theft detection schemes. From Table 1, we can find out that the SVM technique is the most popular method to classify the customer usage patterns. The detection rate of most classification-based schemes is approximately 60%-70% and is not very high. False positive rate is an important metric which indicates how many legal customers are classified into illegal ones by mistake. However, only few schemes such as Ref. [35] provide the quantitative false positive rate. In addition, most classification-based schemes need fully access the customers' energy consumption data and cannot protect the customers' privacy, which may prohibit the promotion of classification-based energy-theft detection schemes.

4.2 State-based detection technique

Another common solution for energy-theft detection is state-based detection technique, which uses monitoring state to improve the detection rate. The monitoring state can be derived from wireless sensor networks[38-40,54], RFID[42], mutual inspection[43], AMI[55], etc.

Since wireless sensor networks are cheap and easy to implement[56], they are popular to assist detecting energy theft. McLaughlin et al. proposed an AMI Intrusion Detection System (AMIDS) that uses information fusion to combine the sensors and consumption data from a smart meter to more accurately detect energy theft[38,39]. AMIDS combines meter audit logs of physical and cyber events with

Table 1 Comparison of classification-based schemes.

Scheme	Technique	Detection rate (%)	False positive (%)	Privacy preservation
Ref. [27]	Genetic SVM	62	-	×
Ref. [28]	SVM	60	13.57	×
Ref. [29]	SVM	98.4	-	×
Ref. [30]	SVM and fuzzy inference system	72	13.57	×
Ref. [31]	Data encoding and SVM	76-92	-	×
Ref. [32]	SVM and high performance computing	92	-	×
Ref. [33]	Fuzzy clustering and classification	74.5	-	×
Ref. [34]	Neural networks ensembles	24.9-62	-	×
Ref. [35]	ARMA models	62	4.2	×
Refs. [36, 37]	P2P computing	100	-	✓

consumption data to more accurately model and detect theft-related behaviors.

In Ref. [40], the authors pointed out that physical attack to smart meters can be extended to a network attack by means of false data injection. They proposed a CONSUMER attack model that is formulated into one type of coin change problem, which minimizes the number of compromised meters without being revealed by maintaining a cumulative load at the aggregation point to which multiple households are connected in today's radial tree-like distribution network. A hybrid detection framework is developed to detect anomalous and malicious activities by incorporating their proposed grid sensor placement algorithm with observability analysis to increase the detection rate.

Depuru et al. proposed a conceptual design for controlling energy theft based on physical monitoring[23,41]. The proposed approach is a paradigm shift from the conventional method of identifying the illegal consumer, by physical observation of the distribution feeder or evaluation of load pattern of all customers. If the computed non-technical losses are more than 5% of the distributed energy, then the external control station will send a control signal to the Internal Control Station (ICS) of smart meter to break the electric supply to the genuine customers. In this process, primarily, the genuine customers are identified and are isolated from the electric grid, leaving the illegal consumers continue to draw energy from the grid. Then the harmonic generator is switched on for a few seconds to destroy the illegal electricity appliances and is switched off after that period just before the scheduled power cut for that neighborhood. This approach can detect the energy-theft behaviours which bypass the smart meter and destroy illegal electricity appliances. However, compromised smart meters cannot be detected and the genuine customers may be disgruntled due to the energy break in this scheme.

Khoo and Cheng proposed a system that implements Radio Frequency IDentification (RFID) technology to help the electricity supply company deal with its ammeter inventory management and prevent energy theft[42]. There are two parts in the proposed system: ammeter inventory management and ammeter verification control. The ammeter inventory management includes an RFID tag on each ammeter, RFID readers, the middleware, and the network with the Enterprise Resource Planning (ERP) system of the electricity supply company. The integrity of the RFID tag can be used to detect energy theft. In addition, the reader acquires the information transmitted from the tag and sends it to the company's ERP system through the network to determine whether it is the approved tag or a different one placed by electricity thieves. Although the RFID technology can be used to detect energy theft, the utility companies have to pay extra cost to install the system. In order to find out whether implementing RFID technology is beneficial for the utility company, cost-benefit theory is used to analyse different value changes caused by the proposed system. In the case study, the Return On Investment (ROI) of the proposed system is 1.24 and the value of the total cost-benefit is approximately \$ 14 444.

Xiao et al. argued that meter readings may not be trustworthy due to malicious behaviors (e.g., energy theft) or external attacks[43]. The root cause is that power providers have no means to obtain the reading value other than receiving it from the energy customers. To solve this issue, they presented a mutual inspection strategy, which enables non-repudiation on meter readings for smart grid. The goal of the proposed scheme is to discover problematic meters that report inaccurate reading values. There are only two roles in this scheme: smart meter MP (representing the provider reading) and smart meter MS (representing the subscriber reading). The power provider and the subscriber do not trust each other because the smart meters may be compromised or attacked. They designed a protocol to ensure that if the actual bill difference between two smart meters M_{P} and M_{S} exceeds threshold b_0, the trust relationship will break, and the service will be terminated immediately.

Bad data injection is one of most dangerous attacks in smart grid, as it may lead to energy theft and cause breakdown on the power generation. In Ref. [44], a state estimation based approach for distribution transformer load estimation is exploited to detect meter malfunction/tampering and provide quantitative evidences of Non-Technical Loss (NTL). The basic flow diagram of the proposed method is shown in Fig. 6. Following the state estimation results, an analysis of variance is used to create a suspect list of customers with metering problems and estimate the actual energy usage.

In order to detect more bad data injection and locate the bad data within a smaller area, an Adaptive Partitioning State Estimation (APSE) is proposed[45]. In this method, the power system is transformed to a

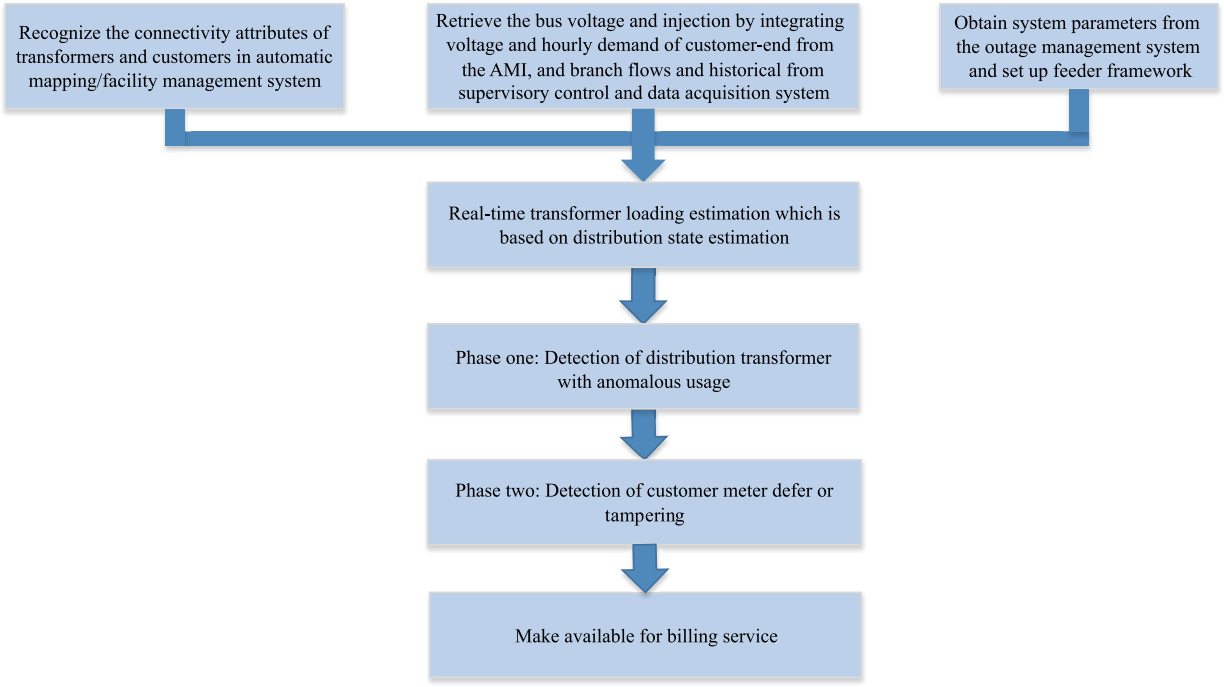

Fig. 6 Basic flow diagram of the proposed method in Ref. [44].

weighted undirected graph and divided into several subgraphs. Chi-squares test is used to detect bad data in each subgraphs. Since the threshold of subgraph is expected to be lower than that of the entire system, it will be more sensitive to detect the bad data. The APSE method is based on the proper partitioning graphs and can only detect the bad data on one transmission line. The method to detect multiple bad data should be studied.

4.3 Game theory-based detection technique

Game theory-based energy-theft detection schemes are proposed recently and provide a new perspective to solve the energy-theft issue[46, 47].

In Ref. [46], Amin et al. investigated incentive problems in electricity distribution when customer energy usage is imperfectly observable by the distributor. From the perspective of privacy protection, each customer has private information about the amount of his consumed electricity, and therefore distributor cannot observe customers' energy usage precisely, which results in non-technical energy losses, especially by energy theft. Although installing AMI can reduce such losses to a large extent, it requires substantial cost for distributor. Therefore, the authors presented the optimal investment and tariff strategy for distributor with rational customers from a game theory point of view. They also aimed to provide an effective suggestion to regulator how to decide an explicit targets for the allowable losses to remedy the problem of incentive misalignment.

Specifically, Amin et al.[46] modeled the energy theft and combat losses as a non-zero sum Stakelberg game with unregulated distributor, where the distributor acts as leader and the customers act as follower. The distributor can deploy AMIs to improve the monitoring and billing efficiency and thus reduce the total quantity non-technical losses due to theft. The efficiency of detecting stolen electricity increases with the corresponding investment of AMIs e. In addition, the electricity offers a non-linear tariff schedule T and selects output level Q. Customers, given the strategy of the distributor and the fine schedule for detected unbilled electricity, choose their consumption levels of billed and unbilled quantities to maximize their individual utility. The distributor, given the consumers' rational strategy, must select optimal e^*, T^*, and Q^* to maximize his profit. Based on these results, they further analyze a form of price cap regulation in which distributor faces an average revenue constraint. They conclude that such regulation can stimulate the total output level Q and AMI investment level e while maintaining the same marginal price schedule corresponding to the optimal tariff T.

Even through the optimal quantity of stolen electricity can be estimated by distributor, smart

customers are also possible to avoid detection using sophisticated strategies. Cárdenas et al.[47] formulated the problem of electricity theft detection as a game between the distributor and the electricity thief. For the electricity thief, they want to minimize the likehood of being detected to steal a predefined quantity of electricity. They can achieve it by changing their probability density function of electricity usage during the measurement period. On the other hand, the distributor wants to maximize the probability of energy-theft detection and determine the optimal investment incurred by AMIs installation. The Nash equilibrium of the game is found as a probability density function that attackers and defenders must choose in order to send AMI measurements.

In a word, although game theory-based detection technique is not mature yet, it provides a new perspective to recognize and address the energy theft.

4.4 Comparison

Thanks to the development of AMI, more and more technologies can be used to detect the energy theft. In this section, we present the comparison of the three categories of energy-theft detection schemes. The comparison result is shown in Table 2 from the point of view of methodology, detection rate, false positive, and cost.

Specifically, these energy-theft detection techniques have their own unique features:

- The classification-based detection schemes take advantage of the energy consumption data frequently collected from the AMI. Machine learning and data mining technologies are used to generate a good classifier based on some sample datasets. If the classifier and sample datasets are selected appropriately, most of the energy-theft behaviours can be detected with moderate cost. However, due to the zero-day attacks, there are many practical situations where we cannot obtain example of the attack class in advance. In addition, most schemes assume that the attackers are not adaptive and will not try to evade the detection mechanism, which results in missing some intelligent energy-theft. As a result, the detection rate can be affected dramatically in this case. To address this issue with the automated techniques, more frequent manual inspections by the power system engineers are needed to ensure that the learned profiles reflect the reality precisely.
- With the help of specific devices, the state-based detection schemes can improve the detection rate and reduce the false positive. The price which these schemes have to pay is that the monitoring devices need extra investment by the utility companies. The major cost of implementing the monitoring system includes device cost, software cost, system implementation cost, and increased operating/training cost. In addition, accurate detection of energy-theft efforts requires precise construction of the monitoring system and estimation of the involved parameter value. The system construction and parameter selection can be done either manually by the expert or automatically by the machine learning solutions. The drawbacks and advantages of both of those solutions should be considered.
- The game theory-based detection schemes provide a new perspective to solve the energy-theft. The problem of electricity theft detection is formulated as a game between the electric utility and the electricity thief. In the game, the goal of the electricity thief is to steal a predefined amount of electricity while minimizing the likelihood of being detected, while the utility companies want to maximize the probability of detection and the degree of operational cost it will incur for managing this anomaly detection mechanism. The game theory-based detection schemes may present a stable and reasonable (even if not optimal) solution to reduce the electricity losses as a result of energy theft. However, how to formulate all players' (regulator, distributor, and thieves) utility function and potential strategies is still a challenging work.

5 Challenges and Future Directions

5.1 Challenges

5.1.1 Privacy issue

In most current works, the utility companies have to obtain some of customers' private information such as

Table 2 Comparison of energy detection schemes.

Scheme	Methodology	Detection rate	False positive	Cost
Classification-based	Machine learning/Artificial intelligence	Medium	Medium	Medium
State-based	State monitoring by specific equipment	High	Low	High
Game theory-based	Game theory	Medium	Medium	Low

customers' load profiles or meter readings periodically in order to find the energy thieves. However, the disclosure of such information would violate customers' privacy and raise concerns about privacy. Customers worry about their private information to be referred from the frequently collected monitoring information. In particular, customers' private information may be sold to the interested third-parties, such as insurance companies and marketing companies. Even worse, criminals may utilize such private information to commit crimes. For instance, robbers may analyze the energy consumption pattern of potential victims to deduce their daily behavior. They can even know whether there is anyone in the house or if a robbery alarm has been set at their target location. Many researchers have realized how high resolution electricity consumption information can be used to reconstruct many intimate details of a customer's daily life and invade his/her privacy, and thus call for state legislators and public utility commissions to address this new privacy threat. Therefore, energy-theft detection and customers' privacy seem to be two conflicting problems. How to detect energy theft while preserving customers' privacy is a challenging issue. Unfortunately, there is a lack of research on privacy-preserving energy-theft detection in AMI currently.

5.1.2 Secure data collection

Current energy network hardware in un-controlled environments relies on physical security for protections. However, such mechanisms are not sufficient if smart meters are connected to open communication networks. Therefore, additional protection mechanisms are necessary. As software solutions are in principle vulnerable to active attacks, worms, viruses, etc., hardware security mechanisms in AMI should be considered[57].

5.1.3 Data storage and processing cost

Due to the frequent collection and the huge amount of customers, the scale of metering data becomes bigger and bigger. The metering data in smart grid are surging from 10 780 TB in 2010 to over 75 200 TB in 2015[58], which is far beyond the control center's data management capability. How to efficiently storage and process the massive metering data is also a challenging issue.

5.2 Future directions

5.2.1 Privacy preservation

Privacy issue is one of the most important concerns which prohibit the development of AMI. Failure to address privacy issue in the AMI will cause the AMI not be accepted by regulators and customers. Designing an energy-theft detection scheme without violating the privacy of customers is very meaningful. Privacy issue in AMI may be addressed by adopting newly anonymous communication technologies and cryptographic algorithm such as homomorphic encryption. Current approaches to anonymize traffic in general networks will cause overhead problems or delay issues. How to improve the efficiency of anonymous communication is a research direction.

5.2.2 Trusted computing

Trusted Computing (TC)[59] can offer a hardware root of trust providing certain security functionalities for smart meters. Trusted computing is defined by Trusted Computing Group (TCG) which aims to provide trust to the computing environment. Trust means that components of the system always work as implemented. Any mismatch of the configuration can be detected promptly by the Trusted Platform Module (TPM), which is mostly realized as a hardware chip hard-wired to the computer platform. The TCG defines three different roots of trust: The Core Root of Trust for Measurement (CRTM), the Root of Trust for Reporting (RTR), and the Root of Trust for Storage (RTS). The AMI development can benefit a lot from trusted computing technologies in various ways. The most obvious application of trusted computing in the AMI is to protect smart meters installed in physically insecure environments from manipulation.

5.2.3 Cloud computing and big data

Outsourcing data to cloud servers is a promising approach to relieve the control center in AMI from the burden of a large amount of data storage and maintenance. In this approach, energy customers can store their energy consumption data on cloud servers and execute computation and queries using the servers' computational capabilities[60]. Nevertheless, cloud servers might be untrustworthy, and may intentionally share sensitive data with the third parties for commercial purposes. Therefore, data confidentiality is important in financial audit for AMI in smart grid in cloud computing environment[61].

In general, utility companies can gather more data from many devices and they can leverage big data analytics by cloud computing to obtain better situational awareness of the health of their system. How to effectively leverage the cloud computing techniques to assist the energy-theft detection is a research direction.

6 Conclusions

Energy-theft detection is a classic and difficult problem in power grid. With the development of advanced metering infrastructure in smart grid, more complicated situation in energy theft has emerged and many new technologies are adopted to try to solve this problem. In this paper, we have investigated the system model and security requirements of AMI in smart grid and present an attack tree based threat model for AMI. We further categorize the energy-theft detection schemes in AMI and introduce the main idea of each individual scheme. Finally, we discuss the challenging issues in energy-theft detection and provide some research directions. In the future, the smart grid requires more accurate and efficient energy-theft detection designed specifically for advanced metering infrastructure, making energy-theft detection a very fruitful and challenging research area.

Acknowledgements

This work was supported by China Scholarship Council, the National Natural Science Foundation of China (Nos. 61170261 and 61202369), and NSERC, Canada.

References

[1] R. Jiang, R. Lu, C. Lai, J. Luo, and X. Shen, Robust group key management with revocation and collusion resistance for scada in smart grid, in *Proc. IEEE Globe Communication Conference (Globecom)*, 2013, pp. 824-829.

[2] 2012 India blackouts, http://en.wikipedia.org/wiki/Indiablackout, 2013.

[3] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications, *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621-1631, 2012.

[4] M. Wen, R. Lu, J. Lei, H. Li, X. Liang, and X. Shen, SESA: An efficient searchable encryption scheme for auction in emerging smart grid marketing, *Security and Communication Networks*, vol. 7, no. 1, pp. 234-244, 2014.

[5] H. Li, X. Liang, R. Lu, X. Lin, H. Yang, and X. Shen, EPPDR: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid, *IEEE Transactions on Parallel and Distributed Systems*, vol. PP, no. 99, pp. 1-10, 2013.

[6] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, UDP: Usage-based dynamic pricing with privacy preservation for smart grid, *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 141-150, 2013.

[7] Independent Electricity System Operator (IESO) Office of the Information and Privacy Commissioner Ontario, Canada, Building privacy into ontario's smart meter data management system: A control framework, Tech. Rep., http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1183, May 07, 2012.

[8] IEE Report, Utility-scale smart meter deployments, plans, & proposals, http://www.edisonfoundation.net/iee/Documents/IEE_SmartMeterRollouts_0512.pdf, 2012.

[9] Z. M. Fadlullah, N. Kato, R. Lu, X. Shen, and Y. Nozaki, Toward secure targeted broadcast in smart grid, *IEEE Communications Magazine*, vol. 50, no. 5, pp. 150-156, 2012.

[10] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, A lightweight message authentication scheme for smart grid communications, *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 675-685, 2011.

[11] P. Antmann, Reducing technical and non-technical losses in the power sector, Background paper for the WBG Energy Strategy, Tech. Rep., Washington, DC, USA: The World Bank, 2009.

[12] P. McDaniel and S. McLaughlin, Security and privacy challenges in the smart grid, *IEEE Security & Privacy*, vol. 7, no. 3, pp. 75-77, 2009.

[13] B. Krebs, FBI: Smart meter hacks likely to spread, http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/, 2012.

[14] CBC News, Electricity theft by B.C. grow-ops costs $100m a year, http://www.cbc.ca/news/canada/british-columbia/electricity-theft-by-b-c-grow-ops-costs-100m-a-year-1.969837, 2010.

[15] Ministry of power, India, Overview of power distribution, Tech. Rep., http://www.powermin.nic.in, 2013.

[16] Federal Court of Audit, Operational audit report held in national agency of electrical energy, aneel, Brazil, Tech. Rep., No. TC 025.619/2007-2, 2007.

[17] Electric meter hack! how to cut your electricity bill in half! http://www.youtube.com/watch?v=YVA8M2YV_QW8, 2013.

[18] S. McLaughlin, D. Podkuiko, and P. McDaniel, Energy theft in the advanced metering infrastructure, in *Proc. the 4th International Conference on Critical Information Infrastructures Security*, Springer, 2010, pp. 176-187.

[19] B. Schneier, Attack trees, *Dr. Dobbs Journal*, vol. 24, no. 12, pp. 21-29, 1999.

[20] R. Jiang, J. Luo, and X. Wang, An attack tree based risk assessment for location privacy in wireless sensor networks, in *Proc. 8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM)*, 2012, pp. 1-4.

[21] F. Skopik and Z. Ma, Attack vectors to metering data in smart grids under security constraints, in *Proc. IEEE 36th Annual Computer Software and Applications Conference Workshops*, 2012, pp. 134-139.

[22] A. Hahn and M. Govindarasu, Cyber attack exposure evaluation framework for the smart grid, *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 835-843, 2011.

[23] S. 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, 2011.

[24] D. Grochocki, J. H. Huh, R. Berthier, R. Bobba, W. H. Sanders, A. A. Cárdenas, and J. G. Jetcheva, AMI threats, intrusion detection requirements and deployment recommendations, in *Proc. 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, 2012, pp. 395-400.

[25] R. J. Bolton and D. J. Hand, Statistical fraud detection: A review, *Statistical Science*, vol. 17, no. 3, pp. 235-249, 2002.

[26] Y. Kou, C.-T. Lu, S. Sirwongwattana, and Y.-P. Huang, Survey of fraud detection techniques, in *Proc. IEEE International Conference on Networking, Sensing and Control*, 2004, vol. 2, pp. 749-754.

[27] J. Nagi, K. Yap, S. Tiong, S. Ahmed, and A. Mohammad, Detection of abnormalities and electricity theft using genetic support vector machines, in *Proc. TENCON 2008-2008 IEEE Region 10 Conference*, 2008, pp. 1-6.

[28] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed, and M. Mohamad, Nontechnical loss detection for metered customers in power utility using support vector machines, *IEEE Transactions on Power Delivery*, vol. 25, no. 2, pp. 1162-1171, 2010.

[29] S. Depuru, L. Wang, and V. Devabhaktuni, Support vector machine based data classification for detection of electricity theft, in *Proc. 2011 IEEE/PES Power Systems Conference and Exposition (PSCE)*, 2011, pp. 1-8.

[30] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed, and F. Nagi, Improving SVM-based nontechnical loss detection in power utility using the fuzzy inference system, *IEEE Transactions on Power Delivery*, vol. 26, no. 2, pp. 1284-1285, 2011.

[31] S. Depuru, L. Wang, and V. Devabhaktuni, Enhanced encoding technique for identifying abnormal energy usage pattern, in *Proc. IEEE North American Power Symposium (NAPS)*, 2012, pp. 1-6.

[32] S. Depuru, L. Wang, V. Devabhaktuni, and R. C. Green, High performance computing for detection of electricity theft, *International Journal of Electrical Power & Energy Systems*, vol. 47, pp. 21-30, 2013.

[33] E. W. S. dos Angelos, O. R. Saavedra, O. A. Cortes, and A. N. de Souza, Detection and identification of abnormalities in customer consumptions in power distribution systems, *IEEE Transactions on Power Delivery*, vol. 26, no. 4, pp. 2436-2442, 2011.

[34] C. Muniz, K. Figueiredo, M. Vellasco, G. Chavez, and M. Pacheco, Irregularity detection on low tension electric installations by neural network ensembles, in *Proc. IEEE International Joint Conference on Neural Networks*, 2009, pp. 2176-2182.

[35] D. Mashima and A. A. Cárdenas, Evaluating electricity theft detectors in smart grid networks, in *Research in Attacks, Intrusions, and Defenses*, Springer, 2012, pp. 210-229.

[36] S. Salinas, M. Li, and P. Li, Privacy-preserving energy theft detection in smart grids, in *Proc. 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, 2012, pp. 605-613.

[37] S. Salinas, M. Li, and P. Li, Privacy-preserving energy theft detection in smart grids: A P2P computing approach, *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 257-267, 2013.

[38] S. McLaughlin, B. Holbert, S. Zonouz, and R. Berthier, AMIDS: A multi-sensor energy theft detection framework for advanced metering infrastructures, in *Proc. IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, 2012, pp. 354-359.

[39] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, A multi-sensor energy theft detection framework for advanced metering infrastructures, *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1319-1330, 2013.

[40] C.-H. Lo and N. Ansari, CONSUMER: A novel hybrid intrusion detection system for distribution networks in smart grid, *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 1, pp. 33-44, 2013.

[41] S. Depuru, L. Wang, V. Devabhaktuni, and N. Gudi, Measures and setbacks for controlling electricity theft, in *Proc. IEEE North American Power Symposium (NAPS)*, 2010, pp. 1-8.

[42] B. Khoo and Y. Cheng, Using RFID for anti-theft in a chinese electrical supply company: A cost-benefit analysis, in *Proc. IEEE Wireless Telecommunications Symposium (WTS)*, 2011, pp. 1-6.

[43] Z. Xiao, Y. Xiao, and D. H.-C. Du, Non-repudiation in neighborhood area networks for smart grid, *IEEE Communications Magazine*, vol. 51, no. 1, pp. 18-26, 2013.

[44] S.-C. Huang, Y.-L. Lo, and C.-N. Lu, Non-technical loss detection using state estimation and analysis of variance, *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 2959-2966, 2013.

[45] T. Liu, Y. Gu, D. Wang, Y. Gui, and X. Guan, A novel method to detect bad data injection attack in smart grid, in *Proc. IEEE INFOCOM*, 2013, pp. 3423-3428.

[46] S. Amin, G. A. Schwartz, and H. Tembine, Incentives and security in electricity distribution networks, in *Decision and Game Theory for Security*, Springer, 2012, pp. 264-280.

[47] A. A. Cárdenas, S. Amin, G. Schwartz, R. Dong, and S. Sastry, A game theory model for electricity theft detection and privacy-aware control in AMI systems, in *Proc. IEEE 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2012, pp. 1830-1837.

[48] M. A. Hearst, S. Dumais, E. Osman, J. Platt, and B. Scholkopf, Support vector machines, *IEEE Intelligent Systems and their Applications*, vol. 13, no. 4, pp. 18-28, 1998.

[49] V. N. Vapnik, *Statistical Learning Theory*. Wiley, 1998.

[50] S. Depuru, L. Wang, V. Devabhaktuni, and P. Nelapati, A hybrid neural network model and encoding technique

for enhanced classification of energy consumption data, in *Proc. IEEE Power and Energy Society General Meeting*, 2011, pp. 1-8.

[51] A. Nizar, Z. Dong, J. Zhao, and P. Zhang, A data mining based NTL analysis method, in *Proc. IEEE Power Engineering Society General Meeting*, 2007, pp. 1-8.

[52] A. Nizar, Z. Dong, and Y. Wang, Power utility nontechnical loss analysis with extreme learning machine method, *IEEE Transactions on Power Systems*, vol. 23, no. 3, pp. 946-955, 2008.

[53] A. Nizar and Z. Dong, Identification and detection of electricity customer behaviour irregularities, in *Proc. IEEE/PES Power Systems Conference and Exposition*, 2009, pp. 1-10.

[54] R. V. P. Yerra, A. K. Bharathi, P. Rajalakshmi, and U. Desai, WSN based power monitoring in smart grids, in *Proc. IEEE Seventh International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, 2011, pp. 401-406.

[55] P. Kadurek, J. Blom, J. Cobben, and W. Kling, Theft detection and smart metering practices and expectations in the Netherlands, in *Proc. 2010 IEEE/PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe)*, 2010, pp. 1-6.

[56] R. Jiang, J. Luo, and X. Wang, HRKT: A hierarchical route key tree based group key management for wireless sensor networks, *KSII Transaction on Internet and Information Systems*, vol. 7, no. 8, pp. 1754-1773, 2013.

[57] C. Shen, H. Zhang, D. Feng, Z. Cao, and J. Huang, Survey of information security, *Science in China Series F: Information Sciences*, vol. 50, no. 3, pp. 273-298, 2007.

[58] R. Yu, Y. Zhang, S. Gjessing, C. Yuen, S. Xie, and M. Guizani, Cognitive radio based hierarchical communications infrastructure for smart grid, *IEEE Network*, vol. 25, no. 5, pp. 6-14, 2011.

[59] C. Mitchell, *Trusted Computing*. Iet, 2005.

[60] C. Wang, Q. Wang, K. Ren, and W. Lou, Privacy-preserving public auditing for data storage security in cloud computing, in *Proc. IEEE INFOCOM*, 2010, pp. 1-9.

[61] M. Wen, R. Lu, K. Zhang, J. Lei, X. Liang, and X. Shen, PaRQ: A privacy-preserving range query scheme over encrypted metering data for smart grid, *IEEE Transaction on Emerging Topics in Computing*, vol. 1, no. 1, pp. 178-191, 2013.

Rong Jiang received the BS and MS degrees in 2007 and 2009, respectively, from National University of Defense Technology, Changsha, China, where he is currently pursuing the PhD degree. He was a joint PhD student at Broadband Communications Research (BBCR) Group, Department of Electrical and Computer Engineering, University of Waterloo, Canada in 2013. His research interests include wireless sensor networks security and privacy preservation, cloud computing, and smart grid.

Rongxing Lu received the PhD degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2006, and the PhD degree in electrical and computer engineering from the University of Waterloo, Canada, in 2012. He is currently an assistant professor in the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore. His current research interests include wireless network security, applied cryptography, and trusted computing.

Ye Wang received the BS degree from Harbin Engineering University, Harbin, China, in 2007, and the MS and PhD degrees from Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, China, in 2009 and 2013. He is currently a post-dotoral fellow in the Communication Engineering Research Center, Harbin Institute of Technology Shenzhen Graduate School. His research interests include game theory, cognitive radio, and smart grid.

Jun Luo received the BS degree from Wuhan University, Wuhan, China, in 1984, and the MS degree from National University of Defense Technology, Changsha, China, in 1989. He is currently a professor in the School of Computer Science, National University of Defense Technology. His research interests include operating system, cloud computing, information security, and wireless sensor networking.

Changxiang Shen received the B S degree from Zhejiang University, China in 1965. He is currently a professor and PhD supervisor. He is an academician of Chinese Academy of Engineering and a senior member of China Computer Federation. His research interests include information security, trusted computing, computer architecture, and cloud computing security.

Xuemin (Sherman) Shen received the BS degree from Dalian Maritime University, Dalian, China, and the MS and PhD degrees from Rutgers University, NJ, USA, in 1982, 1987, and 1990, respectively, all in electrical engineering. He is a professor and University Research Chair with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He was the Associate Chair for Graduate Studies from 2004 to 2008. His current research interests include resource management in interconnected wireless/wired networks, wireless network security, wireless body area networks, vehicular ad hoc, and sensor networks. He is the co-author or editor of six books, and has published more than 600 papers and book chapters in wireless communications and networks, control, and filtering. He served as the Technical Program Committee Chair for IEEE VTC in 2010, the Symposia Chair for IEEE ICC in 2010, the Tutorial Chair for IEEE VTC in 2011, and IEEE ICC in 2008, the Technical Program Committee Chair for IEEE Globecom in 2007, the General Co-Chair for Chinacom in 2007 and QShine in 2006, the Chair for IEEE Communications Society Technical Committee on Wireless Communications, and P2P Communications and Networking. He serves/served as the Editor-in-Chief for the IEEE Network, Peer-to-Peer Networking and Application, and IET Communications, a Founding Area Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, COMPUTER NETWORKS, and ACM/Wireless Networks, and the Guest Editor for the IEEE JSAC, IEEE Wireless Communications, the IEEE Communications Magazine, and ACM Mobile Networks and Applications. He received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award from the University of Waterloo in 2004, 2007, and 2010, the Premiers Research Excellence Award from the Province of Ontario, Canada, in 2003, and the Distinguished Performance Award from the Faculty of Engineering, University of Waterloo, in 2002 and 2007. He is a registered Professional Engineer of Ontario, Canada. He is a fellow of the Engineering Institute of Canada and the Canadian Academy of Engineering. He is a Distinguished Lecturer of IEEE Vehicular Technology Society and Communications Society. He has been a Guest Professor of Tsinghua University, Shanghai Jiao Tong University, Zhejiang University, Beijing Jiao Tong University, and Northeast University.