Non-Repudiation in Neighborhood Area Networks for Smart Grid

Zhifeng Xiao and Yang Xiao, University of Alabama
David Hung-Chang Du, University of Minnesota

ABSTRACT

Lack of non-repudiation is a major barrier of building a trustworthy smart grid. In current power systems, bills are generated based on the amount of service consumed by residential or commercial users. However, meter readings may not be trustworthy due to malicious behavior (e.g., energy theft) or external attacks. The root cause is that power providers have no means to obtain the reading value other than receiving it from the users. To resolve this issue, we present a mutual inspection strategy, which enables non-repudiation on meter readings for smart grid. The goal of our scheme is to discover problematic meters that report inaccurate reading values.

INTRODUCTION

Smart grid [1–3] has become one of the research hotspots in recent years. A smart grid not only delivers electricity from the power provider to subscribers, but it also enables two-way digital communications to gather, distribute, and act on information about the behavior of all participants. The goal of replacing traditional power grids with smart grid is to save energy, reduce cost, and increase reliability and transparency.

The traditional power grid does not possess the property of non-repudiation. Back in the 20th century, power providers employed meter readers to do door-to-door meter readings. There are many drawbacks of artificial meter reading, such as high time cost and labor cost, low accuracy, and error-prone reading. Additionally, there is no evidence pointing to a cheater who falsifies or manipulates the reading data. For instance, if a meter is tampered with and the reading value is less than the actual amount, the power company is unable to detect the theft behavior. Advanced metering infrastructure (AMI) is being developed to tackle some of these issues. The goal of AMI is to provide automatic measurement and transmission of meter readings. However, AMI cannot ensure non-repudiation of meter readings as well. The root problem lies in the method of collecting the reading values of smart meters. In order to acquire the service amount of each subscriber, the power provider must rely on the digital communication network for data transmission. Since the reading value is generated on the subscriber end, an attacker or energy thief still has multiple means to tamper with it. The most common methods [4] of energy theft include metering tampering, meter switching, wire partial bypass of the meter inside the meter enclosure, complete bypass of the meter from the low-voltage grid, and direct connection to the primary voltage grid with a pirate distribution transformer. The original reading may be altered before it is sent to the provider. Since the smart meter may be the only source for the power provider to acquire the service amount, whether the meter reading is accurate or falsified, the power provider has no means to prove the correctness of the meter's reading report.

A straightforward solution is to physically secure the smart meter. Other people who attempt to break the box may trigger an alarm or leave an undeniable trace on the box. However, this does not solve the root problem: the service amount can only be obtained via the meter on the subscriber end, and the power provider cannot obtain this information directly through the power grid.

In this article, we address non-repudiation in terms of accountability, which assigns responsibility to each smart meter, whether it is accurate or not. We adopt a mutual inspection strategy to ensure non-repudiation. Following this strategy, we install two smart meters with one electric wire connecting the subscriber and the provider. This means that for each individual wire, there is one smart meter on each end; one represents the subscriber's reading, and the other represents the provider's reading. In a normal situation, although these two meters measure the same wire, their readings are not the same due to:

- Power loss during power transfer
- Measuring errors caused by communication delays and synchronization issues
- Dynamic factors caused by the environment (e.g., temperature)

Additionally, the remarkable difference between readings can be caused by a meter that is com-

0163-6804/13/$25.00 © 2013 IEEE

promised or out of order. In our strategy, the readings are exchanged between the power provider and the subscriber in order to resolve a dispute (if there is any). If the dispute lies in a range that is acceptable for both ends, the service continues to be delivered; however, if the dispute exceeds a certain threshold, the service will be terminated and further investigation will begin. In the mutual inspection strategy, two distrusted parties can inspect each other to realize non-repudiation in smart grid.

Mutual inspection requires that the quantity of smart meters is doubled, and this increase seems to incur high expense. However, the estimated annual loss due to energy theft is $6 billion dollars in the United States [4]. There were around 22 million smart meters deployed in the United States by the end of 2011. To fully adopt mutual inspection, the number of smart meters will be doubled. The market price of a smart meter is around $100. Therefore, the hardware cost will be less than $3 billion. In addition, the cost of deployment and maintenance should be considered. If the strategy saves the $6 billion loss or at least the majority, the saved money in one year may entirely cover the investment. The return on investment is considerable because the country can save up to $6 billion per year in the future.

This article is based on our preliminary work presented at a conference [12], and we have made substantial new contributions. The contributions of this article are listed below. We formalize the non-repudiation problem in smart grid. Based on our knowledge, this is the first time the non-repudiation problem in smart grid has been addressed. We adopt mutual inspection and design a protocol to realize non-repudiation in smart grid so that any misbehavior and malicious operation that compromises power readings will eventually be detected. Mutual inspection can stop all theft behavior relying on meter compromising and wire bypassing. We consider three kinds of structure: centralized structure, point-to-point (P2P) structure, and hybrid structure, and discuss how mutual inspection is applied to the three environments. We conduct both numeric analysis and simulation to evaluate the proposed scheme.

The rest of this article is structured as follows. Related works are reviewed in the next section. Then some background knowledge of the smart grid, smart grid architecture, and the billing mechanism are introduced. Furthermore, the problem statement and mutual inspection protocol are presented. Finally, the evaluation and conclusions are included.

Related Work

Security has been a significant concern for smart grid [5–7, 11–13]. Smart grids have leveraged many hardware and software technologies, such as smart meters, sensors, and advanced communication networks. Although these techniques bring many exciting features to smart grid, they also introduce new vulnerabilities that may be exploited by adversaries. We briefly introduce the smart grid security issues in four aspects.

Trust

A smart grid is a heterogeneous environment containing various devices, such as smart meters, appliances, collectors, and backend servers. A trust relation is expected before real data can be exchanged and processed. The issue discussed in this article falls into this category.

Privacy

Smart metering and load management is incorporated into smart grid. However, since the subscriber's power consumption pattern is revealed to the provider, the customer's privacy, especially lifestyle, may be disclosed. For instance, it is easy to tell whether the customer is at home or not. With careful analysis, it is even possible to figure out which appliance is in use. This kind of information may be used by criminals.

Device Security

Devices in smart grid should be protected physically and cryptographically. A recent study showed how a smart meter was compromised in a security incident, which incurs the loss of cipher keys and memory data.

Security Management

The scale of smart grid keeps increasing; thus, more and more devices will join in. Handling the security management issues such as key generation, update, and revoke is a challenge.

In this article, our focus is on non-repudiation, which is the foundation of a trustworthy smart grid. Without non-repudiation, energy theft is hard to control at root. McLaughlin *et al.* [6] demonstrate that not only is energy theft possible in the AMI system, but the AMI commodity devices can also be taken advantage of by adversaries in order to perform a number of attacks. There are three classes of attacks depending on when and where meter reading is manipulated. They include:

- While it is recorded
- While it is at rest in the meter
- As it is in flight across the network

Today's energy theft detection models generally fall into two categories [7]: peer comparison and characteristic analysis. Peer comparison models group residential and commercial customers with similar homes and businesses in similar geographical and environmental settings. If a customer's actual usage deviates from the expected usage, it may indicate incorrectness of energy metering. Characteristic analysis, on the other hand, attempts to model the consumption pattern for an account; thus, any anomalies not following the pattern may be indicative of energy theft. In this area, machine learning techniques (e.g., support vector machines [SVMs] [8]) can be leveraged for building fundamental patterns and detecting anomalies. However, these analytical methods cannot be used as evidence of energy theft, because a deviation from expected normal usage can be caused by multiple reasons other than energy theft. For example, one needs to consider the trend of energy usage in the entire area or other legitimate changes. In this article, our method differs from the early analytical methods in that we aim to

Smart metering and load management is incorporated into smart grid. However, since the subscriber's power consumption pattern is revealed to the provider, the customer's privacy, especially the living style, may be disclosed. For instance, it is easy to tell whether the customer is at home or not.

The billing mechanism in the future will change accordingly. Based on how utility companies and independent users choose to participate in the smart grid system, there are three structure options to build a neighborhood smart grid: centralized, P2P, and hybrid.

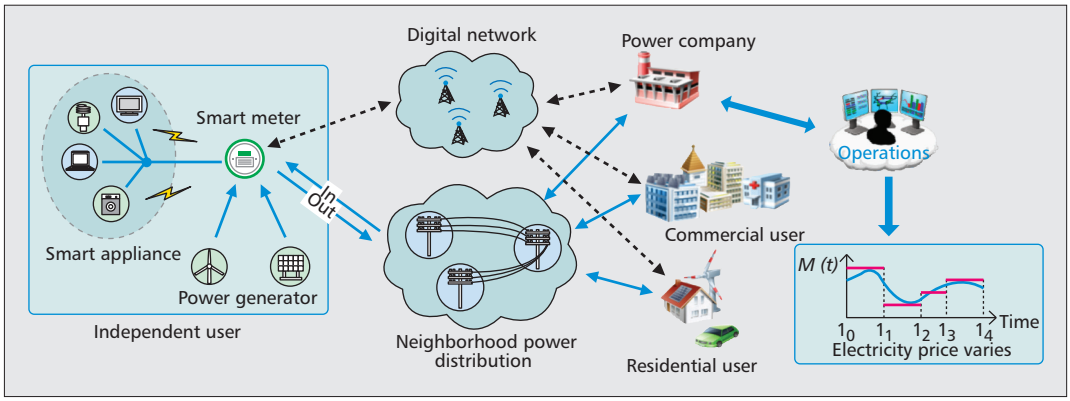

Figure 1. *Overview of smart grid in a neighborhood area network.*

isolate the compromised meter(s) with undeniable evidence, which can be used as proof of misbehavior.

Accountability has been a longstanding concern for trustworthy computer systems [9], and it has recently been elevated to a first class design principle for dependable networked systems [10]. In general, accountability implies an entity's capacity to identify a party that is responsible for specific events with undeniable evidence. Regarding smart grid, accountability has not been thoroughly studied. Liu *et al.* [11] have addressed accountability as a solution to build trustworthy smart grid in a home area, where:

- The smart meter and the smart appliance group are able to verify the correctness of each other.
- A power company can prove the correctness of the smart meter.

In this article, we focus on smart grid in neighborhood areas where the power company and independent users do not trust each other. We adopt mutual inspection to realize non-repudiation in smart grid so that any misbehavior or malicious operation that compromises power readings will eventually be detected; this also helps prevent massive financial loss.

Smart Grid in NAN

As shown in Fig. 1, there are two basic parties in a neighborhood smart grid: the power company and independent users. An independent user may own a power generator; therefore, it can play the roles of both a power provider and a power subscriber. All entities are connected by generating two types of flows: electricity flow and information flow.

Pricing

Theoretically, price is changing in real time in smart grid (as shown in Fig. 1). The price is mainly determined by the variation of power supply and demand in a certain area. In real world scenarios, however, the price will usually be discredited. For example, the power company may divide a day into several time segments, each of which corresponds to a certain price. In the future, the length of a time segment may be significantly reduced to adopt a fine-grained pricing scheme.

Smart Grid Structure and Billing

The Cisco brief [13] mentioned a few security challenges in smart grid, and one of them is "integration of distributed energy suppliers such as independent power producers, of renewable energy generation, and of distributed energy resources." This means that independent power producers play a more important role in smart grid. Moreover, the billing mechanism in the future will change accordingly. Based on how utility companies and independent users choose to participate in the smart grid system, there are three structure options to build a neighborhood smart grid.

Centralized Structure — In the centralized structure, the utility company is the major power provider, and it also determines the market price $M(t)$. Every subscriber follows this price. Let $E_i(t)$ denote the amount of power consumed by user i, and let $S_i(t)$ be the power generated and sold by user i. The billing function $B_i(t_0, \Delta t)$ gives the total bill of subscriber i during the time interval $[t_0, t_0, t + \Delta t]$. In the centralized structure,

$$B_i(t_0,\Delta t)=\int_{t_0}^{t_0+\Delta t} M(t)\cdot\big(E_i(t)-S_i(t)\big)dt.$$

Since $M(t)$, $E_i(t)$, and $S_i(t)$ are functions of t, the bill can be calculated in terms of the integral on $M(t) \cdot (E_i(t) - S_i(t))$.

P2P Structure — In the pure P2P structured smart grid, every independent user acts as both a power provider and a subscriber, and the users can determine their own prices. Let $m_i(t)$ denote the price function given by user i, and let $E_{i,j}(t)$ denote the service amount user i bought from provider j. If there are n other users from which user i bought power during time window $[t_0, t_0 + \Delta t]$, the billing function is given as

$$B_i(t_0,\Delta t)=\int_{t_0}^{t_0+\Delta t}\left(\sum_{j=1}^{n} m_j(t)\cdot E_{i,j}(t)-m_i(t)\cdot S_i(t)\right)dt.$$

Therefore, the amount that user i pays to its provider j is given as

$$B_{i,j}(t_0,\Delta t)=\int_{t_0}^{t_0+\Delta t}\big(m_j(t)\cdot E_{i,j}(t)-m_i(t)\cdot S_{i,j}(t)\big)dt.$$

Hybrid Structure — In the hybrid structure, the power company is still the major provider and determines the market price; however, independent users can set their own price as well. Therefore, it is straightforward to give the billing function as

$$B_i(t_0,\Delta t)=\int_{t_0}^{t_0+\Delta t}\left(M(t)\cdot E_i(t)+\sum_{j=1}^{n} m_j(t)\cdot E_{i,j}(t) -m_i(t)\cdot S_i(t)\right)dt$$

In this situation, the total bill of user i should be the sum of the amount paid to the power company (the first term in parentheses) and the amount paid to other independent users (the second term), minus the money that user i makes from other users. If we treat the power company as another independent user, the hybrid structure becomes a special form of the P2P structure.

Problem Statement

Terms and Definitions

Based on the mutual inspection strategy, for a subscriber S there are two meters, M_S and M_P, to record its service amount at both ends of the wire connecting the subscriber S and the provider P.

Definition 1: The power demand function $P(t)$ gives the power service amount of a subscriber at time t. Obviously, $P(t)$ depends on the condition of all power appliances. A concrete model of $P(t)$ will be given in the next section.

Definition 2: The power loss function $l(P)$ defines the power line loss during transmission given that the power demand is P. According to electricity knowledge, we have $l(P(t)) = (P(t)^2 \cdot R)/V^2$, where R is the wire resistance and V is the transmission voltage. R is dependent on the cable material, cable length, and environment factors like temperature. In this article, we rule out the variability of resistance and consider R as a constant. Therefore, l is a function of power demand P of a subscriber.

Definition 3: The bill difference (i.e., dispute) function $b(t_0, \Delta t)$ gives the bill difference (starting from t_0) between two end smart meters connected by the same power line during a time window Δt. Let $M(t)$ denote the price function, which can be either the market price or the independent power seller's price. Therefore, $b(t_0, \Delta t)$ can be given as

$$\frac{R}{V^2}\int_{t_0}^{t_0+\Delta t} M(t)\cdot P(t)^2\,dt+\alpha(t_0,\Delta t).$$

The first term is the bill due to power loss; this is considered the main part of bill differences. However, there are other factors affecting the bill difference, including measuring error, communication delay, and synchronization issue. Therefore, before we can have further information to express these factors, we use $\alpha(t_0, \Delta t)$ to represent all of them.

Problem Formulation

In order to resolve the dispute, M_s and M_p exchange billing data constantly; however, there should be a proper time window that determines how frequently they exchange. If the time window is too large (e.g., once per month/day/hour), the power provider undertakes a higher risk because there may be large disputes accumulated before the provider can recognize them. On the contrary, if the time window is very small, the power provider can be notified before it suffers more losses. Unfortunately, there is a high communication overhead that will undermine the system performance. Therefore, we need to determine an optimal time window in order to maximize the time window without bringing an unbearable overhead. The Time Window Maximization (TWM) problem is formulized as follows:

Time Window Maximization (TWM) problem: Given t_0, maximize Δt s.t. $b(t_0, \Delta t) \le b_0$; $H(\Delta t) \ge H_0$, in which b_0 is a predefined dispute threshold. $H(\Delta t)$ is the throughput function that is constrained by a threshold H_0.

Solution Sketch

The TWM problem aims at maximizing Δt with two constraints. An intuitive solution to this problem is that the maximal Δt can be determined by the intersection of the solution sets for the two constraints. Suppose that constraints $b(t_0, \Delta t) \le b_0$ and $H(\Delta t) \le H_0$ have solution sets W_1 and W_2. If $W_1 \cap W_2 = W_* = \varnothing$, no optimal Δt can be found. This means that b_0, or H_0 should be adjusted in order to generate a satisfactory Δt. If $W_1 \cap W_2 = W_* \uparrow \varnothing$, an optimal Δt can be obtained. According to the opposite influences of Δt on bill difference and throughput, we can determine that an optimal Δt can always be found if $W_1 \cap W_2 \uparrow \varnothing$.

Design of Accountable Neighborhood Smart Grid

Protocol Overview

We 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.

There are only two roles in this protocol. They are smart meter M_P (representing the provider reading) and smart meter M_S (representing the subscriber reading). The power provider and the subscriber do not trust each other because the smart meters may be compromised or attacked.

Protocol Detail

We assume that one subscriber can only have one power provider during a certain amount of time aside from the electricity produced by home power generators. We also assume that the AMI system has already employed public-key infrastructure (PKI) to establish the authentication framework. Under this assumption, there is a certificate authority (CA) acting as a trusted third party.

When a new independent user k joins the smart grid, it follows the protocol until the electricity is cut off or the service is shut down due to the detection of anomaly. The protocol can be described as follows:

There is a high communication overhead that will undermine the system performance. Therefore, we need to determine an optimal time window in order to maximize the time window without bringing an unbearable overhead.

Current AMI requires smart meters report reading value at regular intervals; our scheme keeps it but the message quantity doubled since we adopt a request-response process. Every time a new meter joins, message overhead increases, but the overall complexity is linear.

• User k joins the neighborhood smart grid system by registering itself at the CA and then starts to produce electricity with a power generator. User k needs to request a certificate from the CA for authentication purposes.

• If the self-produced electricity cannot meet the power demand, user k becomes a power subscriber that will find a power provider in the neighborhood and will then negotiate a bill difference threshold b_0 with its power provider (i.e., power company in centralized architecture, other independent users who have extra electricity to sell in P2P/hybrid architecture). Once the provider is determined, an authentication process will be initiated by the subscriber via a handshake protocol. The outcome of the authentication process is that:

– The two parties are authenticated to each other.

– A secret key is securely distributed between the subscriber and the provider for the future use of encryption/hashing.

For example, SSL protocol establishes a secure channel between two parties to ensure multiple security properties.

• If the self-produced electricity is more than the power demand, user k becomes a power provider because it has extra power to sell. The action to be taken depends on the type of architecture:

– In centralized architecture, user k follows the price made by the utility company. It only needs to send extra electricity back to the power grid. This can mean that the power company will buy the electricity from some home users and then sell to other ones.

– In P2P/hybrid architecture, user k broadcasts its own price to the entire neighborhood smart grid. If there is a request to subscribe, user k will start delivering power service after authentication by the subscriber.

• Both the power provider and the subscriber will maintain a service record in which each entry is a four-tuple e_i = <type, ts_i, $R_k(ts_i)$, partner>. Type indicates the role of the record owner (i.e., provider/subscriber); ts_i is the timestamp of entry i; $R_k(ts_i)$is the incoming/outgoing reading measured by the meter k at ts_i; partner indicates the other side of the service. Based on the record, the provider and the subscriber are able to compute the bill during a time window. Depending on the structure of the neighborhood smart grid, the billing function differs. Given two entries e_i and e_j, in order to calculate the bill, there is one condition: the two fields "type" and "partner" do not change in e_i, e_j and the entries between e_i and e_j. This condition ensures that service is continuously delivered during ts_i and ts_j. We let $b(e_i, e_j)$ denote the bill.

• After the bill is computed, a billing message will be constructed as follows: $M_{bill} = b(e_i, e_j)|e_i|e_j|\ nonce|MAC_{bill}$. $b(e_i, e_j)$ represents the bill; e_i and e_j are used to recompute the bill for verification purposes; a nonce value is adopted to prevent replay attack. A message authentication code (i.e., MAC_{bill}) that covers the previous three fields is attached so that the receiver can check the integrity of the bill message. Then M_{bill} will be encrypted and transmitted through a secure channel. We let the bill exchange process follow a request-response pattern. When it is time to exchange a bill message, the provider sends a request message that contains its own bill. Upon receiving it, the subscriber first computes its bill based on e_i and e_j in the request message, and then sends a respond bill message back to the provider.

• We studied two approaches to exchange the billing information. First, two meters can follow a constant time window so that bill messages are exchanged periodically. Second, the time window is optimized in terms of system overhead (i.e., the throughput in this case). We have formalized the TWM problem. To adopt the optimized time window strategy, a meter needs to compute the time window length every time it receives a bill message.

• After the bill message is received, user k is able to calculate the actual bill difference; this is the result of the subscriber's bill after subtracting the provider's bill. Possible cases are discussed below:

– If the actual bill difference is larger than 0 and less than the threshold b_0, the difference is minor and acceptable.

– If the difference exceeds b_0, there are four possibilities: first, the subscriber manipulates the bill data and attempts to pay less than the amount it should; second, the provider manipulates the bill data and attempts to charge more; third, both the provider and the subscriber misbehave; fourth, both the provider and the subscriber have no problem, and the cause is from outside (e.g., environment factors). The last case is the source of a false alarm, which is evaluated in later sections. No matter what the reason may be, the service is terminated, and further investigations are initiated.

– However, if the actual difference is less than 0, there must be some problems with the meters because the provider is unable to provide less energy than the amount the subscriber has consumed. A report is filed based on the incident.

The mutual inspection scheme is scalable and easy to implement. The scheme can easily be tailored to fit the three kinds of structures discussed earlier because by nature the power service, no matter which structure it adopts, involves two parties (i.e., the provider and the subscriber), while mutual inspection targets to provide accountability between the two parties. In addition, the implementation is feasible. The smart meter software needs to update to accommodate the protocol, and the update can be done remotely through the Internet. The scheme is also scalable in terms of message overhead. Current AMI requires smart meters to report reading values at regular intervals; our scheme keeps this, but the message quantity is doubled since we adopt a request-response process. Every time a new meter joins, message overhead increases, but the overall complexity is linear.

Security Analysis

Confidentiality — Confidentiality can be provided by both symmetric and asymmetric encryption. During authentication, data is encrypted by

the public key of the other end. Once authentication is accomplished, a session key is negotiated to establish a secure channel through which every message is encrypted.

Integrity — Integrity is ensured by the MAC attached to each bill message. In addition, the original entries are included in the message in case the other side needs the bill to be recomputed. In the real world, MAC may use various hash functions (e.g., SHA-1) as its implementation.

Accountability — Accountability can be ensured when:
- Misbehavior can be detected.
- Any misbehavior can be traced back to a responsible entity.

In our context, it means that when excessive bill difference is detected, which party (provider or subscriber) misbehaved should be able to be determined. Currently, the mutual inspection strategy can only achieve the first goal, leaving the second goal to further manual investigation.

Spoofing Attack — A user's identity is bound with its public key certificate, which is signed and issued by a CA. If the CA is trustworthy, certificates cannot be forged. Therefore, it is unlikely to impersonate other users without breaking the CA.

Replay Attack — Replay attack can be prevented by adopting a unique nonce value, which is by nature a pseudo random number. Each nonce is only for one-time use, making replay attack ineffective.

Man-in-the-Middle Attack — A man-in-the-middle (MITM) attack can be performed when the attacker can take over the communication without being detected by the two ends. In our protocol, an MITM attacker has no means to break into the communication in the process of both handshake (authentication) and bill exchange. Since data is encrypted by public key (during handshake) or session key (during bill exchange), an attacker can only capture the cipher text rather than become a middle man by manipulating the message.

EVALUATION

In this section, we attempt to make the problem more concrete with stronger assumptions in order to evaluate the method.

POWER DEMAND FUNCTION

To define the power demand function, we assume that each smart appliance has two modes, on and off. Once an appliance is on, the capacity is fixed. Power demand function $P(t)$ gives the service amount of a subscriber at time t. Obviously, $P(t)$ depends on the modes of all power appliances. $P(t)$ can be calculated as

$$P(t) = \sum_{k=1}^{K} d_k(t) \cdot p_k,$$

where $d_k(t) = 1$ if appliance k is on and 0 otherwise, and p_k stands for the capacity of appliance k. There are K appliances in total. Based on the assumption, we know that $P(t)$ is a piecewise function of time t.

BILL DIFFERENCE FUNCTION

The bill difference function defines how time window Δt affects the bill difference. The price function $M(t)$ could be either a continuous function or a piecewise function, which means that there are two cases.

Case 1 — $M(t)$ is a continuous function. In this case, $M(t)$ is a continuous function, and $P(t)$, as we have assumed, is a piecewise function. The bill difference function can be transformed to become

$$b(t_0, \Delta t) = \frac{R}{V^2}\left(\sum_{i=0}^{u}\left(P(t_i)^2 \int_{t_i}^{t_{i+1}} M(t)dt\right)\right) + \alpha(t_0, \Delta t),$$

in which $t_{u+1} = t_0 + \Delta t$. This means there are $(u + 1)$ segments of $P(_t)$ in total between $[t_0, \Delta t + t_0]$. Since $M(t)$ is continuous, it is difficult to solve constraint $b(t_0, \Delta t) \le b_0$. However, we can adopt Newton's method to find an approximate solution.

Case 2 — $M(t)$ is a piecewise function. In this case, both $M(t)$ and $P(t)$ are piecewise functions. Then the previous equation can be transformed to

$$b(t_0, \Delta t) = \frac{R}{V^2}\left(\sum_{i=0}^{q}\left(\begin{matrix}(t_{i+1} - t_i)\cdot \\ M(t_i)\cdot P(t_i)^2\end{matrix}\right)\right) + \alpha(t_0, \Delta t),$$

in which $t_{q+1} = t_0 + \Delta t$, meaning that there are $(q + 1)$ segments in total between $[t_0, \Delta t + t_0]$. Since both $M(t)$ and $P(t)$ are known piecewise functions, we can solve constraint $b(t_0, \Delta t) \le b_0$ to find an optimal Δt.

NUMERICAL EVALUATION

In order to get a better understanding of the performance, in this subsection, we assume that there is no limitation on the data transmission rate, but we also assume that the smart grid employs IEEE 802.11 as the communication standard. Based on [14], there is a throughput limit in IEEE 802.11 standards. We only consider ideal one-hop and one-way communication, in which only two nodes are involved; one is the sender, the other is the receiver. In our problem, the actual data traffic depends on the time window Δt. When Δt is large, the data traffic is very low and vice versa. In the extreme case, when Δt approaches 0, the data traffic can achieve full speed.

Based on physics, wire resistance R can be calculated by $R = (\rho \cdot L)/S$, where ρ stands for the resistivity, L is the wire length, and S represents the cross sectional area. Given that most power wires are made of copper, we let $\rho = 3.06 \times 10^{-7}$ (Ωm). Wire length varies. As a case study, we let $L = 100$ (m), and $S = 1.6 \times 10^{-5}$ (m^2). Based on the parameter setting, we have $R = 1.9125$ (Ω). The voltage is 110 V, which is the standard voltage in North America.

In our protocol, an MITM attacker has no means to break into the communication in the process of both handshake and bill exchange. Since data is encrypted by public key or session key, an attacker can only capture the cipher text rather than become a middle man by manipulating the message.

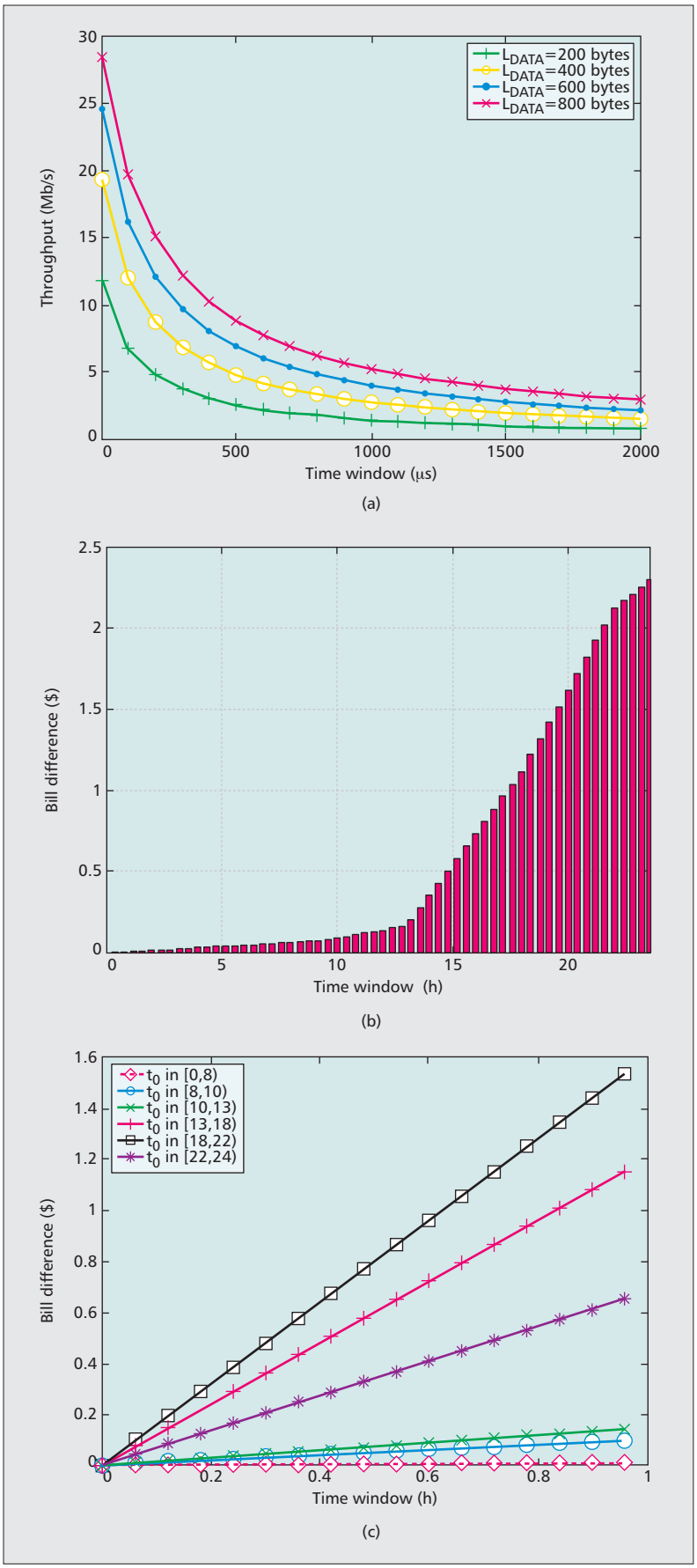

Figure 2. *Numeric results: a) time window and throughput; b) time window and bill difference; c) time window and bill difference when* t_0 *lies in different intervals.*

Since we have assumed that $P(t)$ is a piecewise function, a test case function of $P(t)$ is given as follows: $P(t) = 500$ (w) when t is in [0, 8); $P(t) = 700$ when t is in [8,13); $P(t) = 2000$ when t is in [13, 22); $P(t) = 1300$ when t is in [22, 24). In this case, we consider $M(t)$ as a piecewise function (the case of $M(t)$ being continuous has similar results), and repeat every 24 hours. We let $M(t)$ be $M(t) = 0.2$ ($kwh) when t is in [0, 10); $M(t) = 0.3$ when t is in [10, 18); $M(t) = 0.4$ when t is in [18, 24).

If we let $t_0 = 0$, the bill difference function can be determined. In this specific case, we describe the following bill difference function as follows: $b(0, \Delta t) = 7.9\times\ \Delta t$ when t is in [0,8); $b(0, \Delta t) = 15.484 \times\ \Delta t - 60.672$ when t is in [8,10); $b(0, \Delta t) = 23.226\times\ \Delta t - 138.092$ when t is in [10,13); $b(0, \Delta t) = 189.6 \times\ \Delta t - 2301$ when t is in [13,18); $b(0, \Delta t) = 252.8 \times\ \Delta t - 3438.6$ when t is in [18, 22); $b(0, \Delta t) = 106.8 \times\ \Delta t - 226.73$ when t is in [22, 24).

Figure 2a shows that when the time window Δt increases from 0 to 500 μs, the throughput keeps decreasing. This is reasonable since the larger the time window is, the lower the communication frequency is, and this decreases the throughput. We can also observe that when the time window is fixed, throughput increases when the payload data becomes larger.

Figure 2b shows how time window Δt influences the bill difference. In our case, when $t_0 = 0$, the bill difference will become larger with the increase of Δt. Based on this result, we can determine the maximum Δt with a given bill difference threshold.

Figure 2c shows how different t_0 changes the relation between the time window and bill difference. We can observe that t_0 is a key factor for determining the actual bill difference because both power price and user demand are constantly changing. Once any of those changes, the calculation for bill difference also changes. This illustrates that for every time a dispute is resolved, a new Δt should be computed based on the current status.

Simulation Results

The two strategies being compared are constant time window (TW) and optimized TW. The former strategy adopts a constant TW between two dispute resolving processes. The latter, which is suggested in our scheme, attempts to optimize the TW to reduce the system overhead. The mutual inspection approach is applicable to the smart grid regardless of its architecture model. Therefore, in the simulation, we only focus on one smart grid structure (i.e., the P2P architecture) as the evaluation environment.

The goal of this simulation is twofold:

- To show the effectiveness of the mutual inspection scheme on non-repudiation and accountability
- To show that the optimized TW reduces system overhead and improves system performance

We pick four metrics to evaluate the scheme. The first is P-Accountability [15]. This is a metric to evaluate the degree of accountability. In this context, we define P-Accountability = (detected malicious meter #)/(total malicious

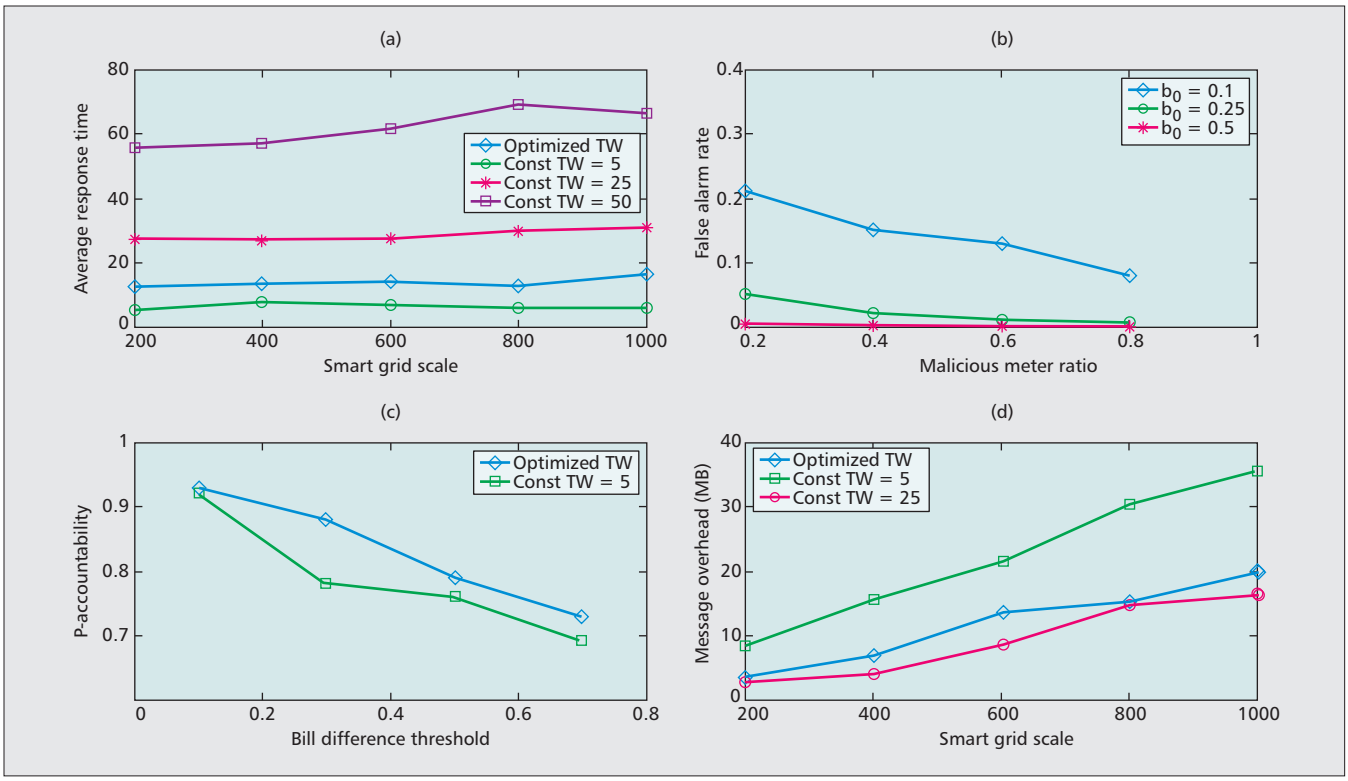

Figure 3. *Simulation results.*

meter #). The second is average detection time, which measures how much time is needed to detect a malicious meter after it becomes malicious. We believe that it is important to know how promptly the system responds to misbehavior. The third is the false alarm rate since it could be regular power loss or other accidental causes that trigger the alarm. The simulation attempts to figure out how the dispute threshold would affect the false alarm. Intuitively, the higher the threshold is set, the lower the false alarm rate will be because variance of regular disputes will be covered. On the other hand, P-Accountability will be reduced as well since the average detection time will be prolonged. The fourth is system overhead, which is the message overhead in this context.

The parameters we use are:

- The smart grid scale (i.e., the number of independent users)
- The ratio of malicious meters
- The dispute threshold

In this simulation, we assume that each independent user has a fully functional smart meter that is able to measure all input/output electricity amounts in real time.

Figure 3a describes the way the smart grid scale affects average detection time. In this experiment, we set the malicious node ratio to 0.1 and dispute threshold to $1. We have compared the optimized Δt method with the constant TW method (i.e., the TW is fixed at 5 ms, 25 ms, and 50 ms, respectively). From this result, we observe that the smart grid scale does not affect the average detection time no matther what TW method we adopt. This is because the mutual inspection mechanism enables the provider and the subscriber to inspect each other. Additionally, it shows that the optimized TW method can achieve fair performance in terms of average detection time. Although it is not as good as the case where the TW is fixed at 5, we can show that it generates less overhead in later experiments.

Figure 3b shows how a malicious meter ratio relates to the false alarm rate. A false alarm means that a user can mistakenly judge another user as the cause of an anomaly. A false alarm is possible because the dispute threshold cannot completely satisfy every case. For example, if the threshold is too high, real malicious meters may escape detection; if, however, the threshold is too low, the bill difference due to regular variance could be detected, and this is where the false alarm originates. From this figure, we can observe that the threshold and the malicious meter ratio are two key factors that affect the false alarm rate. When the malicious meter ratio is higher, there are fewer false alarms. Furthermore, we have discussed how the threshold affects the false alarm rate.

P-Accountability (shown in Fig. 3c) is defined as the ratio of the number of detected malicious meters and the number of all malicious meters. The major parameter that affects P-Accountability is the bill difference threshold. We can observe that when the threshold increases from 0.1 to 0.7 (in dollar units), P-Accountabilty decreases. This means that a higher threshold can allow some malicious meters to escape; this is similar to the former experiment. In nature, P-Accountability and false alarm partially oppose each other. They evaluate the system performance from two aspects.

In the experiment, we measured the message overhead as the metric to evaluate the optimized time window method and the constant time window method. It can be observed that the optimized time window method performs rather well when compared to the constant time window method.

Overhead is another performance issue. In the experiment, we measured the message overhead as the metric to evaluate the optimized and constant TW methods. It can be observed that the optimized TW method performs rather well when compared to the constant TW method. It introduces relatively low overhead while still maintaining low average detection time (Fig. 3d). This is the trade-off we have attempted to make.

Conclusions

In this article, we have proposed a mutual inspection strategy to enable non-repudiation and accountability in neighborhood smart grid. Our strategy is scalable and easy to implement. Evaluation results show that the mutual inspection can achieve decent performance when combined with the optimized time window method.

Acknowledgment

This work is supported in part by the U.S. National Science Foundation (NSF) under grant numbers CNS-0737325, CNS-0716211, CCF-0829827, and CNS- 1059265.

References

[1] H. Farhangi, "The Path of the Smart Grid," *IEEE Power and Energy Mag.*, vol. 8, no. 1, 2009, pp. 18–28.

[2] X. I. E. Kai *et al.*, "The Vision of Future Smart Grid," *Electric Power*, vol. 41, no. 6, 2008, pp. 19–22.

[3] M. Amin and B. F. Wollenberg, "Toward A Smart Grid: Power Delivery for the 21st Century," *IEEE Power and Energy Mag.*, vol. 3, no. 5, 2005, pp. 34–41.

[4] Accenture Inc., "Achieving High Performance With Theft Analytics — Leveraging Smart Grid Employments to Enhance Revenue Protection," 2011, http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Achieving-High-Performance-with-Theft-Analytics.pdf

[5] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," *IEEE Security & Privacy*, vol. 7, no. 3, 2009, pp. 75–77.

[6] S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy Theft in the Advanced Metering Infrastructure," Critical Information Infrastructures Security Lecture Notes in Computer Science, 2010, volume 6027/2010, 176-187, DOI: 10.1007/978-3-642- 14379-3_15

[7] M. Madrazo, "Today's Energy Theft Detection Models Help Protect Revenues While Enhancing Neighborhood Safety," http://www.pipelineandgasjournal.com/today's-energy-theft-detection-models-help-protect-revenues-while-enhancing-neighborhood-safety vol. 237, no. 7, July 2010.

[8] S.S.S.R. Depuru, L. Wang, and V. Devabhaktuni, "Support Vector Machine Based Data Classification for Detection of Electricity Theft," *Power Sys. Conf. and Expo.*, 2011.

[9] Dept. of Defense, "Trusted Computer System Evaluation Criteria," tech. rep. 5200.28-STD, 1985.

[10] A. R. Yumerefendi and J. S. Chase, "The Role of Accountability in Dependable Distributed Systems," *Proc. HotDep*, 2005.

[11] J. Liu, Y. Xiao, and J. Gao, "Accountability in Smart Grids," *IEEE Consumer Commun. and Networking Conf. 2011*, Smart Grids Special Session.

[12] Z. Xiao, Y. Xiao, and D. Du, "Building Accountable Smart Grids in Neighborhood Area Networks," *Proc. IEEE GLOBECOM 2011*.

[13] Cisco Smart Grid Security Solutions Brief, 2009 Cisco Systems, Inc. http://www.cisco.com/web/strategy/docs/energy/CiscoSmartGridSecurity_solutions_brief_c22-556936.pdf

[14] Y. Xiao and J. Rosdahl, "Throughput and Delay Limits of IEEE 802.11," *IEEE Commun. Letters*, vol. 6, 2002, pp. 355–57.

[15] Z. Xiao and Y. Xiao, "P-Accountable Networked Systems," *IEEE INFOCOM Commun. Wksps.*, 2010, pp. 1–5.

Biographies

ZHIFENG XIAO [S'11–12] (zxiao1@crimson.ua.edu) is a Ph.D. candidate in the Department of Computer Science at the University of Alabama. He received his Bachelor's degree in computer science from Shandong University, China, in 2008. His research interests are in design and analysis of secure distributed and Internet systems.

YANG XIAO [SM'04] (yangxiao@ieee.org) worked in industry as a medium access control architect involving IEEE 802.11 standard enhancement work before he joined academia. He is currently with the Department of Computer Science at the University of Alabama. He was a voting member of the IEEE 802.11 Working Group from 2001 to 2004. His research areas are security and communications/networks. He has published more than 200 refereed journal papers (including 50 IEEE/ACM transactions papers), and over 200 refereed conference papers and book chapters related to these research areas. He currently serves as Editor-in-Chief for *International Journal of Security and Networks* and *International Journal of Sensor Networks*.

DAVID H. C. DU [F'98] (du@cs.umn.edu) received his B.S. degree in mathematics from National Tsing-Hua University, Taiwan in 1974, and M.S. and Ph.D. degrees in computer science from the University of Washington, Seattle, in 1980 and 1981, respectively. He is currently the Qwest Chair Professor at the Computer Science and Engineering Department, University of Minnesota, Minneapolis. He served as a program director at the National Science Foundation from 2006 to 2008. His research interests include cyber security, sensor networks, multimedia computing, mass storage systems, high-speed networking, database design, and CAD for VLSI circuits. He has authored and co-authored more than 240 technical papers, including 110 referred journal publications in these research areas. He currently serves on the editorial boards of several journals. He has also served as Conference Chair and Program Committee Chair of several conferences in parallel processing, security, multimedia, networking, and database.