Achieving Accountability in Smart Grid

Jing Liu, Yang Xiao, *Senior Member, IEEE*, and Jingcheng Gao

***Abstract*—Smart grid is a promising power infrastructure that is integrated with communication and information technologies. Nevertheless, privacy and security concerns arise simultaneously. Failure to address these issues will hinder the modernization of the existing power system. After critically reviewing the current status of smart grid deployment and its key cyber security concerns, the authors argue that accountability mechanisms should be involved in smart grid designs. We design two separate accountable communication protocols using the proposed architecture with certain reasonable assumptions under both home area network and neighborhood area network. Analysis and simulation results indicate that the design works well, and it may cause all power loads to become accountable.**

***Index Terms*—Accountability, advanced metering infrastructure (AMI), security, smart grid.**

I. Introduction

WITH THE increasing demand for electricity these years, conventional power grids present a number of inefficient and unreliable drawbacks due to out-of-date technologies that were originally designed decades ago. Many nations plan to modernize their current power grids due to events such as voltage sags, overloads, blackouts, large carbon emissions, etc. [22]. Most of these countries believe that it not only requires reliability, scalability, manageability, and extensibility but also should be secure, interoperable, and cost-effective. Such electric infrastructure is referred to as "smart grid." Generally, smart grid is a promising power delivery infrastructure integrated with bidirectional communication technologies which collects and analyzes data captured in near real time, including power consumption, distribution, and transmission [1]. According to these data, the smart grid can provide predictive information and relevant recommendations to all stakeholders, including utilities, suppliers, and consumers, regarding the optimization of their power utilization [1]. By two-way electrical flow, consumers are able to sell their surfeit energy back to utilities [2].

Smart grid is a complex system of systems. Deploying such a system has enormous and far-reaching technical and social benefits. Nevertheless, increased interconnection and integration also introduce cyber vulnerabilities into the grid. Based on experiences gained from developed information technology (IT) [30] and telecommunication systems, we know that the envisioned grid will be a potential target for malicious, well-equipped, and well-motivated adversaries [13], [15]. In addition, the increased connectivity of the grid will enable personal information collection, which may invade consumer privacy [12], [14]. Failure to address these issues will hinder the modernization of the existing power system.

One specific problem in the smart grid is about the billing information. From the homeowners' perspective, their primary concern regarding power usage is the monthly power bill sent by their service providers (e.g., power utilities). If possible, homeowners would rather know the details of their power usage than simply receive a bill with a total consumption. Albeit the real-time, or day-to-day, consumption of electricity could be revealed by the smart meter, we still doubt its reliability: The utility, or the smart meter itself, may alter transmitted data to suit someone's interests or for some other possible reasons (e.g., due to the fact that they are under attack or malfunction). As a consequence, a homeowner could have two different electric bills: one from the utility's meter and one from the home meter. Furthermore, in smart grids, prices change with time such that the traditional billing method using a unit price is no longer feasible. Therefore, the exact times when power is used are important and should be made accountable.

From utilities' perspective, they charge customers solely based on the readings from their power meters. In order to get individual power consumption, in the past, the utility would send technicians to manually gather meter readings. At present, by using automatic meter reading (AMR) technology, meter information can be remotely obtained via a private corporate network or the public Internet. Once the meter is compromised or malfunctions (i.e., we denote it as a faulty meter), the reading may not reflect the actual information of power consumption. The utility therefore could have economic loss. This kind of events is usually caused by unauthorized meter modification. A possible solution is to prevent the meter from being altered. For example, if there is an illegal change on the meter, it will be disabled automatically, and a relevant notification will be sent to the utility. The authors could use a circuit design to do this job [3]. However, the hardware approach has the capability of being bypassed by sophisticated cyber attacks in more complex networks of smart grid. Malicious ones may hack the meter via a network system without touching the meter physically. Considering the operating cost and technical difficulty, utility only measures the aggregated power supply (in a substation) to a service area. For each branch of the supply, the utility installs one meter (at the consumer's side) to monitor the power usage. Within such infrastructure, it is really difficult for the utility to find a faulty meter. They just monitor the aggregated reading and the sum of all branch readings. If

Manuscript received April 3, 2012; revised September 30 2012; accepted January 23, 2013. Date of publication June 21, 2013; date of current version May 22, 2014. This work was supported in part by the U.S. National Science Foundation under Grants CNS-0737325, CNS-0716211, CCF-0829827, and CNS-1059265.

The authors are with the Department of Computer Science, The University of Alabama, Tuscaloosa, AL 35487-0290 USA (e-mail: yangxiao@ieee.org).

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

Digital Object Identifier 10.1109/JSYST.2013.2260697

there is any difference (within a tolerable range considering normal transmission loss) between them, then the monitored area might be suspicious. Through this means, the utility only narrows down the suspicious group but may hardly identify the faulty one.

To solve the aforementioned problems and to make the smart grid reliable are the two major motivations of this paper. We design two accountable communication protocols for home area network (HAN) and neighborhood area network (NAN) by using a peer review strategy in this paper. Through a logical analysis, we argue that our scheme may effectively detect any faulty meter under some reasonable assumptions. The following three major contributions are made in this paper: 1) A smart meter can prove the correctness of any smart appliance in a home area; 2) a group of smart appliances can prove the correctness of the smart meter; and 3) a service provider can prove the correctness of the smart meter.

The rest of this paper is organized as follows. Section II briefly introduces smart grid and accountability technologies. Section III discusses how an accountable system for a home area smart grid is designed and deployed. Section IV designs system accountability in a neighborhood area smart grid. Section V shows the analytical and simulation results. Finally, we conclude this paper in Section VI.

II. Background and Related Work

A. Smart Grid

Smart grid requirements and characteristics are introduced as follows. Emerging from current power grid systems, the smart grid has more requirements and new characteristics that have to be accomplished which are listed as follows. *Advanced metering infrastructure (AMI)* is an integration of multiple technologies which provides intelligent connections between consumers and system operators [3]. It is designed to help consumers know the real-time prices of power and to optimize their power usage accordingly [4], [5]. It also helps the grid obtain valuable information about the consumers' power consumption in order to ensure the reliability of the electric power system [6]. *Wide-area situational awareness* needs to monitor and manage all the components of the electric power system. For example, their behaviors and performance may be modified and predicted to avoid or to deal with potential emergencies [4]. *IT network integration* requires that the smart grid scopes and subscopes will use a variety of communication networks, which are integrated from IT networks. *Energy storage and transportation* requires that the smart grid will change the available bulk energy storage technology into new storage capacities, particularly for distributed storage [4]. *Demand response and consumer efficiency* requires that utilities and customers will cut their usage during peak times of power demand. Furthermore, mechanics will also be made for consumers to use their power devices intelligently to decrease their cost [4]. We can conclude that the smart grid will have the characteristics of being more efficient, reliable, and intelligent. However, integrating information networks into the current power grid system causes many security and privacy issues that must be dealt with. IT networks introduce obvious vulnerabilities. For example, hackers can steal customers' power without any trace in their metering devices. This makes accountability a necessary research problem in this area, particularly so that, when users get the power bill from their utility company, they will have adequate evidence to prove the exact power load that they have consumed.

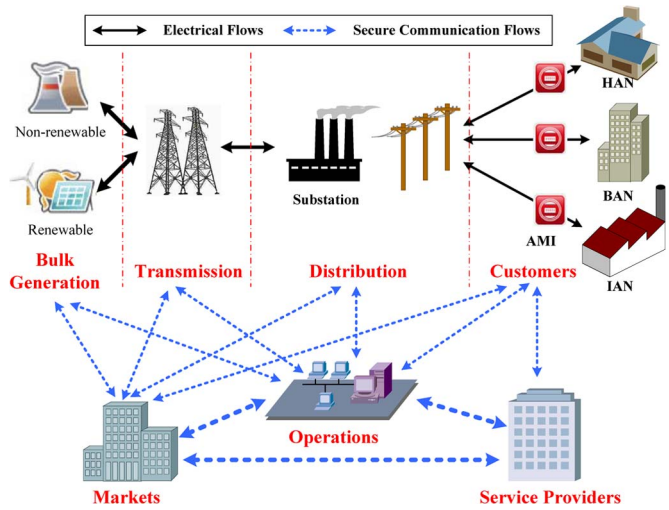


Fig. 1. Smart grid power system architecture [4].

Several architectures of smart grid have been proposed by national organizations and companies, such as the Department of Energy (DOE, U.S.), State of West Virginia, National Institute of Standards and Technology (NIST), Cisco, etc. DOE's *Smart Grid System Report* [2] claimed that a smart grid's architecture should include the following scopes: Market Operators, Reliability Coordinators, Gen/Load Wholesalers, Transmission Providers, Balancing Authorities, Energy Service Retailers, Distribution Providers, and End Users (Industrial, Commercial, and Residential). West Virginia's abstract architecture [5] mostly focused on four key technology areas: Sensing and Measurement, Advanced Control Methods, Improved Interfaces and Decision Support, and Advanced Components. NIST proposed an architectural reference model in the *NIST Framework and Roadmap for Smart Grid Interoperability Standards* [4]. This model (shown in Fig. 1) listed the relevant components as follows: Customers, Markets, Service Providers, Operations, Bulk Generation, Transmission, and Distribution [4]. Cisco's architecture is totally different because it argues that the whole system would use an independent "network of networks" [7]. Cisco also claims that the best standard suite of protocols for the smart grid is the Internet Protocol (IP) [1]. Due to the fact that IP has already achieved great success in the current Internet in terms of flexibility, security, and interoperability, Cisco believes that the interoperability standards of the smart grid should use IP architecture as a reference [1]. Aside from the aforementioned national organizations and companies, several other researchers also proposed smart grid architectures with certain features that they want to add into the system. Clark and Pavlovski [7] proposed a wireless smart grid architecture that has the ability to remotely sense power delivery. Gadze [8] proposed a hierarchical architecture for the smart grid, which is a multilevel decentralized platform dealing with the

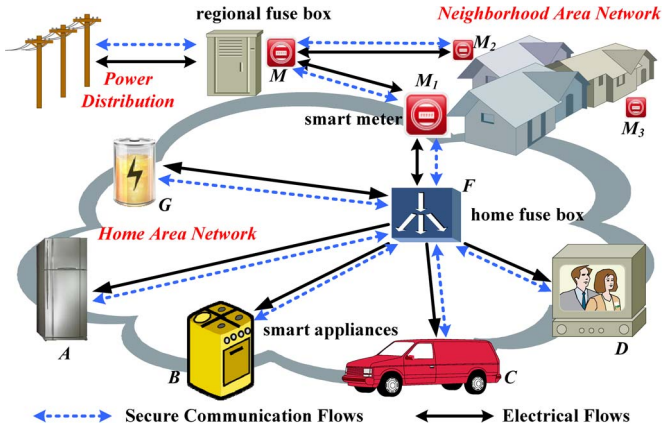


Fig. 2. Typical design for the AMI in smart grid.

potential impacts of harsh power environments. The remainder of the presented architectures [9]–[11] are focused on a part of the whole system in some fashion and are intended to deal with specific requirements that would be worthy to address. Essentially, a smart grid architecture must address the following critical issues [1]: 1) transmitting data over multiple media; 2) collecting and analyzing massive amounts of data rapidly; 3) changing and growing with the industry; 4) connecting large numbers of devices; 5) maintaining reliability; 6) connecting multiple types of systems; 7) ensuring security; and 8) maximizing returns on investments.

After reviewing these proposed architectures, we believe that NIST's model is the most fully described architecture proposed in the recent smart grid literature. It contains almost every scope brought up by the standard organizations mentioned earlier, from bulk generation to end users. In addition, it provides a means to analyze use cases, to identify interfaces for which interoperability standards are needed, and to facilitate the development of a cyber security strategy [4]. Therefore, we will adopt this model as the basic framework. As shown in Fig. 2, the smart meter is a key component of the AMI, which manages consumer areas, such as the HAN, building area network (BAN), and industrial area network (IAN). Householders in a HAN can use smart meters to automatically turn home appliances on and off or up and down and to switch smart appliances to an economy mode based on how they want to conserve energy. A group of HAN (BAN or IAN) forms a NAN. Utility usually installs one master meter at a substation to monitor all branch power supplies. The individual power consumption can only be measured by the smart meter installed at the consumer side. Albeit the NIST sets a number of regulations to secure the AMI, vulnerabilities still exist in its model. As the NIST suggested itself, accountability should be involved in the smart grid design. To design an accountable AMI is the major research thrust of this paper.

B. Accountability

Security is especially challenging in the smart grid. Although advanced cyber security technology has protected every level of the current network infrastructure, new vulnerabilities have continued to emerge under the framework of the smart grid [2], [12]–[15]. As a complement, accountability is required to further secure the smart grid in terms of privacy, integrity, and confidentiality. Even if a security issue presents itself, the built-in accountability mechanism will find out who is responsible for it. Once detected, some problems can be fixed automatically through the predefined program, while others may provide valuable information to experts for evaluation.

In essence, accountability means that the system is recordable and traceable, thus making it liable to those communication principles for its actions. Every change in a local host or network traffic, which may be the most important or most desirable information, may be used as evidence in future judgment. Under such a circumstance, no one can deny their actions, not even the administrators or other users with high privileges. Together with some suitable punishments or laws in the real world, this will prevent a number of attacks.

Accountability logic is regarded as an effective way to analyze the accountability of a secure system. Most of accountability logic has been designed for electronic transactions. Kailar [16] proposed accountability logic for electronic commerce protocols such as payment and public key distribution protocols. He defined accountability as a property whereby the association of a unique originator with an object or action can be proved to a third party. Provability has an important role in the analysis of accountability. Since time-critical applications require proofs that guarantee the temporal activities of each principal, Kailar's accountability logic can be extended for use in analyzing such applications [17]. Although Kailar's original logic allows some temporal context, such as *During* and *Until* properties, to be added to represent the validation period of security-related information, such as a time-critical delegation key, Kudo [17] extended Kailar's logic so that it could represent temporal accountability. Based on Kailar's logic, Kudo added nine new logic constructs (e.g., *timestamp, at, before, after*, etc.) and ten new logic postulates (e.g., A *CanProve* x generated *at* t, A *CanProve* x generated *before* t, etc.). Since our design is associated with temporal activities, we would like to use Kudo's logic provability in this paper. Note that an early version of this paper was presented in a conference [25], [26]. There are also some related works [27]–[60].

III. Accountability in Home Area

Although the framework and blueprints of the smart grid have been discussed in recent years [3]–[15], a specific standard for its implementation is still to be determined. Two steps need to be clarified before designing an accountable system for the AMI in a home area: to build a possible architectural framework for its implementation and to identify potential security problems.

A. Architecture

Due to the smart grid characteristics and system framework, we proposed a reasonable architecture for a HAN (BAN or IAN) grid. As illustrated in Fig. 3, a smart meter M acts as a middleman between the service provider S and home appliances (e.g., A, B, and C). It acts as a gateway, which

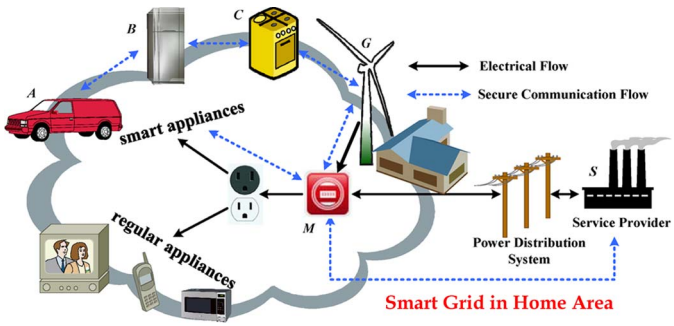


Fig. 3. Smart grid in home area.

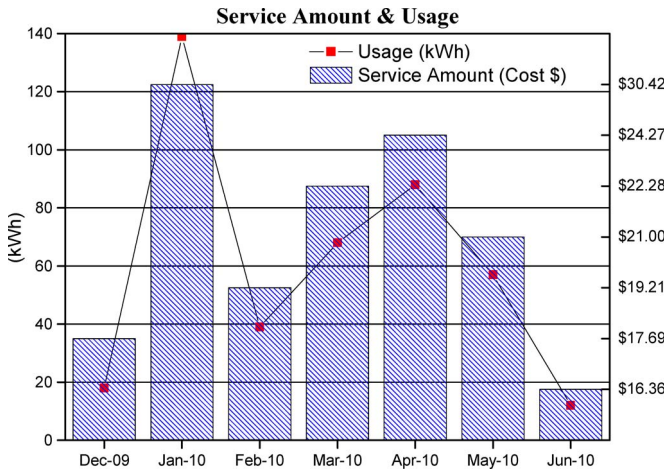


Fig. 4. Conventional service amount and usage chart.

monitors all incoming and outgoing electricity flows. Meanwhile, it also records power consumption and generation in home areas. We divide electrical appliances into two categories based on their communication capability. One refers to smart appliances, and the other refers to regular appliances. In this specific case, only smart appliances have the ability to exchange information or ***message*** (e.g., market price, trading price, and consumption logs) with others, including the smart meter. They are also capable of recording those *messages*. For those regular appliances that are not interactive, the smart meter simply monitors their activities on corresponding power supply ports. In a modern power grid, most families would typically equip a power generation and storage device, denoted as G. We assume that such equipment is a type of smart appliance. Due to the fact that regular appliances have no communication capabilities, we simply assume that all appliances in future home areas will be smart appliances.

B. Problem Statement

Conventional metering systems charge electricity consumption according to its reading at the end of each month, as shown Fig. 4. If the meter reading says that n kWh has been used within a month, the bill (aka. service amount) without tax will be the product of n and a unit average price (denoted as m dollars/kWh). Basically, m is predefined and published by the service provider. It does not change very often. Therefore, it may be regarded as a constant value.

Unlike the simple conventional approach, a modern power grid will use smart meters to read electricity usage at a predetermined requested interval (e.g., daily, hourly, or per minute). That reading data are subsequently stored locally and then transmitted to the service provider as it would usually. At higher levels, the smart meter will get a real-time unit price (aka. market price) from the service provider or other market via a bidirectional wired or wireless network. Together with the powerful energy management of the AMI, households cannot only make economic choices based on dynamic prices, but they can also shift, load, and store or sell surplus energy. Hence, calculating the service amount in such a new power infrastructure is difficult.

Basically, only two key factors affect the bill: 1) the real-time power usage and 2) the corresponding market price. The smart meter can obtain both aspects in real time. However, we cannot simply do a multiplication to get the service amount since the market price is not a constant value and may vary from time to time. For example, the price could remain high during peak hours or high demand periods due to electricity shortage. When outside of peak periods, the price is decreased accordingly. The price may also become affected by local weather conditions. Continuous cloudy or rainy days may reduce the local production of solar energy, and then, the price might increase. However, if a strong hurricane follows, the price will reasonably fall since it enhances wind power generation at the same time. Hence, it is hard to predict the exact market price at a particular time and a specific location. We instead maintain a record of forepassed market price. Current solutions, reported by the U.S. DOE [2], take three typical tariff forms: time of use (TOU), critical peak pricing (CPP), and real-time pricing (RTP). TOU pricing is solely based on a peak or off-peak period designation. Prices are set higher during peak hours. Under CPP, prices during peak hours (basically some short periods within a year) are set at a much higher level compared to that under normal conditions. RTP is far more flexible in that hourly prices are differentiated according to the day-of or day-ahead cost of power to the service provider. Pricing in the smart grid is an interesting and essential open issue that must be addressed. The author in [18] argued that a price-response demand mechanism should be introduced in the smart grid. Since pricing is not our primary scope in this paper, we simply assume that the real-time market price may be obtained in a secure and feasible way (via service provider or third party, e.g., markets). Under such conditions, we reasonably suppose that, given any past time t, the market price may be determined by a function $M(t)$. As it is a dynamic feature, $M(t)$ should be a nonlinear and random curve regarding time t, as illustrated in Fig. 5.

Another possible factor affecting the service amount is the presence of a home-generated power system (e.g., wind or solar energy). Without consideration of its own consumption, the generated energy may be divided into two parts: those consumed by other electrical appliances at home and those sold back to the service provider. Both of them are monitored and recorded by the smart meter, but only the trading portion impacts the service amount. Note that the trading price might be the market price or could possibly even be set by the

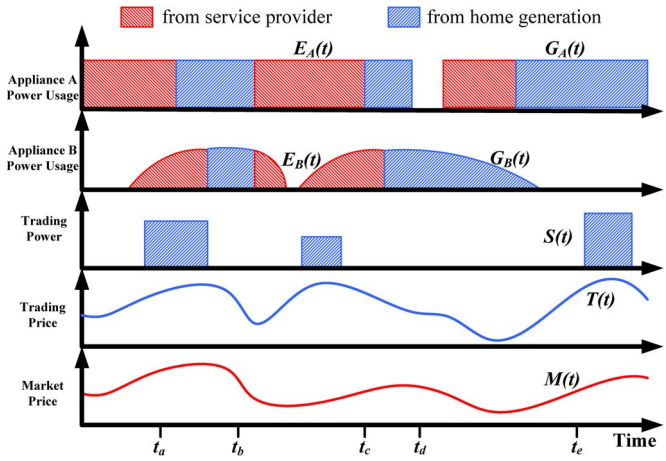


Fig. 5. Aggregation information in the smart meter.

homeowner. Here, we suppose that the trading price is a nonlinear function of t and denoted as $T(t)$, as shown in Fig. 5.

Fig. 5 is an example of energy usage in a modern power grid. We denote purchased energy (from a service provider) as $E(t)$, self-consumed energy (from home generation) as $G(t)$, and trading power as $S(t)$. They are all functions with respect to time t. If there is no power consumption or sale event during a period, the relevant functions will automatically be zero. Given any time period from t_a to $t_b(t_b > t_a)$, the total service amount denoted as $Bill(t_a, t_b)$ should be

$$Bill(t_a, t_b) = \int_{t_a}^{t_b} (M(t) \cdot E(t) - T(t) \cdot S(t))\, dt. \quad (1)$$

In (1), $E(t)$ can be obtained by attaining the sum of every individual consumption (denoted as $E_i(t)$ where i is the name of the electrical appliance). For each appliance i, the service amount from t_a to $t_b(t_b > t_a)$, denoted as $Bill_i(t_a, t_b)$, can be determined by the following equation:

$$Bill_i(t_a, t_b) = \int_{t_a}^{t_b} M(t) \cdot E_i(t) dt. \quad (2)$$

Equation (1) can thus be rewritten as

$$Bill(t_a, t_b) = \sum_{i=A,B,\ldots} Bill_i(t_a, t_b) - \int_{t_a}^{t_b} T(t) \cdot S(t) dt. \quad (3)$$

According to the former, it is not difficult to see that computing service amounts in a smart grid is indeed a complicated procedure. Many factors in the smart meter may affect the final bill. Any alternation, forgery, delay, or removal of those historical records may lead to a different price. Although we could equip secure smart meters to enhance reliability, it is still possible for homeowners or cyber attackers to manipulate the smart meter for their own interests. In addition, when the service provider brings alternative bills to a homeowner, whom should we trust? Since most service providers rely on meter readings, ensuring a secure and reliable smart meter is the primary task.

We consider an entity as ***correct*** only if it strictly follows a given protocol. Otherwise, we regard it as ***faulty***. Here, we use smart appliances as witnesses to prove that the smart meter is *correct*. The witness idea was inspired by the PeerReview system [19]. In this case, three new problems should be addressed. First, a smart appliance itself may have errors or be controlled by a malicious person. To make every *faulty* smart appliance detectable is necessary (***Challenge 1***). Second, since appliances have limited capabilities for communication and storage, designing a feasible observable mechanism for witnesses is also required (***Challenge 2***). Third, home-generated power is managed solely by the smart meter. Other smart appliances do not know where the power load comes from; it might be supplied by the free home generation or purchased from the service provider. Without supervision, the smart meter may deny that, during a certain period, an appliance was using power from the service provider (***Challenge 3***). In the following sections, we will describe our design of accountable AMI that addresses these challenges.

C. Terms and Assumptions

Several terms and assumptions should be addressed as follows. Let $\{A, B, \ldots\}$ denote a set of communication participants in the smart grid, known as ***principals***. Specifically, M stands for the smart meter, G represents the home generation and storage device, and S refers to the service provider. Let $\{m, m', n\}$ denote a set of *messages* or *message* components. Let $\{t_i | i = a, b, \ldots\}$ denote a set of time points. Let $\{K_i, K_i^{-1}\}$ denote a pair of public/private keys of *principal* i. Let $\{m\}K_i$ denote the message m encrypted with the public key of principal i. Let $\{m\}K_i^{-1}$ denote the message m encrypted or signed with the private key of principal i.

We assume the following: 1) Every electrical appliance i in the home area is a smart appliance with sufficient storage space and a constant capacity factor P_i (kW); 2) the running state of every smart appliance (e.g., on or off) is known by the others in real time; 3) functions of market price $M(t)$ and trading price $T(t)$ are authenticated by the service provider, and every smart appliance shares these functions at the same time; 4) there is a function w that maps each appliance to its set of witnesses, and we suppose that, for any appliance i in a home area, the set $\{i\} \cup w(i)$ contains at least one *correct* smart appliance; 5) a *message* sent from one *correct* appliance to another will eventually be received; 6) each involved communication *principal* uses public key infrastructure (PKI) technology to identify itself, and they can sign *messages*, but a *faulty principal* cannot forge the signature of a *correct* one; 6) a home generation and storage device G must record its own power load $G(t)$ truthfully; and 7) each appliance i will record its consumed power that is supplied from G, denoted as $G_i(t)$.

Assumption 2 depends on circuit/communication designs which may be achieved by particular sensor units in the smart grid. For simplicity, we suppose that Assumption 2 can be met. More specifically, we suppose that there is a function $R_i(t)$ that records the running state of appliance i. When t is within the running period of i, $R_i(t)$ is granted to 1; otherwise, $R_i(t)$ is set to 0.

In Assumption 7, $G_i(t)$ is given by the smart meter. Because the appliance does not know where the supply comes from, the smart meter should provide such information. $G_i(t)$ will be signed by the smart meter so that it can be further verified with $G(t)$.

D. Accountable Protocol

Since the power usage of appliance i can be determined by its capacity factor P_i and running state $R_i(t)$, the (2) for its market service amount can be rewritten as

$$MPA_i(t_a, t_b) = P_i \cdot \int_{t_a}^{t_b} M(t) \cdot R_i(t) dt. \tag{4}$$

According to (4) and Assumption 1 (for flexible P_i, please see discussions in Section III-E), if any *principal*$j(j \neq i)$ holds P_i, $M(t)$, and $R_i(t)$ at the same time, j is able to determine i's market service amount for any past period. Notice that j still does not know the exact service amount of i since j has no knowledge of i's power source. If i were using home-generated power all the time, i's service amount would be zero. For auditing, i's market service amount can also be specified by

$$MPS_i(t_a, t_b) = \int_{t_a}^{t_b} M(t) \cdot (E_i(t) + G_i(t))\, dt. \tag{5}$$

Next, we borrow some ideas from the PeerReview system [19]. Given any period from t_a to t_b, $MPA_i(t_a, t_b)$ should equal to $MPS_i(t_a, t_b)$. Based on this fact, we can design a deterministic mechanism in order to detect *faulty principals* in a home area. Under our proposed architecture, each appliance i has two modules for accountability: a log module L_i and a detector module D_i. L_i generates a complete evidence log of i's power usage. D_i checks other logs to tell whether faults are, or are not, present. Informally, *faulty(j)* is issued when i can prove that j is abnormal, *suspected(j)* is raised when i has not received an expected *message* from j on time, and *correct(j)* is released if otherwise. Our design therefore follows the following protocols: 1) When a new appliance i is plugged in, i will sign P_i with its unique signature K_i^{-1} and broadcast $\{P_i\}K_i^{-1}$ among all principals in the home area; 2) the smart meter will notify each appliance as to whether it currently uses home-generated power; 3) each appliance has one copy of its own log, which is ensured by the tamper-evident log mechanism [19]; other logs will be retrieved when required, and appliances exchange just enough *messages* to prove themselves; 3) each appliance is mapped to several other appliances, and they act as witnesses that collect its log, check its correctness, and report the results to the rest of the system; 4) a commitment protocol [19] is then adopted in order to ensure that witnesses will retrieve exactly the same log as the target appliance owns, and it also guarantees that no one can deny a received *message*; 5) this protocol uses a challenge/response scheme [19] to address the problem that some appliances do not respond or fail to acknowledge that *messages* were successfully sent.

Next, we will demonstrate how it works in detail. Initially, every new appliance i will be assigned a set of witnesses w_i by the smart meter. Then, i will sign P_i with its unique signature K_i^{-1} and send $\{P_i\}K_i^{-1}$ to the smart meter and each member of w_i. When i is running, L_i generates a tamper-evident log to record its power usage. Since the smart meter will notify i regarding its power source, the log will record both $E_i(t)$ and $G_i(t)$. In order to check whether i is *correct* or not, each witness of w_i will periodically request its most recent log segment. Suppose that the last audit time is t_a and the current time is t_b. In this case, i first requests and records the latest $M(t)$ and $T(t)$ from the smart meter. Then, it sends back each and every one of the log entries since time t_a, together with the corresponding market service amount determined by (5). Specifically, the response *message* m_i should have $\{t_a, t_b, E_i(t), G_i(t), MPS_i(t_a, t_b)\}K_i^{-1}$. Note that m_i could have other information to support certain needs, for instance, adding a sequence number to prevent replay attacks. In this paper, we only focus on the accountability part for simplicity. When a witness $j(j \in w_i)$ receives m_i (using K_i to verify m_i), D_j will recalculate i's market service amount $MPA_i(t_a, t_b)$ by (4) according to its own records of P_i, $M(t)$, and $R_i(t)$ (refer to Assumptions 1, 2, and 3). If the difference of $MPA_i(t_a, t_b)$ and $MPS_i(t_a, t_b)$ is tolerable (i.e., less than a predefined threshold Δ), D_j will issue *correct(i)*; otherwise, *faulty(i)* is issued (***Challenge 2*** is addressed). Since we use a challenge/response protocol here, every appliance i must respond to the requests from its witnesses, or else, *suspected(i)* will be indicated. We also adopted the commitment protocol here, so that all signed *messages* may become evidence against *faulty* appliances. Because there is always a *correct* witness j within w_i (Assumption 4) and all delivered *messages* will be received (Assumption 5), a *faulty* appliance i will eventually be exposed by D_j with its indicators: *suspected(i)* or *faulty(i)* (***Challenge 1*** is addressed).

To deal with ***Challenge 3***, we consider all appliances in the home area as witnesses of the smart meter. When suspicions are raised against the smart meter, the third party (e.g., the service provider) will retrieve all evident logs regarding $G_i(t)$ from each home appliance i, together with the self-consumed energy record $G(t)$ from the home generation and storage device G. Since every principal uses tamper-evident logs to record its behavior, any mismatch between $\sum(G_i(t) + E_i(t))$ and $G(t) + E(t)$ will prove that the smart meter is not correct according to Assumptions 4 and 7.

The protocol described up to the current point has addressed the three aforementioned challenges. Convinced evidences are able to eliminate the questionable charges on the final bill. As to the message latency, throughput, and traffic overhead, Haeberlen *et al.* [19] have shown that this peer review mechanism is scalable in a distributed system based on experiments and mathematical analysis.

E. Assumption Analysis

The proposed protocol only works under certain assumptions. In Assumption 1, all electrical devices in home areas are determined to be smart appliances. In fact, the smart grid should

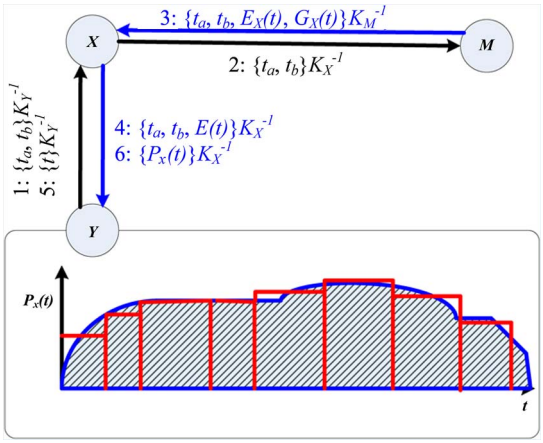


Fig. 6. Improved protocol without constant power capacity factor.

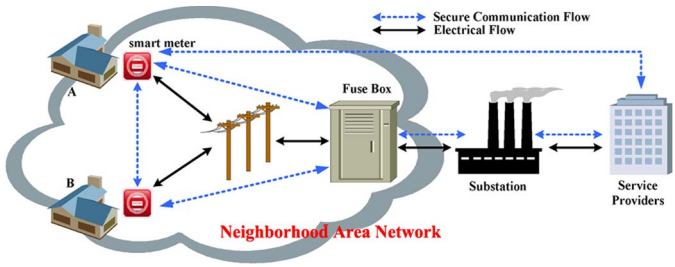


Fig. 7. Smart grid in neighborhood area.

obtain downward compatibility. Current regular appliances may still work in the modern power grid. For those appliances with no capabilities of communication, finding appropriate witnesses for them subsequently becomes a problem. Considering regular appliance issues, our protocol needs to be modified in future work. In addition, we suppose that every appliance has a constant value for its power capacity factor. In reality, this may be a false assumption. Electric cookers and water heaters are good counterexamples. With a flexible power capacity factor, our protocol is unable to detect *faulty* principals. For Assumption 7, if home power generation device G can forge its power load before recording it into the tamper-evident log, the accountability goal **G4** cannot be met. Since only the smart meter monitors its behavior in our architecture, it is hard to convince others that G is correct solely based on the proof of the smart meter. Making G accountable is required in the next step. Regardless of the architectural design, there is still much research to do before we can build an accountable smart grid.

Considering the issue of flexible power capacity factor, we remove the condition of constant value in Assumption 1. Meanwhile, we require an extra assumption (Assumption 8): *Every appliance is able to sample others' power capacity factor* $P_i(t)$ *at a certain time* t. The sampling job can be done by particular sensors. The witness will record the sensors' reading with its "tamper-evident log." As depicted in Fig. 6, the real power capacity factor (continuous area) can be estimated by using simple integral knowledge on these recorded discrete factors (blocks). The other protocol remains the same. By this means, the *faulty* principal still may be found with certain possible false reports. This idea should be further studied in the future work, particularly when $P_i(t)$ is not accurately sampled.

IV. Accountability in Neighborhood Area

In Section III, we proposed an accountable communication protocol for smart grid in a HAN. Through mutual observations among smart appliances, their power consumptions can be verified whether they are veritably recorded or not. A *faulty* meter therefore may be found out if the reading does not match the appliances' records. The records will be served as evidences against the *faulty* meter. It appears that our scheme well solved this problem in the smart grid. However, it is only reasonable when the user claims the power bill is incorrect. Utility company can hardly know there is a problem if the *faulty* meter holds all the evidence and never sends them out. From the utility's perspective, obtaining all the observed records to find *faulty* meters is an unwise choice. On the one hand, it generates too much network traffic that is hard to process and manage. On the other hand, no *faulty* meter would send evidence against itself. In this case, a more efficient and feasible solution is required for the utility. Since HAN and NAN are different scenarios, we need to first study the NAN architecture before proposing our accountable scheme.

A. Architecture

Despite the fact that there are currently no explicit specifications available for smart grid implementation, we still can reach a consensus that both communication and electric paths are bidirectional. According to the characteristics and blueprint of the smart grid, we can reasonably present a framework for smart grid in a neighborhood area as shown in Fig. 7.

In a conventional power distribution system, a community power supply is typically served by the same electric utility company. Within every community, there is a distribution room or a fuse box that delivers power to each customer's home. It is just like a "power router" as described in [23]. This fuse box may equip a meter, denoted as master meter, which measures the aggregated power supply from the service provider but not the power consumption for each end user. For each branch of the supply, utility only installs one meter at the consumer side to monitor their power usage. Current power grid widely uses AMR technology to remotely collect the meter information. For the sake of saving operating cost, it is more efficient to maintain the same topology of the distribution system. The main difference is that, in the smart grid, all communication and electric flows are bidirectional. A smart meter may directly connect to the service provider via a feasible public communication network (e.g., Internet). It may also connect the service provider through a fuse box and multiple substations using a private corporate network. We do not specify the communication technology preference since we believe the accountability protocol should not rely on that. In addition, all regional smart meters could exchange information with each other. This functionality not only enables power transactions among neighbors but also helps accountability systems to collect convinced evidence. For the case in Fig. 7, meters A and B located in a same

community have a common service provider. We refer to the power distribution system in that community as a "NAN."

Considering customers' privacy, a meter would never expose too much information to the others. The communication flows within the NAN can become anonymous by using pseudonym mechanism. The traffic information therefore is not easily associated with its originator. More specific solutions are given in [23] and [24]. Since our goal is to design an accountable NAN scheme, we simply assume that the privacy problem has already been addressed.

B. Problem Statement

Generally speaking, accountability systems will set a number of witnesses to monitor activities of the observation object. Once an abnormal behavior is detected, those witnesses will provide relevant observation evidence in order to support their findings. These evidences are typically undeniable and thus trustworthy. Making power consumption accountable is the primary target of the current text. In Section III, with certain assumptions, we make all power loads in a home area accountable. By this means, a customer can easily verify his/her monthly electricity bill, and thus, the *faulty* meter will be discovered. In this section, we try to address the problem from the utility's perspective. However, we cannot use the proposed scheme for the smart grid in a NAN directly. Since a meter can only measure one power line at a time, it is very difficult for a household meter to monitor other neighbor's power usage. In other words, if we want to prove the correctness of a smart meter, an additional meter should be installed on the same power line for witness purpose.

As we discussed in Section IV-A, the conventional power grid at most deploys one extra meter (aka. master meter) in the fuse box for one NAN. Once there exists a faulty meter, it is highly possible that the sum of all meter readings in that area does not match the master meter's reading. Notice that such difference may be caused by power loss for normal distribution. For computational simplicity, we regard it as an empirical value that has the capability of being obtained from previous measurements. Based on this value, we may define a threshold Δ so that, if the difference is less than the Δ, the NAN works properly; otherwise, the power usage in that NAN is abnormal. Still, the utility does not know how many *faulty* meters exist and where they are located. Instead of sending technicians to inspect every meter in that area, a more efficient way should be considered for the smart grid.

In fact, we may deploy multiple meters in the fuse box for witness purpose. Intuitively, the more witnesses at hand, the fewer steps are required to locate faulty meters. The optimal method is, of course, one-to-one witness as well as object pairs. However, it is quite impossible to double the number of meters nationwide. Therefore, a feasible solution would be adopting "intersected grouping" technology to minimize the number of witnesses. As the case shown in Fig. 8, there are six household meters in a NAN (e.g., a, b, c, d, e, and f) and three witnesses in a fuse box (e.g., one master meter M and two additional meters A and B). By using witnesses A and B, six household meters have been divided into three groups: Group A (e.g., a and b), Group A-B (e.g., c and d), and Group B (e.g., e and f). According to the witness results, we have the ability to narrow down the searching area for *faulty* meters. For example, if there is only one *faulty* meter in the NAN but both witnesses A and B report abnormal activities, we may reasonably infer that the *faulty* one is in Group A-B. Then using witnesses A and B to monitor c and d, respectively, the *faulty* meter will be found eventually. Nevertheless, if the number of *faulty* meters becomes two or more, things will be more complicated. How to do the grouping and regrouping under different scenarios is therefore our task in the following sections.

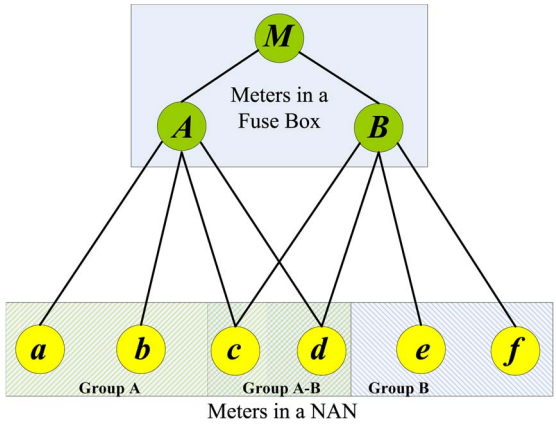


Fig. 8. Accountable power distribution system in NAN.

C. Terms and Assumptions

Aside from the terms defined in Section III-C, we define the following terms. Let $\{A, B, \ldots\}$ denote a set of meters in the fuse box, known as witnesses. Specifically, M stands for the master meter, and S refers to the service provider. Let $\{a, b, \ldots\}$ denote a set of household meters in the NAN, known as observation objects (or objects). Let λ denote the number of witnesses in the fuse box except the master meter. Let μ denote the number of household meters in the NAN. Let τ denote the number of *faulty* meters in the NAN.

We have the following assumptions: 1) Every meter is a smart meter that can communicate with each other, and it has sufficient storage space to save log files; 2) the fuse box has at least two witnesses and one master meter inside, and all of them are *correct* meters; 3) a witness can choose and change its observation objects at any time; 4) the number of *faulty* meters is much less than the total number of meters in the NAN (e.g., $\tau = 1$ or 2); 5) there exists a function w that maps each witness to its group of observation objects so that the number of groups in the NAN is maximized; 6) a *message* sent from one *correct* meter to another will eventually be received; and 7) each involved communication principal uses PKI technology to identify themselves; they may sign *messages*, but a *faulty principal* cannot forge the signature of a *correct* one.

Assumption 1 is a fundamental premise of our scheme. Without mutual observation and communication, no one believes a single device who claims itself is *correct*. Assumption 2 may increase the operation cost of the power utility. An economic way to achieve this goal is to manually deploy the

witness' meter when necessary (e.g., on demand or periodically checking). Assumption 3 depends on circuit/communication designs, which may be achieved by dynamically dispatching power supply to the desired branch. This function has already been achieved in a power router [23]. The router can switch power supplies (inputs) to different devices (outputs) and may also choose the desired supply from many power sources. It acts like the router in the computer networks. In our assumption, we just adopt its circuit design in the fuse box and deploy the witness meters at the inputs to monitor those outputs. For simplicity, we suppose that Assumption 3 can be met.

D. Accountable Scheme

By using the "intersected grouping" method described in Section IV-B, μ household meters are assigned to λ witnesses according to function w. Therefore, those household meters are divided into several groups. After a fixed time of observation, denoted as t, the witnesses will know which groups are *correct* and which are *suspected* by comparing their readings. Our accountable scheme therefore may be described as follows: 1) When a new household meter i is deployed, M will assign a pseudonym P_i to i with its unique signature K_M^{-1}, and P_i will be periodically changed due to privacy consideration; 2) every meter has one copy of its own log, which is ensured by the tamper-evident log mechanism [19]; other logs will be retrieved when required, and meters exchange just enough messages to prove themselves; 3) each household meter is mapped to several other witnesses, and the witnesses collect its log, check its correctness by comparing the readings, and report the results to the rest of the system; 4) the witnesses will be reassigned observation objects according to function w at set intervals; 5) a commitment protocol [19] is adopted to ensure that witnesses will retrieve exactly the same log as the observation object owns, and it also guarantees that no one can deny a received message; 6) this protocol uses a challenge/response protocol [19] to address the problem that some household meters do not respond or fail to acknowledge that messages were successfully sent.

Next, we will demonstrate how it works in detail. Every household meter i will be assigned a pseudonym P_i and a set of witnesses w_i by M. All the witnesses in w_i will be notified that P_i is their observation object. When meter i is running, it will generate a tamper-evident log to record its power usage $E_i(t)$. In order to check whether meter i is *correct* or not, each witness of w_i will periodically request its most recent log segment. Such requests are sent by group broadcasting *messages*. Only i in W's observed group will accept the corresponding request, while others simply discard it. Suppose that the last audit time is t_a and the current time is t_b. In this case, meter i will send back all the log entries since time t_a. Specifically, the response *message* m_i should be $\{t_a, t_b, E_i(t)\}K_{P_i}^{-1}$. When a witness $W(W \in w_i)$ receives all corresponding *messages* from its observation objects, W will compare its own reading with the sum of all $E_i(t)$ during the same period (from t_a to t_b). If their difference is within a tolerable range (e.g., considering the distribution power loss), W will claim its observation objects

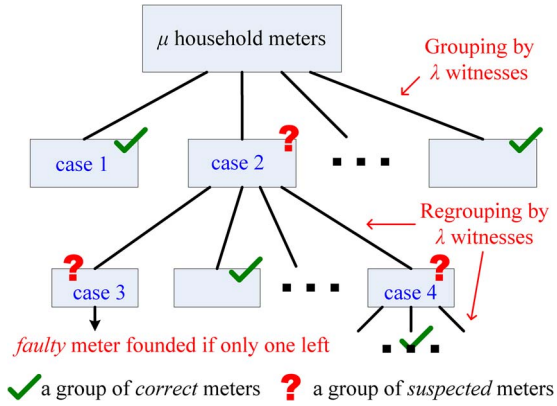


Fig. 9. Accountable scheme in NAN.

are all *correct*. Otherwise, W reports that its observation objects are all *suspected*.

As an example shown in Fig. 9, case 1 is a group of *correct* meters, and case 2 is a group of *suspected* meters. For each group that falls into case 2, M will regroup it using the same λ witnesses and do further observations in the next time period. This process will be repeated until we reach case 3. Case 3 refers to a *suspected* group with only one meter inside. By then, we may claim that a *faulty* meter is found. As we noticed, not all *suspected* groups have *faulty* meters inside. Taking case 4 as an example, all meters in that group are actually *correct*. The reason this group has been marked *suspected* is because some mutual witnesses find abnormal activities in their observation set. Fortunately, case 4 will be immediately clarified after one-step further observation. Since there are only a few *faulty* meters in the NAN (Assumption 4), case 4 should be an infrequent event.

Apparently, "intersected grouping" is the key of our accountable scheme. There are plenty of ways to do this job. One could group *suspected* meters based on their previous behaviors (e.g., previous *suspected* meters would be grouped together), while others may divide them according to their geographic locations. It is hard to tell which one is better to detect *faulty* meters. They could be anywhere at any time, or they may appear in the same community. The size of NAN is also an important impact factor. Different scenarios may have different results. To use the same grouping strategy for every situation is not a wise choice. We let the utility companies design the best one for their interests. In this paper, a feasible approach is presented for demonstration purpose.

To call the above function GROUP (shown in Table I), initially set the input parameters to all witnesses and all household meters, respectively. It is a straightforward algorithm, which continuously reduces the number of *suspected* meters by separating the *faulty* meters from *correct* ones. Lines 4 to 7 are normal grouping procedures. In line 6, the word "enough" means that each subgroup at least has one *suspected* meter, and any two subgroups must have at least one different witness. Lines 8 through 12 will be called when all witnesses find problems. In this case, we first check those *suspected* meters with the most witnesses. Then, check the others (i.e., by the order of the number of witnesses) after that. Due to Assumption 4

TABLE I
GROUP ALGORITHM

```
1.  FUNCTION GROUP (witnesses, suspected_meters)
2.  faulty_meters = Φ;
3.  REPEAT UNTIL suspected_meters == Φ
4.    IF |suspected_meters| ↓, THEN   // do regrouping
5.      reset observation sets for all witnesses;
6.      setup enough subgroups to hold suspected_meters;
7.      uniformly assign suspected_meters to subgroups;
8.    ELSE     // means all witnesses report suspected
9.      check suspected_meters with the most witnesses;
10.     check the rest of meters;
11.     regroup suspected_meters again;
12.   END IF
13.   wait for a fixed period of time;
14.   check the readings for each witness;
15.   update suspected_meters and faulty_meters;
16. END REPEAT
17. RETURN faulty_meters
```

(in Section IV-C), it is highly possible to find the *faulty* ones in the groups that have the most witnesses. Lines 13 to 15 may identify some meters through observations. The loop will end when all *suspected* meters are identified. It may also be terminated after a period of time. This function may also instead return a group of *suspected* meters.

V. EVALUATION

A. HAN Scheme Analysis

Throughout this section, we will analyze the accountability of our HAN protocol by using the same analysis method as in [17]. First, it defines accountability goals. Then, it will interpret every *message* into a logical description. After that, the initial assumptions will be restated in a logical way. Based on the logic described in [17], we can eventually prove that our protocol can achieve all accountability goals by using the message interpretation and the initial assumptions.

We present different accountability goals for our proposed protocol based on the definitions and three ***Challenges*** stated in Section III-B. Suppose that X is any appliance in the home area and that Y is X's witness. The goals can be described as follows: **G1**: M CanProve (X *is faulty or correct*); **G2**: X CanProve (M *is faulty or correct*); **G3**: Y CanProve (X *is faulty or correct*); **G4**: S CanProve (M *is faulty or correct*).

Since an unsigned *message* has no effect on the achievement of goals in accountability logic, we only consider signed ones. The *message* flows can therefore be interpreted as follows: ***Message 1***: M Receives ($\{P_X\}$ SignedWith K_X^{-1}); ***Message 2***: Y Receives ($\{P_X\}$ SignedWith K_X^{-1}); ***Message 3***: X Receives ($\{t_a, t_b, E_X(t), G_X(t), \{M(t), T(t)\}$ SignedWith $K_S^{-1}\}$ SignedWith K_M^{-1}); ***Message 4***: Y Receives ($\{t_a, t_b, \{M(t), T(t)\}$ SignedWith $K_S^{-1}\}$ SignedWith K_M^{-1}); ***Message 5***: Y Receives ($\{t_a, t_b, E_X(t), G_X(t), MPS_X(t_a, t_b)\}$ SignedWith K_X^{-1}); ***Message 6***: S Receives ($\{\{G_i(t)\}$ SignedWith $K_i^{-1} | i \in$ all appliances$\}$, $\{G(t)\}$ SignedWith K_G^{-1}, $\{E(t)\}$ SignedWith K_M^{-1}).

The initial state assumptions required in the analysis are follows: **A1**: Y Receives ($\{P_X\}$ SignedWith K_X^{-1}) => (Y CanProve(P_X isTrusted)); **A2**: X Receives ($\{E_X(t), G_X(t)\}$ SignedWith K_M^{-1}) => (X CanProve($E_X(t)$ isTrusted) and ($G_X(t)$ isTrusted)); **A3**: X Receives ($\{M(t), T(t)\}$ SignedWith K_S^{-1}) => (X CanProve($M(t)$ isTrusted) and ($T(t)$ isTrusted)); **A4**: Y CanProve ($R_i(t)$ isTrusted).

Message 1: When M receives *message* 1, M knows that it was sent by X based on its unique signature. Since M can monitor X's power usage, P_X can be verified by M. If P_X is not true, M can claim X is *faulty*. Otherwise, M can prove the following statement by applying the accountability postulate [16], [17]: M CanProve (X *says* P_X) and (P_X isTrusted). When a suspicion is issued against P_X, this statement can be used as evidence to prove (P_X isTrusted). This is the accountability goal **G1**.

Message 2: Y receives *message* 2 at the same time as M receives *message* 1. Y can prove the following statement by applying the accountability postulate and **A1**: Y CanProve (X *says* P_X) and (P_X isTrusted). When a suspicion is issued against P_X, this statement can be used as evidence to prove (P_X isTrusted). This is the accountability goal **G3**.

Message 3: *Message* 3 is required when Assumption 3 is made. X will periodically request *message* 3 from M. Since X knows its total power consumption $cost_{ab}$ during the period from t_a to t_b, X can verify $E_X(t)$ and $G_X(t)$ by comparing their summation with $cost_{ab}$. *Faulty(M)* will be issued if the result is not equal. Although X could be compromised, at least we know that there must be a *faulty* node between X and M. Further investigation is needed here. This is the accountability goal **G2**. Then, X can prove the following statement by applying the accountability postulate, **A2**, and **A3**: X CanProve ($\{E_X(t), G_X(t), M(t), T(t)\}$ isTrusted). When a suspicion is issued against $E_X(t)$, $G_X(t)$, $M(t)$, and $T(t)$, this statement can be used as evidence to prove ($\{E_X(t), G_X(t), M(t), T(t)\}$ isTrusted).

Message 4: *Message* 4 is similar to *message* 3. By recording *message* 4, Y can prove the following statement by applying the accountability postulate and **A3**: Y CanProve ($M(t)$ isTrusted) and ($T(t)$ isTrusted). When a suspicion is issued against $M(t)$ and $T(t)$, this statement can be used as evidence to prove that they are both trusted. This is also the accountability goal **G2**.

Message 5: *Message* 5 is a key to achieving accountability goal **G3**. When Y receives *message* 5, D_Y will process the auditing of this *message*. Together with the statements from *messages* 2 and 4, Y can eventually prove the following statement by applying the accountability postulate and **A4**: Y CanProve (X *is faulty or correct*). By combining all such statements from every appliance, the accountability goal **G2** will also be achieved. That is, if no *suspected* signal is issued among appliances, the total power consumption of all appliances should equal to the reading of M. *Faulty(M)* will be issued if they are not matched.

Message 6: Through checking the difference between $G(t)$ and the summation of $G_i(t)$ for each appliance i, S can easily verify whether the home power supply is correctly recorded by M. Hence, we have the following statement: S CanProve ($G(t)$ isTrusted). If the above checking fails, S can directly issue a *faulty(M)* signal against M. Otherwise, S will further check $E(t)$ with its supply records, if

possible. For most situations, the supply records are solely based on previous readings from M. How to determine if the M is misbehaving varies on different utilities' policies. If there is a suspicion, S can retrieve all log files of home appliances to see whether $E(t)$ is correctly recorded. By this means, S can prove the following statement by using the *message* 6: S CanProve (M *is faulty or correct*). This is the accountability goal **G4**.

B. HAN Scheme Simulation

In this section, we simulate our protocol running in HAN. Note that (4) and (5) are time-sensitive functions. Different time periods may cause distinct service amounts. If the smart meter has not synchronized the witness' local time, the witness' calculation result by (4) could be different from the service amount in *message* 5. Therefore, this witness could issue a false report against a correct *principal*. One possible solution to address this problem is the threshold mechanism. By using a predefined value Δ, witnesses will issue a *faulty(i)* only when the difference of two service amounts [one from (4) and another from (5)] exceeds Δ. In order to choose a better value for Δ to minimize the number of false reports, we need to evaluate the accuracy of detection for *faulty principals* on different Δ. Throughout this section, we also simulate our protocol to evaluate its scalability in terms of the average message delay, amount of network traffic, and disk space per witness.

We use the discrete event simulation method to simplify our experiment. Specifically, we deploy α (e.g., $\alpha = 10$, 20, 50, and 100) smart appliances and one smart meter in HAN. Each appliance has β (e.g., $\beta = 3$, 4, and 5) witnesses and can communicate with the smart meter directly. We assume that all *principals* are in the same communication range. The distance between any two *principals* is one hop. No forwarding is necessary in our scenario. This is a reasonable assumption due to the limited space in a home area.

The constant capacity factor P_i is randomly selected from 0.1 to 1 kW. Each appliance will be turned on or off at short intervals. This process will follow a Poisson distribution, whose mean value is uniformly distributed in an hour for each appliance. In addition, witnesses will challenge each observed appliance every few hours. It is also a Poisson process with a mean interval time of γ (e.g., $\gamma = 1, 1.5, 2 \ldots$) hours. A challenge event will only be processed when both observed *principal* and its witness are in running status. If the observed *principal* is off, the witness will postpone its scheduled challenge time for an hour.

For simplicity reasons, we do not consider the home power supply. Hence, there is no trading part in our simulation. The market price $M(t)$ is a hourly based discrete function. According to the DOE report [20], the peak price is 20 cents/kWh, and the minimum price is 7 cents/kWh. We also do not consider the propagation time in our environment. Therefore, the propagation time is assumed to be zero.

For every evaluated situation, we run 100 times, 500 time units (e.g., virtual hours) at a time, and take the average value of the outputs as our results. The simulation platform is 64-b Windows 7, 2-GB RAM, and Intel Core 2 6400 2.13-GHz CPU.

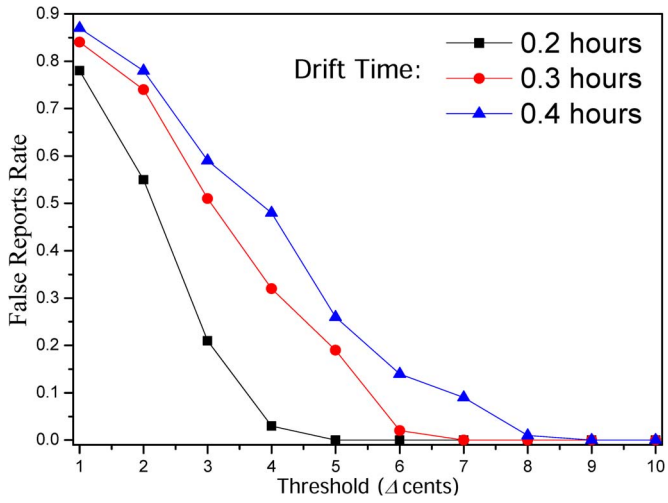


Fig. 10. Simulation results on threshold effect.

1) Accountability Versus Threshold Value: The threshold directly affects the judgment of a witness. In order to evaluate what is a good threshold, we set different Δ values and measure the number of false reports under different conditions. If the rate of false reports goes to zero, that means that we find the right threshold value for Δ.

Different wired or wireless devices may have distinct local times with a certain timer resolution. One may be slower or faster than another. Temporal records therefore may vary from each individual. In order to simulate distinct local times for different *principals*, we adopt the time-driven simulation method [21]. That is, the drift clock for each *principal* is subject to three factors: $offset$, $skew$, and $drift$. If current system time is t, the drift clock $D(t)$ can be presented as

$$D(t) = offset + skew \times t + drift \times t^2. \tag{6}$$

Therefore, the local time $L(t)$ can be obtained by

$$L(t) = t + D(t) = offset + (skew + 1) \times t + drift \times t^2. \tag{7}$$

As we can see, the three factors have the capability of being positive or negative. In our simulation, all $offset$ values are uniformly distributed between -0.2 and 0.2, all $skew$ values are uniformly distributed between -0.002 and 0.002, and all $drift$ values are uniformly distributed between -0.0002 and 0.0002. The reference clock is the smart meter's local time. In fact, the difference between two service amounts derives from the time drift of the objects and its witness. Intuitively, the maximum value of the difference is the peak price ($0.2/kWh) times the maximum drift time (0.4 h) times the maximum constant capacity factor (1 kW). Hence, we set the threshold value between 1 cent and 10 cents (around the maximum value of 8 cents).

Suppose that all *principals* are *correct*. If there are n packets of *message* 5 in the simulation and $m (m < n)$ packets have been reported as *suspected* by witnesses, the rate of false reports is defined as m/n. We set $\alpha = 10$, $\beta = 3$, and $\gamma = 1$. As shown in Fig. 10, with the increase in value of threshold Δ from 1 cent to 10 cents, the rate of false reports gradually approaches

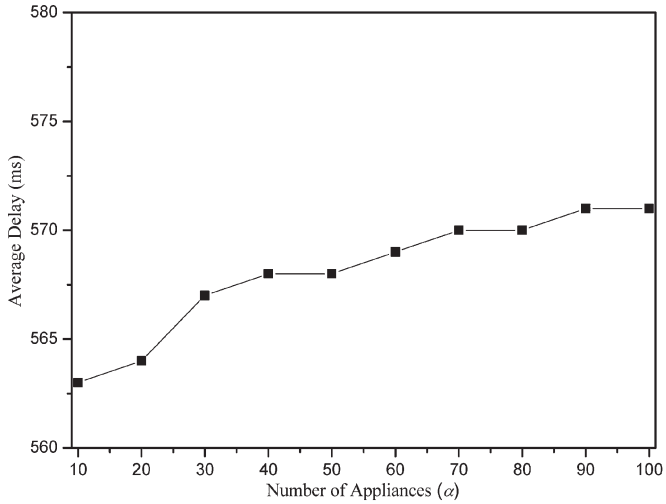


Fig. 11. Simulation results on average message delay in smart meter.

to 0%. When the maximum *drift* time increases, the best value for Δ is increased as well. This is in accordance with what we thought. That is, the threshold value Δ should be bigger than the maximum product value of the drift time, the constant capacity factor, and the peak price.

2) Average Message Delay: Suppose that the average access time for retrieving some data from the log file is 500 ms and the average processing time (e.g., calculating the service amount, send message, etc.) is 50 ms. Messages will be queued in the buffer area when another message is sending. Due to the fact that witnesses will issue challenge messages at hourly based intervals, the message delay in milliseconds will not impact the performance of the smart appliance. We therefore only examine the message delay brought by the smart meter. If x *messages* have been processed by the smart meter and the total delay time is y ms, the average message delay is defined as y/x.

We set $\beta = 3$, and $\gamma = 1$. As Fig. 11 depicts, with the increase of α from 10 to 100, the average delay is slight; it is in milliseconds and less than a second. Since the number of appliances in most families is less than 100, this result indicates that our protocol is scalable in terms of average message delay.

3) Network Traffic: We measure the network traffic as the average number of *messages* that have been sent during one unit time (e.g., a virtual hour). At first, we set $\alpha = 20$, $\beta = 3$, and $\gamma = 1$. Then, we only adjust one parameter and let the other two remain the same. As Fig. 12(a) and (b) depicts, with the increase of α (from 20 to 100) and β (from 3 to 10), the total number of *messages* grows linearly. However, the upper bound of the network traffic in each case is just thousands of *messages* per hour. It becomes acceptable for communication in a home area. As shown in Fig. 12(c), with the increase of γ (from 0.1 to 1), the total number of *messages* decreased logarithmically. Since γ is the mean interval time for sending challenge *messages*, this curve indicates that the larger the interval, the lower the number of challenges in a unit time. Typically, the interval time will be set at least 0.5 h. Only thousands of *messages* occur in an hour. This result indicates that our protocol is scalable in terms of network traffic.

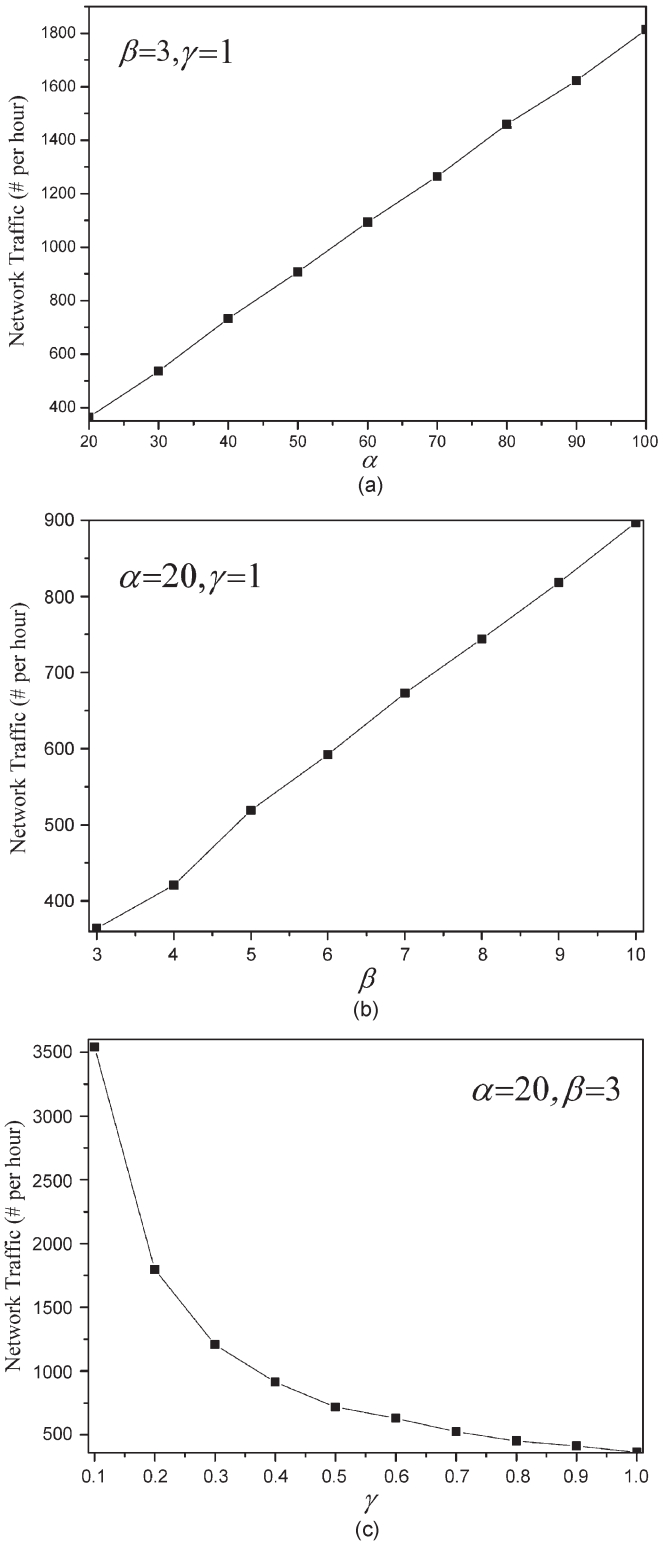


Fig. 12. Simulation results on network traffic effect. (a) α effects. (b) β effects. (c) γ effects.

4) Disk Space: Suppose that each log entry will occupy one unit (e.g., 8 kb) of disk space. According to our protocol, the log entry could be the running state $R_i(t)$, market price $M(t)$, and own power consumption. For each *principal*, the size of the log files for the market price and own power consumption is a fixed value during one time unit (e.g., hourly). Only the log for

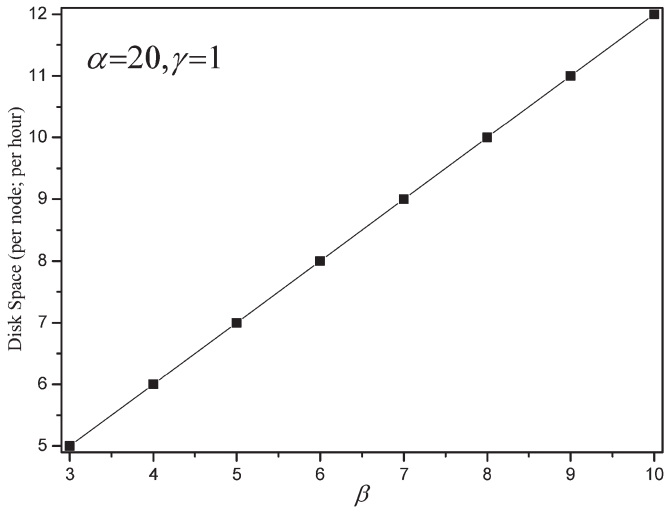


Fig. 13. Simulation results on disk space effect.

the running state of the observed *principal* will affect the disk space of that witness node. Therefore, we set $\alpha = 20$ and $\gamma = 1$ and then measure the disk space on different value of β.

Fig. 13 shows the average logging space (in unit size) in a smart appliance that has been used during 1 h. As we can see, the disk space grows linearly with the increase of the number of witnesses. Nevertheless, only several space units are used during 1 h. If a unit is 8 kb, it will take a week to occupy a 1-MB-size disk space for logging. In addition, the smart appliance can clear a portion of log files after a period (e.g., monthly). Hence, the usage of disk space is acceptable in HAN. This result indicates that our protocol is scalable in terms of disk space usage.

C. NAN Scheme Analysis

As we may see, λ witnesses in the fuse box can at most divide a group of household meters into 2^λ subgroups. Since every household meter should have at least one witness, the number of valid subgroups is $2^\lambda - 1$ (empty subgroup is eliminated). As shown in Fig. 9, every regrouping will cause at most $2^\lambda - 1$ branches for one *suspected* group. The architecture is similar to a classical data structure—B-tree. Each node (aka. subgroup) in the tree has at most $2^\lambda - 1$ children. In the first level of the tree, every node has at most $\mu/(2^\lambda - 1)$ meters inside. In the second level, the number goes down to $\mu/(2^\lambda - 1)^2$ for each node. If the tree height is h, we have $\mu/(2^\lambda - 1)^h = 1$. Thus, we may reasonably draw the conclusion that finding one *faulty* meter should cost $O(h) = \mathrm{O}(\log^{\mu}_{2^\lambda - 1})$ time. In a NAN, the number of household meters μ is typically less than 10 000. In essence, it only requires less than six times of regrouping to find a *faulty* meter if λ is equal to 2 or 3. However, if there is more than one *faulty* meter in the NAN, things become much more complicated. The running time for searching the *faulty* meters depends on a variety of factors, such as the number of witnesses (λ), the number of household meters (μ), and the way to do the regrouping. We will analyze it in Section V-D.

Similarly, based on the logic described in [17], we can prove that our protocol can achieve all accountability goals by using the message interpretation and the initial assumptions.

Our goal is to find the *faulty* meters in a NAN. Suppose that x is any household meter in a NAN and that W is x's witness. The goals can therefore be described as follows: **G1**: M CanProve (x *is faulty* or *correct*); **G2**: W CanProve (x *is suspected or correct*).

Since an unsigned *message* has no effect on the achievement of goals in accountability logic, we only consider signed ones. The *message* flows can therefore be interpreted as follows: ***Message 1***: x Receives ($\{P_x\}$ SignedWith K_M^{-1}); ***Message 2***: x Receives ($\{t_a, t_b\}$ SignedWith K_W^{-1}); ***Message 3***: W Receives ($\{t_a, t_b, E_x(t)\}$ SignedWith K_{Px}^{-1}); ***Message 4***: M Receives ($\{t_a, t_b, E_W(t), \{t_a, t_b, E_x(t)\}$ SignedWith$K_{Px}^{-1}\}$ SignedWith K_W^{-1}).

The initial state assumptions required in the analysis are as follows: **A1**: M Receives ($\{P_x\ is\ faulty\}$ SignedWith K_W^{-1}) => (M CanProve($P_x\ is\ faulty$)); **A2**: W Receives ($\{t_1, t_2, E_x(t)\}$ SignedWith K_{Px}^{-1}) => (W CanProve(x *is suspected or correct*)). Note that **A2** will use "intersected grouping" technique to check whether P_x is in a suspected group or not.

Message 1: When x receives *message* 1, x knows that it was sent by M based on its unique signature. After that, x can use P_x as its pseudonym to communicate with other meters. Since W also knows that P_x is one of its observation objects, if P_x does not respond to W's request/challenge, W can claim that P_x is *faulty*. It will be sent to M for further verification. By applying the accountability postulate [18], [19] and **A1**, we have the following: M CanProve (W *says* P_x *is faulty*) and (P_x *is faulty*). When *suspected* is issued against P_x, the above statement can be used as evidence to prove (x *is faulty*). This is the accountability goal **G1**.

Message 2: W will periodically broadcast *message* 2 to all of its observation objects. Since x knows that its pseudonym is P_x, it will be received by x. Other meters who got this broadcast *message* will discard it. When W does not get any response from P_x after a given time, this *message* can be served as an evidence to prove (P_x is *suspected*). This is the accountability goal **G2**.

Message 3: *Message* 3 is a key to achieving accountability goal **G2**. When W receives *message* 3 from all its observation objects within a given time, W will process the auditing procedure. If there is any one missing (possibly too much delay) or one whose time stamps (e.g., t_a and t_b) do not match its corresponding challenge *message*, W can directly claim the following statement: W CanProve (x *is suspected*). Otherwise, the auditing procedure will adopt the aforementioned "intersected grouping" technique to filter out *suspected* meters. Given enough time, W can eventually prove the following statement by applying the accountability postulate and **A2**: W CanProve (x *is suspected or correct*).

Message 4: When x is *suspected*, its witness W will notify M with *message* 4. If there is only one *suspected* household meter, M can directly claim the following statement: M CanProve (x *is faulty*). For those meters in *correct* groups,

we have the following: M CanProve (x *is correct*). Otherwise, M will reassign all *suspected* meters to λ witnesses for further checking. *Message* 4 becomes the evidence against *faulty* meters. By combining all such statements from every witness, the accountability goal **G1** will be achieved: M CanProve (x *is faulty or correct*).

D. NAN Scheme Simulation

One goal in this paper is to achieve accountability in the NAN. As we can see, it relies on witnesses' observations and undeniable log files. The logic proof has been given in Section V-C for the log file exchanging protocol. The remaining part of this section should evaluate the performance of witnesses' observations. According to the regrouping times and hitting ratio (percentage of *faulty* meters in a *suspected* group), we analyze the performance of our grouping algorithm in different scenarios.

We use the GROUP function described in Section IV-D for our experiment. Specifically, we deploy λ (e.g., $\lambda = 2, 3, 4$, and 5) witnesses and μ (e.g., $\mu = 10^2, 10^3, 10^4$, and 10^5) household meters in a NAN. According to our test cases, manually set τ (e.g., $\tau = 1, 2, 3, 4$, and 5) meters' readings different from their actual consumptions, denoted as *faulty* meters. There is only one master meter in the fuse box that manages all λ witnesses. Each witness is able to communicate with any household meter directly. No matter how they communicate, either via wireless or wired channel or private or public network, the *message* will be eventually delivered, safely and in a timely manner.

For simplicity reasons, we assume that all meters' local time is synchronized. Because meters barely have constraints on power and computing resources, it may be easily achieved by a variety of time synchronization methods in computer networks. In addition, we assume that there is no power loss during distribution and no prorogation delay. To remove this assumption, one may simply adopt a predefined threshold and minimize the false report as we did in Section V-B. Here, we only focus on more important aspects of our protocol.

For every evaluated situation, we run 100 times, 500 time units (e.g., virtual hours) at a time, and take the average value of the outputs as our results. The simulation platform is 64-b Windows 7, 2-GB RAM, and Intel Core 2 6400 2.13-GHz CPU.

1) Performance in Unlimited Time: Given unlimited time, witnesses can eventually find out all *faulty* meters. To evaluate the performance under different scenarios, we use the total times of regrouping as a "criterion." Apparently, less regrouping time means better performance on finding the *faulty* meters.

Typically, the number of household meters in a NAN is ranging from 10^2 to 10^5. We deploy a small number (e.g., 2 to 5) of witnesses in the fuse box to monitor the NAN. As shown in Fig. 14, if there are less than five *faulty* meters in a NAN, the average regrouping time is no more than 62. It seems unacceptable in reality when we challenge *suspected* meters every 1 h for regrouping. The worst case will cost three days to locate all *faulty* ones. However, as we can see, about 73.4% (i.e., 47 out of 64) of cases can be done within a day, which is somehow tolerable for most situations. In particular, if there is only one *faulty* meter in the NAN, our algorithm is able to find it

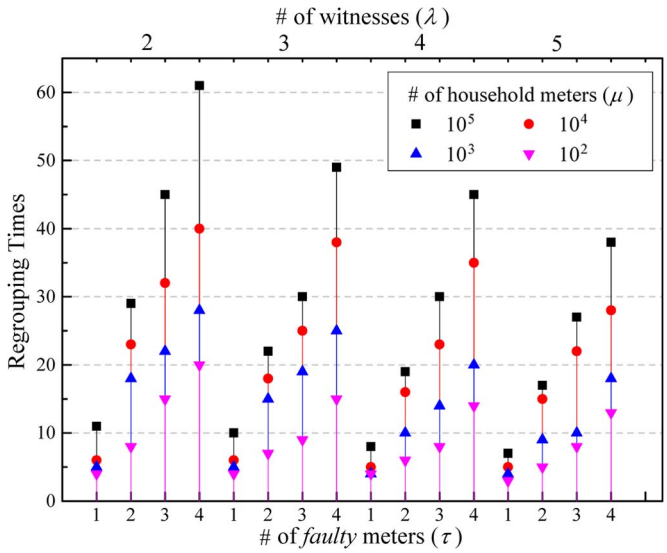


Fig. 14. Performance in unlimited time with little witnesses.

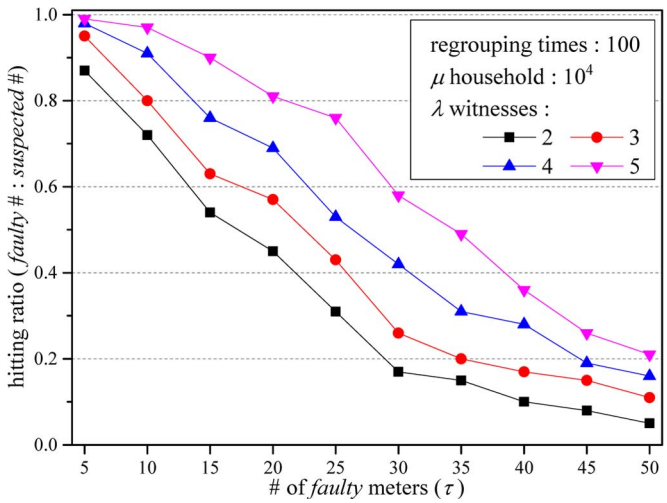


Fig. 15. Performance in limited time with different number of witnesses.

with average time of 6 h. When the number of household meters (on each vertical line) increases, the average time of regrouping goes up as well. When the number of *faulty* meters increases by one, the regrouping time could be doubled. Based on the simulation result, we may claim that our algorithm works well when there are only a few *faulty* meters in the NAN.

2) Performance in Limited Time: In fact, we do not know how many *faulty* meters are out there at the beginning. If there are plenty, our algorithm may cost days to get the result. It is absolutely not acceptable. One solution is to set a timer for the program. Within a given time, witnesses may not find out all *faulty* meters. However, returning a small group of *suspected* meters is tolerable. We could manually check those meters using our traditional way. To evaluate the performance in such case, we use the hitting ratio (i.e., number of *faulty* meters/ number of *suspected* meters) as a "criterion." Apparently, a higher hitting ratio means better performance on finding the *faulty* ones.

In our simulation, the NAN has ten thousands of household meters, which is a very typical case for a community. The timer

is set as 100 regrouping times, which could be up to four days in reality. When the time is up, we calculate the hitting ratio under different scenarios. As we can see in Fig. 15, the ratio drops quickly as the number of *faulty* meters grows up. Adding a witness only gains 10% to 20% hitting ratio at a time, but it is not an economic solution. When the number of *faulty* meters is above 15, the ratio could be less than 60%. Hence, the grouping algorithm only works for a small number of *faulty* meters. A more sophisticated approach should be studied in the future work.

VI. Conclusion

A feasible architectural framework for the smart grid in HAN and NAN has been presented based on the NIST smart grid interoperability standards (release 1.0). This paper has designed two accountable communication protocols for HAN and NAN using the proposed architecture with certain reasonable assumptions. Analysis and simulation results are indicative that such a design works well and it makes all power loads in HAN and NAN accountable.

References

[1] Cisco Systems, Inc., "Internet protocol architecture for the smart grid," White Paper, Jul. 2009. [Online]. Available: http://www.cisco.com/web/strategy/docs/energy/CISCO_IP_INTEROP_STDS_PPR_TO_NIST_WP.pdf

[2] U.S. DOE, "Smart grid system report," White Paper, Jul. 2009. [Online]. Available: http://www.oe.energy.gov/SGSRMain_090707_lowres.pdf

[3] U.S. NETL, "Advanced metering infrastructure," White Paper, Feb. 2008. [Online]. Available: http://www.smartgrid.gov/white_papers

[4] U.S. NIST, "NIST framework and roadmap for smart grid interoperability standards, release 1.0," NIST Special Publication 1108, Jan. 2010. [Online]. Available: http://www.smartgrid.gov/standards/roadmap

[5] "West Virginia Smart Grid Implementation Plan," West Virginia Div. Energy, Charleston, WV, USA, U.S. DOE/NETL Rep., Aug. 2009.

[6] U.S. NETL, "A systems view of the modern grid," White Paper, Jan. 2007. [Online]. Available: http://www.smartgrid.gov/white_papers

[7] A. Clark and C. J. Pavlovski, "Wireless networks for the smart energy grid: Application aware networks," in *Proc. IMECS*, 2010, pp. 1243–1248.

[8] J. Gadze, "Control-aware wireless sensor network platform for the smart electric grid," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 9, no. 1, pp. 16–26, Jan. 2009.

[9] D. Dvian and H. Johal, "A smart grid for improving system reliability and asset utilization," in *Proc. CES/IEEE 5th Int. Power Electron. Motion Control Conf.*, Shanghai, China, Aug. 2006, pp. 1–7.

[10] G. N. Srinivasa Prasanna, A. Lakshmi, S. Sumanth, V. Simha, J. Bapat, and G. Koomullil, "Data communication over the smart grid," in *Proc. ISPLC*, Dresden, Germany, 2009, pp. 273–279.

[11] H. A. Khan, Z. Xu, H. Iu, and V. Sreeram, "Review of technologies and implementation strategies in the area of smart grid," in *Proc. 10th Postgraduate Elect. Eng. Comput. Symp.*, Perth, Australia, Oct. 2009, pp. 1–6.

[12] A. Cavoukian, J. Polonetsky, and C. Wolf, "SmartPrivacy for the smart grid: Embedding privacy into the design of electricity conservation," in *Identity in the Information Society*. Dordrecht, Netherlands: Springer-Verlag, Apr. 2010.

[13] S. Spoonamore and R. L. Krutz, Smart Grid and Cyber Challenges—National Security Risks and Concerns, Mar. 2009. [Online]. Available: http://www.whitehouse.gov/files/documents/cyber/Spoonamore-Krutz—Smart Grid CyberSecurity Risks and Concerns.pdf

[14] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, May/Jun. 2009.

[15] W. F. Boyer and S. A. McBride, "Study of Security Attributes of Smart Grid Systems—Current Cyber Security Issues," Idaho Nat. Lab., Critical Infrastructure Protection/Resilience Center, Idaho Falls, ID, USA, DOE Scientific/Tech. Inf. Rep., Apr. 2009.

[16] R. Kailar, "Accountability in electronic commerce protocols," *IEEE Trans. Softw. Eng.*, vol. 22, no. 5, pp. 313–328, May 1996.

[17] M. Kudo, "Electronic submission protocol based on temporal accountability," in *Proc. 14th Annu. Comput. Secur. Appl. Conf.*, 1998, pp. 353–363.

[18] H. Chao, "Price-responsive demand management for a smart grid world," *Elect. J.*, vol. 23, no. 1, pp. 7–20, Jan./Feb. 2010.

[19] A. Haeberlen, P. Kouznetsov, and P. Druschel, "PeerReview: Practical accountability for distributed systems," *ACM SIGOPS Oper. Syst. Rev.*, vol. 41, no. 6, pp. 175–188, Dec. 2007.

[20] U.S. DOE, Average Retail Price of Electricity to Ultimate Customers by End-Use Sector, by State, Nov. 2010. [Online]. Available: http://www.eia.doe.gov/electricity/epm/table5_6_b.html

[21] Y. Quan and G. Liu, "Drifting clock model for network simulation in time synchronization," in *Proc. 3rd Int. Conf. Innovative Comput. Inf. Control*, Dalian, China, Jun. 2008, pp. 385–389.

[22] A. Faruqui, R. Hledik, and S. Sergici, "Piloting the smart grid," *Elect. J.*, vol. 22, no. 7, pp. 55–69, Aug./Sep. 2009.

[23] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Proc. 1st IEEE Int. Conf. SmartGridComm*, Gaithersburg, MD, Oct. 2010, pp. 232–237.

[24] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. 1st IEEE Int. Conf. SmartGridComm*, Gaithersburg, MD, Oct. 2010, pp. 238–243.

[25] J. Liu, Y. Xiao, and J. Gao, "Accountability in smart grids," in *Proc. IEEE IEEE, Smart Grids Special Session*, 2011, pp. 1166–1170.

[26] J. Liu and Y. Xiao, "An accountable neighborhood area network in smart grids," in *Proc. EMC*, 2012, pp. 171–178.

[27] Z. Xiao, Y. Xiao, and D. Du, "Building accountable smart grids in neighborhood area networks," in *Proc. IEEE GLOBECOM*, 2011, pp. 1–5.

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

[29] Z. Xiao, Y. Xiao, and D. Du, "Exploring malicious meter inspection in neighborhood area smart grids," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 214–226, Mar. 2013.

[30] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 981–997, Fourth Quarter 2012.

[31] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. L. P. Chen, "A survey of communication/networking in smart grids," *Future Gener. Comput. Syst.*, vol. 28, no. 2, pp. 391–404, Feb. 2012.

[32] J. Gao, J. Liu, B. Rajan, R. Nori, B. Fu, Y. Xiao, W. Liang, and C. L. P. Chen, "SCADA communication and security issues," *Security Commun. Netw.*, DOI: 10.1002/sec.698, to be published.

[33] Y. Xiao, Ed., *Communication and Networking in Smart Grids*. Boca Raton, FL, USA: CRC Press, 2012.

[34] Y. Xiao, Ed., *Security and Privacy in Smart Grids*. Boca Raton, FL, USA: CRC Press, 2012.

[35] Y. Xiao, "Editorial," *Int. J. Security Netw.*, vol. 6, no. 1, pp. 1–1, 2011.

[36] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards modelling the impact of cyber attacks on a smart grid," *Int. J. Security Netw.*, vol. 6, no. 1, pp. 2–13, Apr. 2011.

[37] G. Kalogridis, S. Z. Denic, T. Lewis, and R. Cepeda, "Privacy protection system and metrics for hiding electrical events," *Int. J. Security Netw.*, vol. 6, no. 1, pp. 14–27, Apr. 2011.

[38] F. Li, B. Luo, and P. Liu, "Secure and privacy-preserving information aggregation for smart grids," *Int. J. Security Netw.*, vol. 6, no. 1, pp. 28–39, Apr. 2011.

[39] J. Zhang and C. A. Gunter, "Application-aware secure multicast for power grid communications," *Int. J. Security Netw.*, vol. 6, no. 1, pp. 40–52, Apr. 2011.

[40] Y. Xiao, "Editorial," *Int. J. Security Netw.*, vol. 7, no. 2, pp. 71–72, Oct. 2012.

[41] N. B. Neji and A. Bouhoula, "Managing hybrid packet filter's specifications," *Int. J. Security Netw.*, vol. 7, no. 2, pp. 73–82, Oct. 2012.

[42] Z. A. Baig, "Rapid anomaly detection for smart grid infrastructures through hierarchical pattern matching," *Int. J. Security Netw.*, vol. 7, no. 2, pp. 83–94, Oct. 2012.

[43] S. Boyer, J. Robert, H. Otrok, and C. Rousseau, "An adaptive tit-for-tat strategy for IEEE 802.11 CSMA/CA protocol," *Int. J. Security Netw.*, vol. 7, no. 2, pp. 95–106, Oct. 2012.

[44] I. Butun, Y. Wang, Y. Lee, and R. Sankar, "Intrusion prevention with two level user authentication in heterogeneous wireless sensor networks," *Int. J. Security Netw.*, vol. 7, no. 2, pp. 107–121, Oct. 2012.

[45] V. Kolesnikov and W. Lee, "MAC aggregation resilient to DoS attacks," *Int. J. Security Netw.*, vol. 7, no. 2, pp. 122–132, Oct. 2012.

[46] D. Wong and X. Tian, "E-mail protocols with perfect forward secrecy," *Int. J. Security Netw.*, vol. 7, no. 1, pp. 1–5, Aug. 2012.
[47] L. J. Vespa, R. Chakrovorty, and N. Weng, "Lightweight testbed for evaluating worm containment systems," *Int. J. Security Netw.*, vol. 7, no. 1, pp. 6–16, Aug. 2012.
[48] F. Kandah, Y. Singh, W. Zhang, and T. Wang, "A misleading active routing attack in mobile ad-hoc networks," *Int. J. Security Netw.*, vol. 7, no. 1, pp. 17–29, Aug. 2012.
[49] K. Alsubhi, Y. Alhazmi, N. Bouabdallah, and R. Boutaba, "Security configuration management in intrusion detection and prevention systems," *Int. J. Security Netw.*, vol. 7, no. 1, pp. 30–39, Aug. 2012.
[50] Z. Xiao and Y. Xiao, "PeerReview re-evaluation for accountability in distributed systems or networks," *Int. J. Security Netw.*, vol. 7, no. 1, pp. 40–58, Aug. 2012.
[51] Z. S. Al-Salloum, "Defensive computer worms: An overview," *Int. J. Security Netw.*, vol. 7, no. 1, pp. 59–70, Aug. 2012.
[52] J. Gao and Y. Xiao, "Design for accountability in multi-core networks," *J. Convergence*, vol. 3, no. 3, pp. 9–16, Sep. 2012.
[53] D. Takahashi, Y. Xiao, and K. Meng, "Virtual flow-net for accountability and forensics of computer and network systems," *Int. J. Security Netw.*, 2011, DOI: 10.1002/sec.407, to be published.
[54] Y. Xiao, S. Yue, B. Fu, and S. Ozdemir, "Global view: Building global view with log files in a distributed/networked system for accountability," *Int. J. Security Netw.*, 2011, DOI: 10.1002/sec.374, to be published.
[55] Y. Xiao, K. Meng, and D. Takahashi, "Accountability using flow-net: Design, implementation, performance evaluation," *Int. J. Security Netw.*, vol. 5, no. 1, pp. 29–49, Jan. 2012.
[56] J. Liu and Y. Xiao, "Temporal accountability and anonymity in medical sensor networks," *Mobile Netw. Appl.—Special Issue: Wireless Personal Communications*, vol. 16, no. 6, pp. 695–712, Dec. 2011.
[57] Y. Xiao, "Flow-net methodology for accountability in wireless networks," *IEEE Network*, vol. 23, no. 5, pp. 30–37, Sep. 2009.
[58] K. Meng, Y. Xiao, and S. V. Vrbsky, "Building a wireless capturing tool for WiFi," *Int. J. Security Netw.*, vol. 2, no. 6, pp. 654–668, Nov./Dec. 2009.
[59] Y. Xiao, "Accountability for wireless LANs, ad hoc networks, wireless mesh networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 116–126, Apr. 2008.
[60] D. Takahashi and Y. Xiao, "Retrieving knowledge from auditing log files for computer and network forensics and accountability," *Int. J. Security Netw.*, vol. 1, no. 2, pp. 147–160, Mar./Apr. 2008.

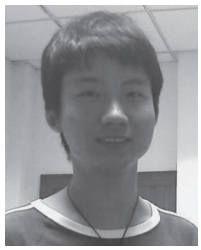
Jing Liu received the B.Sc. and M.Sc. degrees from the Hunan University, Changsha, China, in 2005 and 2008, respectively. He is currently working toward the Ph.D. degree in the Department of Computer Science, The University of Alabama, Tuscaloosa, AL, USA.

He is an active researcher in the area of network security, bioinspired network, and telemedicine, including botnet issues, visual attention, anonymous communication, and accountability in telemedicine.

Yang Xiao (SM'04) received the M.S. and Ph.D. degrees in computer science and engineering from Wright State University, Dayton, OH, USA.

He worked in industry as a Medium Access Control Architect involving the IEEE 802.11 standard enhancement work before he joined the Department of Computer Science, The University of Memphis, Memphis, TN, USA, in 2002. He is currently a Professor with the Department of Computer Science, The University of Alabama, Tuscaloosa, AL, USA. 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. His research has been supported by the U.S. National Science Foundation (NSF), U.S. Army Research, The Global Environment for Network Innovations, Fleet Industrial Supply Center-San Diego, FIATECH, and The University of Alabama's Research Grants Committee. He currently serves as the Editor-in-Chief for the *International Journal of Security and Networks* and *International Journal of Sensor Networks* (SCI-index) (Impact Factor: 1.386 for 2011). He was the founding Editor-in-Chief for the *International Journal of Telemedicine and Applications* (2007–2009).

Dr. Xiao was a voting member of the IEEE 802.11 Working Group from 2001 to 2004. He serves as a panelist for the U.S. NSF, Canada Foundation for Innovation's Telecommunications expert committee, and the American Institute of Biological Sciences, as well as a referee/reviewer for many national and international funding agencies.



Jingcheng Gao is currently working toward the Ph.D. degree in the Department of Computer Science, The University of Alabama, Tuscaloosa, AL, USA.

His research interests include smart grids, security, and computer networks.