Smart Grid and Renewable Energy, **2013, 4, 313-324**
http://dx.doi.org/10.4236/sgre.2013.44038 Published Online July 2013 (http://www.scirp.org/journal/sgre)

Privacy Preservation Scheme for Multicast Communications in Smart Buildings of the Smart Grid

Depeng Li[1], Zeyar Aung[1], Srinivas Sampalli[2], John Williams[3], Abel Sanchez[3]

[1]Computing and Information Science Program, Masdar Institute of Science and Technology, Abu Dhabi, UAE; [2]Faculty of Computer Science, Dalhousie University, Halifax, Canada; [3]Massachusetts Institute of Technology (MIT), Cambridge, USA.
Email: dli@masdar.ac.ae, zaung@masdar.ac.ae, srini@cs.dal.ca, jrw@mit.edu, doval@mit.edu

Received January 10th, 2013; revised February 10th, 213; accepted February 18th, 2013

ABSTRACT

Privacy preservation is a crucial issue for smart buildings where all kinds of messages, e.g., power usage data, control commands, events, alarms, etc. are transmitted to accomplish the management of power. Without appropriate privacy protection schemes, electricity customers are faced with various privacy risks. Meanwhile, the natures of smart grids and smart buildings—such as having limited computation power of smart devices and constraints in communication network capabilities, while requiring being highly reliable—make privacy preservation a challenging task. In this paper, we propose a group key scheme to safeguard multicast privacy with the provisions of availability, fault-tolerance, and efficiency in the context of smart buildings as a part the smart grid. In particular, hybrid architecture accommodating both centralized and contributory modes is constructed in order to achieve both fault-tolerance and efficiency with only one set of group key installed. Key trees are sophisticatedly managed to reduce the number of exponentiation operations. In addition, an individual rekeying scheme is introduced for occasional joining and leaving of member smart meters. Experimental results, on a simulation platform, show that our scheme is able to provide significant performance gains over state-of-the-art methods while effectively preserving the participants' privacy.

Keywords: AMI; Building Area Networks; Group Key; Multicasting; Privacy; Smart Building; Smart Grid

1. Introduction

Smart grids, or the intelligent electricity grid that utilize modern IT/communication/control technologies, become a global trend nowadays [1]. As a novel emerging technology of smart grids, Advanced Metering Infrastructure (AMI) is composed of Home Area Networks (HANs), Building Area Networks (BANs), Neighbor Area Networks (NANs) and grid infrastructure which are used to measure, collect, aggregate, store and process data [2,3].

1.1. Motivations

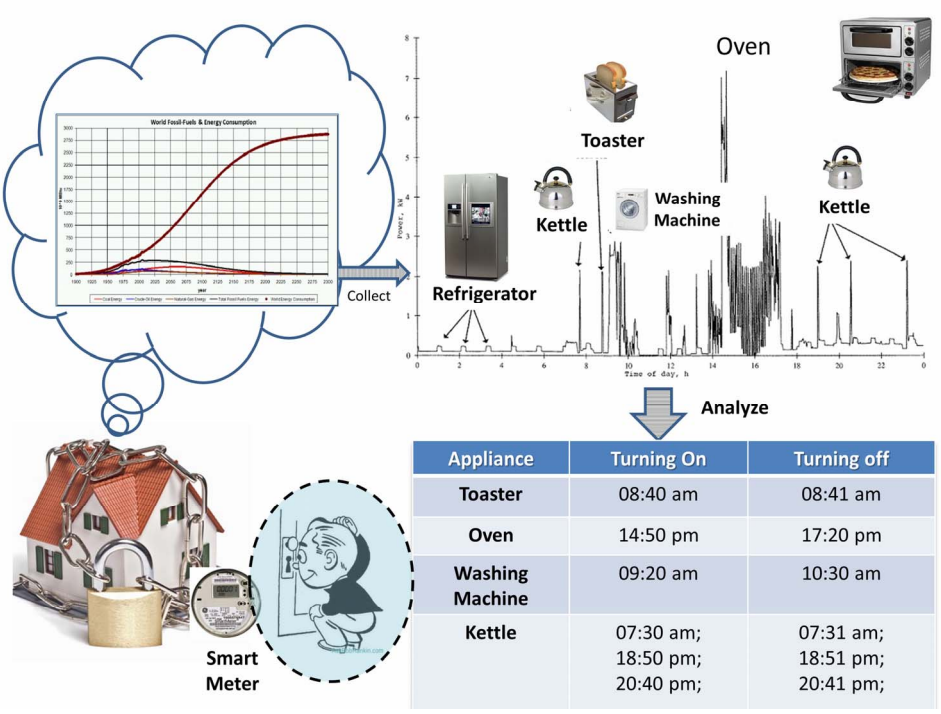
AMI introduces substantial benefits and opportunities to our society, but it also raises challenges concerning privacy as a side effect. For example, fine-grained smart metering data and control messages provide utility companies with the information about ongoing electricity status. However, if misused, these data significantly increase the probability of leaking customers' privacy including personal information, daily activities, individual behaviors, etc., more frequently [4] as shown in **Figure 1**.

Some pioneer studies, e.g. [5], explore means to identify major appliance usages in a building by examining the power usage data collected every 15 minutes within 24 hours. This exposes its residents' daily activities.

To address privacy risks and concerns, most existing researches are more focused on hiding power usage data that is recorded at smart meter ends or unicasted in NAN via encryption schemes [6,7] or perturbation means [8] or extra battery [9]; but they did not take the HAN and BAN and their characteristics into account.

This paper aims to develop an efficient privacy preservation scheme for Communications in Smart Buildings (CSB) in the smart grid, which is still an unexploited area. CSB [3] are consisted of BAN and HAN where resource-constrained wireless networks such as Zigbee [10] and Wi-Fi [11] are deployed. In CSB, not only unicast but broadcast/multicast is popularly utilized due to wireless communications' characteristics. In our viewpoint, the major challenges to preserve privacy in CSB include:

- Requirement of efficient privacy-preserving schemes which should be specifically designed for smart buil-



Appliance	Turning On	Turning off
Toaster	08:40 am	08:41 am
Oven	14:50 pm	17:20 pm
Washing Machine	09:20 am	10:30 am
Kettle	07:30 am; 18:50 pm; 20:40 pm;	07:31 am; 18:51 pm; 20:41 pm;

Figure 1. Privacy leakage in smart grids.

dings;

- Safeguarding of not only unicast but broadcast/multicast for both BAN and HAN in an efficient way;
- Preservation of not only power usage data but other messages in CSB such as power control commands, events, alarms and so on.

1.2. Contributions

We propose a reliable, fault-tolerant, and efficient privacy preserving architecture for CSB in this paper. Our specific contributions are:

Privacy Leakage Modeling: To our best knowledge, this paper is the first to systematically study privacy leakages for CSB. Furthermore, from an adversary's perspective, we practically enumerate privacy threats and illustrate corresponding examples.

Architecture for Privacy Preservation Scheme: Again, we are the first to propose a privacy preservation architecture which is specifically designed for CSB. We analyze the fundamental characteristics of smart buildings, investigate benefits from cryptographic methods and carefully design the most suitable cryptographic components to protect the messages transmitted in smart buildings.

New Group Key Scheme: Directly using the existing raw group key schemes in BAN poses a formidable challenge, namely the need of efficient and reliable group key management for CSB. 1) The nature of smart grid ranks reliability, safety and availability as the highest priorities [12]. Therefore, group key schemes should heavily emphasize the built-in availability as well as minimize the down time during its operation; 2) Most smart devices are equipped with low-capacity devices and limited memory which tends to be restricted in their computation and storage capability. Our group key scheme's contributions are: a) Hybrid architecture with reliability and self-heaing services to incorporate the centralized and the contributory group key scheme in order to achieve fault-tolerance. b) Efficiency is ensured via individual rekeying for members joining and batch rekeying for member leaving at the end of an interval. For even more efficiency, the key tree is organized using special constructs such the fixed and the child key trees.

Experimental Validation: Finally, we implement our scheme on emulated smart devices and key servers as well as simulate it on Network Simulator 2 (NS2) [13]. The experimental results demonstrate that our solution incurs dramatically less computational costs and communication overheads when compared to the state-of-the-art methods.

2. Background and Problem Description

2.1. Structure of Smart Building

As depicted in **Figure 2**, a smart building communication system comprises of components as follows [3]:

- **Smart Appliances or Sensors**

Smart Home Nodes (SHNs) are, generally, embedded devices such as sensors which are located in the customers' premises e.g. an apartment in a smart building. They

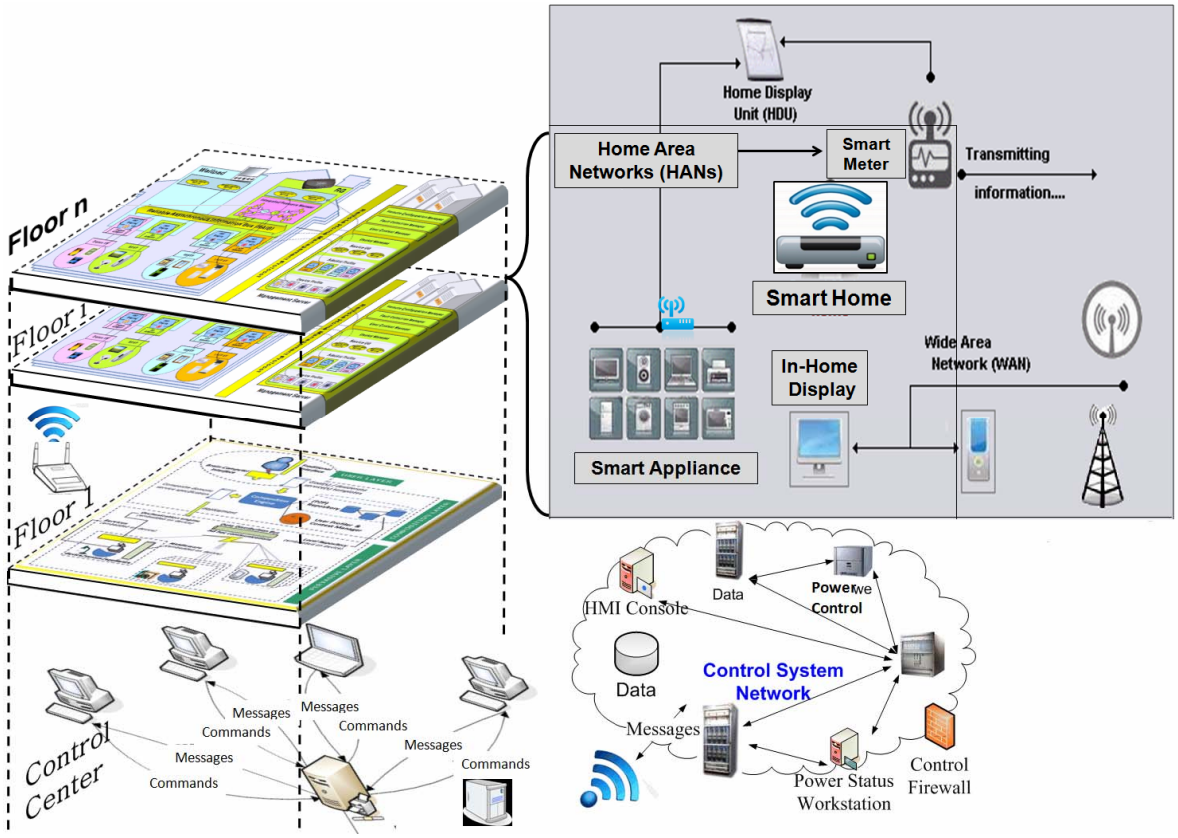


Figure 2. Architecture of communication in smart building.

can be installed at or embedded within a number of smart appliances, e.g., washing machines, dryers, heating, ventilations, refrigerators, air conditioners, In Home Displays (IHDs), and even solar panels as well as wind turbine generators [14]. They are deployed to monitor and control their host smart appliances.

- **Smart Meters**

As a programmable device, the smart meter measures electricity consumption, monitors power status, reports events and remotely enables/disables smart appliances. It also possesses the bi-directional communication functionality to relay the messages from appliance to utilities and vice versa. It enables Demand Response (DR) features which can take charge of appliance control while the system in jeopardy is sensed or at peak times.

- **Control Center in Smart Building**

Generally, there is a control center in smart building to manage the automation control system. In this paper, we will utilize one of the servers/PCs in the control center to play the key server role in our privacy preservation scheme.

- **Home Area Networks (HAN)**

In a smart building, each apartment could construct a HAN, a local area network (LAN) which connects SHNs (e.g. smart appliance, IHDs, local control devices) and smart meters via Zigbee [10] or other cost-saving wireless networks.

- **Building Area Networks (BAN)**

Building Area Networks (BANs) are typically deployed for high rise. A Vertical Back-bone Communication (VBC) [3] system is established for the building to link all smart meters, each of which, generally, measures, controls and connects one HAN. In each floor of the building, the Horizontal Floor Communication (HFC) system [3] is constructed with the utilization of Zigbee to connect each HAN for each apartment in the smart floor.

2.2. Communication in BAN and HAN

Three communication modes are utilized in SGC: unicast, multicast and broadcast [15]. Interactive messages are exchanged via one or more of them. SHNs or smart meters use unicast mode to report metering data such as power usage data, status, and events to utility companies. In contrast, power companies or the smart building control center deploys multicast or broadcast technology to forward control commands to one or more HANs or even the entire BAN in the smart building. Furthermore, DR information including remote load control messages and pricing information and alarms is multicast to corresponding DR project participants.

In terms of the delay limit for message delivery, we

realize that different countries and areas may have their own regulations while accomplishing the multicast/broadcast technologies used in smart buildings. Their values differ. Without lost generality, we follow the standard of State Grid Corporation of China, the time limit of which is defined as less than 15 s [15]. Other countries may set different time limits but it will not impact our solution significantly.

2.3. Problem Description

In CSB, different communication modes demonstrate varied hardness while protecting privacy. Privacy preserving schemes can be easily accomplished for unicast communication technologies even for resource-limited wireless network communication technologies. The reason is that currently deployed wireless networks such as Zigbee [10] or Wi-Fi [11] are utilizing pair-wise keys and encryption algorithms in design. However, it is still a challenge for multicast communication technologies in CSB due to CSB's own characteristics and specific requirements. The SHNs in a HAN, for example, have to share their messages or statuses or events with each other to achieve some collaborative tasks: a DR project, for example, requires an apartment in the building decrease its power consumption to a defined limit at peak time. However, how the customer-side power management in the apartment complete the goal is out of the DR project's knowledge. In this case, the SHNs in the apartment need work with each other to reduce the electricity consumption but meanwhile satisfy customers' comfortableness. It does not conflict with the privacy protection since SHNs in the same HAN belongs to the identical owner. However, these messages cannot be captured by other devices which deployed in the same buildings but different apartment. Otherwise, the privacy leakages discussed in Section 4.2 occur.

However, designing an appropriate privacy preserving scheme for multicast/broadcast in CSB is a challenging task. It should protect aforementioned scenarios and meanwhile overcome the restrictions listed below:

1) Requirement of suitable cryptographic schemes for multicast: current wireless network e.g. Zigbee or Wi-Fi mainly utilizes the pair-wise key scheme and encryption algorithms to protect messages. It is suitable for unicast communications but not for multicast ones. Designing privacy preserving schemes specifically for multicast communications in CSBs is highly demanded.

2) Limited resources for receivers: The receivers, *i.e.*, SHNs or smart meters, are usually equipped with low-end processors and limited amount of memory, both of which hamper the execution of heavy computing operations.

3) Constraints on communication channels: Wireless channels present low-bandwidth. Light-weight communication cost is desirable.

4) Huge volumes of data: the amount of data for smart building communications will be a significant increase in the future. Hence, the solution needs to be efficient and scalable.

5) Delay-tolerance: Data forwarded in smart building communications cannot be delayed for more than 15 s.

6) Vital demands for reliability and fault protection: The nature of smart building highly demands reliability and availability. Hence, to minimize the total outage/fault times, fault-tolerance services are essential.

3. Cryptographic Primitives

3.1. Selection of Group Key Schemes

To satisfy smart grids' privacy-preserving requirement for multicast communications, a common and efficient solution is to deploy a symmetric group key shared by all multicast participants (group members), e.g. SHNs, smart meters, etc. in the same HAN (group). With the support of this shared key (group key), multicast communication data in the same HAN can be encrypted and decrypted. Outsiders, e.g. SHNs in other HANs cannot peek. Therefore, a group key management protocol that computes the symmetric group key and forwards the partial keys to all legitimate SHNs in the HAN is critical to the privacy preservation scheme for the multicast communication in smart buildings.

Rekey Strategies: When one or more SHN (group member) leaves or joins the HAN (group), the group key should be updated so that only current group members contain the group key. This procedure is called *rekey*. There are two kinds of rekey strategies: *individual rekey* and *periodical batch rekey*. The former rekeys the group key for every group membership update such as joining/leaving. The later processes the joining and leaving requests in a batch at the end of each rekey interval.

In this paper, we utilize individual rekeying to process join request and periodical rekeying to process leaving requests because: 1) In smart grids, most SHNs and the smart meter which play group member roles have stationary membership. The group membership change events e.g. joining/leaving are rare; 2) We use one-way hash operation to update the group key when a SHN joins. Since one way hash function is efficient, the rekey operation cost is light; 3) Periodical rekeying introduces a vulnerability window but also leads efficiency. Considering that some SHNs show low-end processing capacity, the tradeoff between performance and security is reasonable; 4) Periodic rekeying introduces group key refresh at the end of the time interval even there are no membership changes. This promotes the security level.

Group Key Management Architecture: In view of

architecture, group key management schemes can be broadly classified into two categories, namely, *centralized* and *contributory*: In a typical centralized group key management scheme e.g. *Logical Key Hierarchy* (LKH) [16], a trusted third party, known as the key server, is responsible to generate, to encrypt and to distribute the symmetric group key, partial keys and individual keys to all other group members. It has the advantages of efficiency of the symmetric key encryption/decryption. However, it suffers from the following drawbacks. 1) Since all group secrets are generated and stored in one place, the key server could present itself as an attractive attack target for adversaries. 2) The key server can become the single point of failure/bottleneck. In contrast, in contributory group key management schemes e.g. *Tree-based Group Diffie-Hellman* (TGDH) [17], every group member contributes to the group key generation. It has the advantage of fault-tolerance. However, for group membership changes, it lacks scalability in terms of computational cost. For example, TGDH has the following drawbacks. 1) Every group member performs the expensive Diffie-Hellman key exchange with $\left[1, O\left(\log_2 n\right)\right]$ times exponentiation operations for every group membership update where n is the group size. 2) Every sponsor should sign and forward a large number of rekeying multicast messages to update a group key. It results in expensive communication overhead and computational costs.

In this paper, we are willing to propose hybrid architecture which combines both centralized and contributory group key schemes in such a way that it takes advantage of both centralized one's efficiency and contribute one's reliability to protect the privacy of smart grid multicast service.

3.2. TGDH

The crux of the group key management scheme in TGDH is to use a binary key tree for group key updates. Let $\boldsymbol{T}$ be a binary tree in which every node is represented by $\langle h, i\rangle$ where h is its height (level) and i is its index. Each node in the binary tree, has two keys, node key(K) and blinded key(BK). The node key associated with node (l, v) is $K_{\langle l,v\rangle}$ and its blinded key $BK_{\langle l,v\rangle} = \alpha^{K_{\langle l,v\rangle}}$.

Each node in the tree is either a leaf or a parent of two nodes. Each leaf represents a group member M_i which generates r_i, a random integer. It can be treated as the leaf node's node key. The node key of an internal node $\langle l, v\rangle$, is derived from keys of its children, $\langle l+1, 2v\rangle$ and $\langle l+1, 2v+1\rangle$:

$$K_{\langle l,v\rangle} = BK_{\langle l+1,2v\rangle}^{K_{\langle l+1,2v+1\rangle}} = BK_{\langle l+1,2v+1\rangle}^{K_{\langle l+1,2v\rangle}} = \alpha^{K_{\langle l+1,2v\rangle} \times K_{\langle l+1,2v+1\rangle}} \quad (1)$$

The node key of the root is the group key. While a group member joins, the shallowest leftmost leaf node in the key tree is selected as the *sponsor* and acts as the sibling for the new group member. When a group member leaves, the *sponsor* is the shallowest leftmost leaf node of the sub-tree rooted as the leaving member's sibling node. The sponsor is responsible for updating its secret random integer r_i, and all keys on its key path. Then, the sponsor multicasts all updated blinded keys, based on which, other members update keys on their key paths and compute the new group key. Refer to [17] for details about how the sponsor is selected, how key material is prepared among all members and how group key is calculated for each participant.

3.3. ID-Based Key Agreement

In the group key scheme, security channels between two parties/members are required. Its purpose is to deliver secret messages between them. For example, when a new group member joins, the sponsor needs to establish the secure channel with the new group member. In our solution, it is fulfilled by a shared key between them: we adapt an ID-based key agreement [18] to generate the secret key.

1) Set-up

Following the RSA algorithm, TC (trusted key generation center) generates and publishes (n, g, e) but keeps (p, q, d) secret.

2) Key generation

For an authorized user A, TC assigns it randomly generated ID, ID_a and computes $s_a = ID_a^{-d} \pmod n$;

For an authorized user B, TC assigns it randomly generated ID, ID_b, and computes $s_b = ID_b^{-d} \pmod n$;

TC issues (n, g, e, ID_q, s_q) to user A and (n, g, e, ID_b, s_b) to user B via secure channel.

3) Key Agreement

Step 1:

A randomly generates an integer r_a, and, computes

$$t_a = g^{r_a + ID_b} \times s_a \quad (2)$$

B randomly generates an integer r_b, and, computes

$$t_b = g^{r_b + ID_a} \times s_b \quad (3)$$

Step 2:

A and B exchange (ID_a, t_a) and (ID_b, t_b) via authenticated channels;

Step 3:

A and B computes formula (4) and (5) respectively:

$$\begin{aligned} k_a &= \left(\left(g^{-ID_a} \times t_b\right)^e \times ID_b\right)^{r_a} \pmod n \\ &= g^{er_a r_b} \pmod n \end{aligned} \quad (4)$$

$$\begin{aligned} k_b &= \left(\left(g^{-ID_b} \times t_a\right)^e \times ID_a\right)^{r_b} \pmod n \\ &= g^{er_b r_a} \pmod n \end{aligned} \quad (5)$$

4. Our Proposed System

4.1. Adversary Model, Assumption and Scope

Adversary Model: Like other researches in areas of privacy preservations [6,19,20] we follow the semi-honest adversary model in which smart devices (e.g. SHNs, smart meters, etc.) obey regulations of the smart buildings. Meanwhile they are also curious about messages they learn (or share) and have the intension to combine these information if possible. Therefore, any participating smart devices should relay packets and also intend to uncover other HANs' privacy by studying sensitive messages received.

Security Assumption: We assume that smart devices such as smart meters, etc. are tamper-resistant. Furthermore, we also assume the availability of the TC and the key server deployed in smart buildings or utilities. Moreover, we assume that device attestations are deployed to validate SHNs, smart meters, etc.

Scope: Our scheme mainly focuses on the confidentiality service to protect privacy in multicast. In terms of unicast, the pair-wise key schemes are already implemented in wireless networks e.g. Zigbee. Efficient encryption algorithms e.g. AES are utilized in sensor networks as well. We will use them in our solution directly rather than proposing new components. The authentication and integrity services guaranteed by digital signatures and one-way hash functions are also important but beyond our paper's scope.

4.2. Privacy Leakage

Privacy threats occur when an adversary associates customers' power usage data and buildings' control commands with their daily activities e.g. breakfast, laundry, wakeup cycles, etc. [21].

Privacy for residence occupancy: An appliance control command C_i can let an adversary infer that the resident is presence or absence (also referred as *absence privacy*).

Example I: A remote control command is sent to "address *A*" aiming to shut down the air conditioner when the local temperature outdoor is high (e.g. >104˚F/40˚C). Eve can probably infer that residents living in "address *A*" may possible be absence and he then takes risks to break in.

Privacy for appliance ownership: The history of appliance control commands $\{\cdots C_i^t \cdots\}$ let an adversary compile a list of household appliances and surmise the lack one.

Example II: Alice had sent home the remote appliance control commands associated with heaters, dish washers or dryers but otherwise air conditioners. Eve extrapolates that it is highly possible for Alice to not own an air conditioner yet. The commercial information is valuable.

Privacy for personal activities model: The appliance control commands $\{\cdots C_i^t \cdots\}$ can let the adversary generalize the residence's activity model.

Example III: Alice always remotely turns on his air conditioner half an hour earlier before arriving at home. Eve finds that theses control commands are sent out at 5:30 pm from every Tuesday to Thursday but, 6:30 pm every Monday. Eve can draw Alice's life pattern in the future based on it.

4.3. System Overview

In this paper, we present a privacy preserving multicast for CSB via using an efficient, reliable, and periodic group key management scheme. As depicted in **Figure 3**, a server in the control center of the building plays the Key Server (KS) role. It generates a group key tree, GK_i, for every HAN, H_i.

We assume that there are N HANs in the smart building. Therefore, there are N group key trees, $\{T_1, T_2, \cdots, T_i, \cdots, T_N\}$ and N group keys $\{GK_1, GK_2, \cdots, GK_i, \cdots, GK_N\}$ generated in KS. The KS multicasts key material associated with each group key tree T_i to SHNs that belong to H_i where $1 \le i \le N$. The SHNs, after receiving the key material, will calculate its group key GK_i. Afterward, multicast messages toward H_i are encrypted by the group key, GK_i. SHNs inside H_i can decrypt cipher text but other SHNs outside H_i cannot since they do not obtain GK_i. The encryption algorithm can be AES, which is out of the scope of this paper.

4.4. Hybrid Architecture

In the centralized group key scheme, a server in the control center of the building plays the key server's role since it is equipped with powerful computation capacity. Following TGDH, for each HAN, the server generates the symmetric group key, partial keys, individual keys,

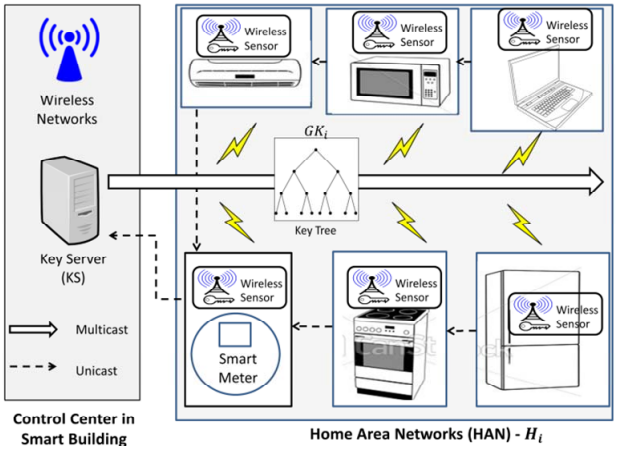


Figure 3. Overview of our proposed system.

key path and key tree which are forwarded to the corre sponding group members—SHNs and smart meters in a HAN, H_i. It takes advantages of symmetric key encryption/decryption's efficiency but the key server is the single-point failure: when it is out of control, the centralized group key scheme ceases and therefore reliability cannot be provided. In contrast, a contributory group key scheme is fault-tolerant. But it is expensive in both computation and communication. Consequently, low-capacity SHNs and smart meters and limited wireless communication channels, e.g., Zigbee, cannot afford the cost.

A naïve/straightforward method to fix this problem is to install one set of centralized scheme and one set of contributory scheme simultaneously on every smart device to guarantee both fault-tolerance and efficiency. However, deployments of two sets of schemes not only make the system more complicated but require more resources such as storages.

In this paper, we propose a hybrid protocol which combines the advantages of the centralized approach's efficiency and the contributory scheme's fault tolerance. The basic idea behind the hybrid architecture is that when the key server is off-line, then group key management will utilize a contributory scheme. If the key server is on-line, there will be two possibilities. If all the group members are able to access the key server (no partitioning of the group), a centralized scheme e.g. LKH is used in which the key server is responsible for calculating and delivering the intermediate keys associated with the binary key tree since the key server is deemed to have a high processing capability. On the other hand, if the group is partitioned (some of the members are not able to access the key server), then a combination of the two schemes is used—the members with access to the key server use the centralized scheme while the others use the contributory scheme. Both of them follow the TGDH key tree to update the node keys and blinded keys associated with the nodes on the binary key tree.

Figures 4(a) and **(b)** demonstrate the required components for implementing the centralized and the contributory key management schemes, respectively. The key tree structure follows that of TGDH or of binary tree-based LKH (TGDH is a binary tree-based LKH in terms of key tree structure). In both centralized and contributory group key scheme, the key tree structure maintenance components within the key server or the group members modify their key tree structures according to the group member joining or leaving.

Generally, the centralized scheme is the primary mechanism: the key server maintains and distributes the key tree. Every group member, e.g. SHNs and the smart meter in the same HAN, receives and stores its key path. Once the key server fails, a contributory scheme takes in charge automatically—every SHN and smart meter in the same HAN, H_i cooperates with each other to manage the group key and the key tree as well. When the key server restores, every meter delivers its latest key path to the gateway via secure channels. The scheme is controlled in centralized way again. Thus, self-healing is ensured. Since both centralized and contributory key management use the same key tree structure, no rekey operations are processed and no rekey messages are forwarded to implement the switch between the centralized scheme and the contributory scheme. Due to space limit, we will not address each component listed in **Figures 4(a)** and **(b)** in detail.

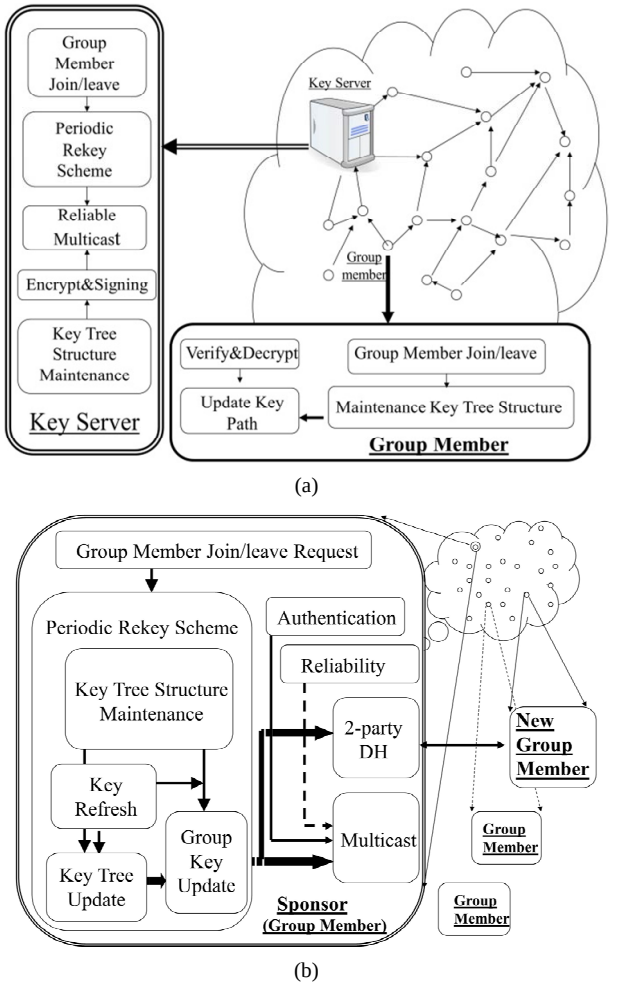


Figure 4. (a) Centralized group key management; (b) Contributory group key management.

4.5. Efficient Group Rekeying Scheme

In this subsection, we address our key tree structure, how to arrange nodes in a key tree while members join/leave and how to compute the shared group key for key server and each group member as well.

Like [16,17,22], our scheme uses a binary key tree $\boldsymbol{T}$ in which every node is associated with a node key and a

blinded key. Each leaf node represents one and only one group member. The node key of a leaf node is also called individual key.

According to our observation, we find that the stationary smart devices will not leave as long as it is legal, works in a good condition and no plan to be replaced. Therefore, even they appear not online sometimes because of device out-of-control or its jammed communication channel, we still do not mark it as leaving. Furthermore, since some roaming devices e.g. customer's PEV intends to return, its node still stays in the key tree and no leaving request should be sent out. They are treated as stationary nodes. However, other devices e.g. rented smart appliance cannot be treated as stationary nodes. Expired/ broken/compromised SHNs. are marked as leaving and will finally be deleted in rekeying process.

The layout of the key tree is demonstrated in **Figure 5(a)**, in which the fixed key tree, T_{fixed} contains all stationary smart devices. The rest group members are located in the subtree T_{main}. Notice that T_{main} is T_{fixed}'s sibling and at the same time, the child key tree, T_{child} is part of T_{main}. T_{child} stores the new incoming smart devices, e.g., newly installed SHNs.

In our scheme, to lessen member's waiting time, a joining request is processed immediately. All leaving requests are handled at the end of the rekeying time interval for the sake of efficiency. This may introduce trivial vulnerability but it is affordable. The reason is that the nature of smart grids informs us that almost all smart devices are stationary and membership changes rarely happen. Therefore, the rekeying interval (e.g. 60 minutes) defined in our scheme is sufficiently secure.

Individual Rekeying for Joining Member:

New joining group members should contain its attributes: stationary or non-stationary. The former will be inserted into the fixed key tree, T_{fixed}. The later is associated with nodes representing rented SHNs. It will be inserted into the main key tree T_{main} at the group key initiation phase. After then, new member will be inserted at child key tree, T_{child}. The insertion point for T_{child}, T_{main} or T_{fixed} is its corresponding shallowest leftmost nodes. Meanwhile, every current group member calculates the new group key via one way hash function $G' = \mathrm{Hash}(G)$ where G is the current group key and G' the new one. The new member receives G' from the sponsor via secure channels e.g. ID-based Diffie-Hellman. Refer to TGDH about how the sponsor node delivers partial keys to the new member.

Batch Rekeying for Leaving Member:

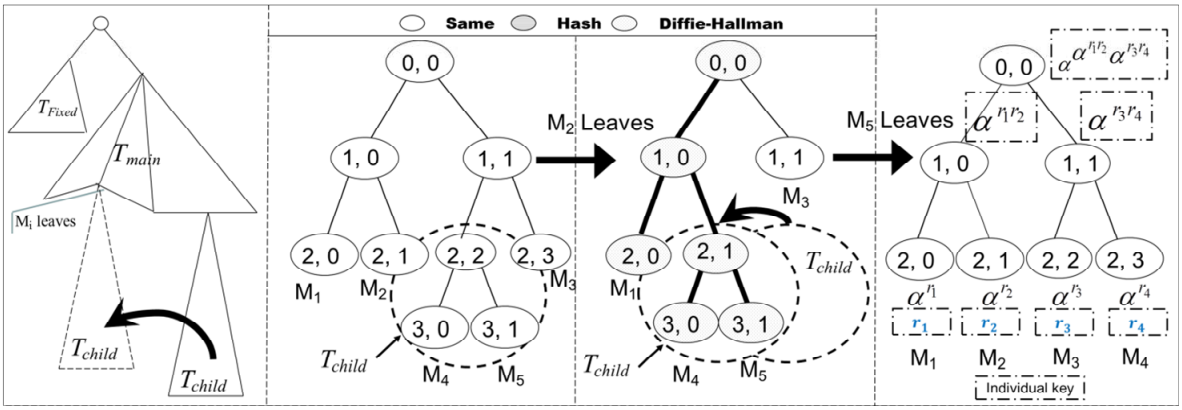
When a group member is going to leave as it is malfunctioning, legacy or expelled, the group key need to be updated at the end of the rekeying interval. The child key tree, T_{child}, may be moved to replace a leaving leaf node's place if any, for sake of computation efficiency. For details, suppose that the group member M_i, is represented by the leaf $\langle h,i \rangle$ which leaves the group. Four cases follow:

Case 1: If T_{child} is not available, our leave protocol is the same as that of TGDH.

Case 2: If T_{child} is available and $\langle h,i \rangle$ is within T_{child}, the key tree structure stays the same.

Cases 3 and 4: If T_{child} is available and $\langle h,i \rangle$ is not within T_{child}, there are two possibilities, moving T_{child} which is shown as **Figure 5(a)**, or not. The leaf node $\langle h,i \rangle$'s position and computational cost decide whether T_{child} should be moved. If moving T_{child} cannot result in the performance gain, T_{child} should stay. This scenario is called *case* 3. Otherwise, T_{child} should be moved to take $\langle h,i \rangle$'s position and $\langle h,i \rangle$ is cut off. It is called *case* 4.

For example, **Figure 5(b)** is the original key tree. **Figure 5(c)** shows that M_2 leaves. Since M_2 is not within T_{child} and moving T_{child} costs less, T_{child} rooted at $\langle 2,2 \rangle$ is moved to replace the position of node $\langle 2,1 \rangle$. The former node $\langle 2,1 \rangle$ is cut off. As its left child node is removed, node $\langle 1,1 \rangle$ is deleted. $\langle 1,1 \rangle$'s right node



(a) (b) (c) (d)

Figure 5. Binary key tree and rekeying procedure. (a) Move child tree; (b) Original tree; (c) M_2 leaves; (d) Individual keys.

$\langle 2,3 \rangle$ is renamed as $\langle 1,1 \rangle$ and promoted to its parent's position. **Figure 5(d)** demonstrates that, when M_5 leaves, T_{child} need not be moved since M_5 is within T_{child}.

5. Implementation and Experiments

5.1. Implementation

During our implementation, we utilize ID-based Diffie-Hellman key exchange agreement introduced in Section 2.4 to calculate the node key for intermediate nodes in the key tree. It can protect our scheme against the Man-in-the-Middle attack.

We implement the adapted ID-based key agreement by C language based on Pairing-Based Cryptography (PBC) library [23] built on the GNU Multiple Precision arithmetic (GMP) library [24]: GMP library provides arbitrary precision arithmetic APIs which are invoked by PBC to support pairing-based cryptosystem. Our implementation has been executed on Virtual Machine hosted by Oracle's *VirtualBox*. Here is the detailed configuration of VM-OS: Ubuntu 11.10; Memory: 4GB; Processor: Intel Core i5-M560 2.67GHz; and HDD 7.9 GB.

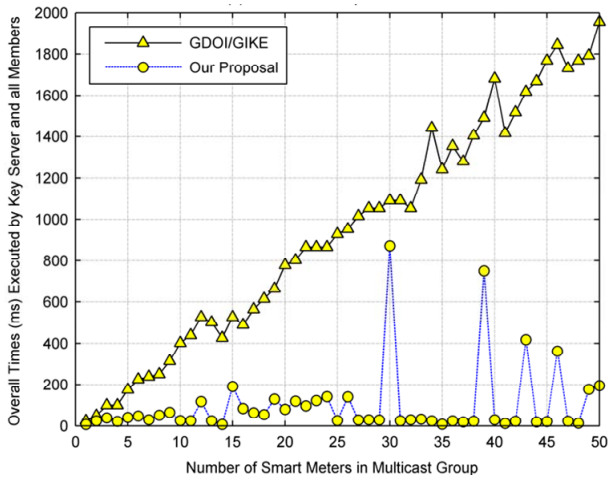
5.2. Experimental Results

The goals of our experiments are to estimate the performance of our group key scheme specifically focusing schemes. Furthermore, it can help us determine the performance gains or additional cost introduced by our scheme at different scenarios.

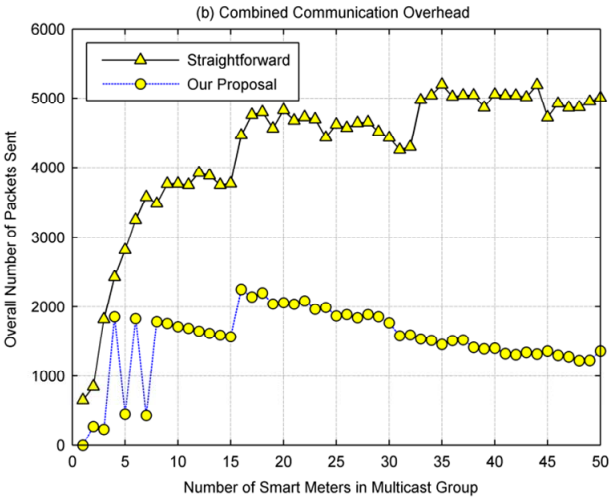
Computational Cost:

In this paper, we use the group membership change data set (duration: 3 months; group size: 250 nodes) collected in MBone [25], a famous and practicing multicast services on Internet. We demonstrate the times used to generate/update a group key for different group size in **Figure 6(a)** based on the number of exponentiation operations required to accomplish our group key scheme. As a comparison, GDOI [26] is also executed and its result is depicted at **Figure 6(a)**. The numbers of computing operations for TGDH and our proposal are depicted in **Figure 7**. Thus, as shown in **Figures 6(a)** and **7**, our proposed group key scheme is significantly efficient than GDOI/TGDH concerning with the overall execution times/number of operations. While the key server is out of control, in terms of computational cost, the hybrid architecture requires no computational operations and the straightforward solution needs a number of operations to generate a new contributory group key.

The developed ID-based key agreement is used as a test bed for experimental evaluation. The test is executed for 10 repetitions (randomly selected number), the average of which is utilized to represent the running time to accomplish the two party key agreement. Our test result



(a) Combined computional cost



(b) Combined communicational overhead

Figure 6. (a) Computational cost; (b) Communication overhead.

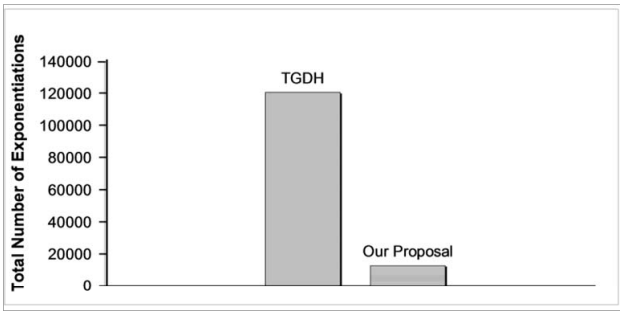


Figure 7. Numbers of exponentiations.

shows that it is 37.625 ms for each party.

Communication Overhead:

In this sub-section, hybrid architecture and straight-forward methods are simulated via Network Simulation-2 (ns-2) [13], a widely used simulation tool. In this test, to achieve the routing function, AODV, a routing protocol,

is deployed to connect wireless nodes and forward packets from one node to another. A multicast AODV (MAODV) module is extended at ns-2 to multicast packets for this project. Specially, this simulation utilized the test scenario components listed below:

*NS*2 *version*: *ns*-2.27
Network: *Mobile Ad Hoc Network* (*MANET*)
Routing Protocol: *AODV*
Multicast Protocol: *MAODV*
Area: 1500 × 300 *meters*
Number of nodes: 50
Physical/*Mac layer*: *IEEE* 802.11 *at* 2 *Mbps*, 250 *meter transmission range*
Mobility model: *random waypoint model with no pause time, maximum speed* 20 *m*/*s* (*high mobility scenarios*).

This test was developed to simulate a scenario which lasts 10 minutes. In the middle of the test, the key server is out-of-service. The purpose of this case study is to compare the communication overhead while managing a group key for straight-forward method and for the proposed hybrid architecture. Specially, in the hybrid architecture, the messages multicast to notify other group members that the key sever is out of service if the key server cannot be detected with heartbeats. Then, a notation to let all group members switch from the centralized method to the contributory one is forwarded. In contrast, in the straightforward method, a new group key will be generated via contributory solutions. **Figure 6(b)** shows experimental results which indicate that our hybrid scheme is efficient in terms of communication overhead. Notice that background messages e.g. routing data, keepalive data are also counted in **Figure 6(b)**.

5.3. Security Analysis and Performance Evaluation

As the group key security has already been formally proved in TGDH, LKH, etc., we will not discuss them in this paper due to limited space.

The realization of our scheme presents an exciting conesquence to preserve privacy multicast communications in smart buildings since: 1) The hybrid architecture to accommodate the centralized and contributory schemes and individual rekey for member joining are designed for multicast in CSB. It presents not only the efficiency but also the availability; 2) The periodic rekeying scheme and the centralized scheme provide receivers (SHNs or smart meters) the lightweight operations to calculate their new group keys; 3) The hybrid architecture reduces the communication overhead by around 50% while the key server is out-line; 4) Our scheme provides a fault tolerance architecture against single point failures; 5) Most importantly, a couple of novel rekeying algorithms e.g. the child key tree, the fixed key tree, etc. are proposed, designed and implemented for rekeying schemes in practice; 6) Despite that our scheme introduces delay, it still complies with the delay limit, 15 s.

6. Related Works

We now summarize the privacy preservations of smart grids. Main approaches such as *cryptographic primitives* [6,7,19,20,27] *battery* [9], *ID anonymization* [28], and *disturbance* [8] are reviewed.

Cryptographic primitives: Zhang and Gunter [7] propose an approach to secure multicast in smart grid via deploying IPsec protocol and Group Internet Key Exchange (GIKE)/Group Domain of Interpretation (GDOI). Both IPsec and GIKE/GDOI [26] are standards for multicast applications: video broadcast and multicast file transfer; nevertheless, it is less efficient as not specifically designed for multicast in smart grid. Furthermore, its goal is confidentiality instead of privacy.

Li, Luo, and Liu [6] focus on privacy preservation for smart metering data aggregation in which all messages are encrypted by using homomorphic encryption algorithm. Garcia and Jacobs [19] proposed a privacy-friendly protocol by using homomorphic (Paillier) encryption and additive secret sharing to realize tasks such as billing, leakage detections, etc. Rial and Danezis [20] use zero knowledge proofs and commitments to preserve smart meters' privacy. This protocol facilitates the accurate bill payment and derives the correctness of power bills without exposing any message about customers' power usage. In [27], Kursawe, Danezis, and Kohlweiss proposed four different protocols, e.g. Diffie-Hellman (DH) Key-exchange based protocol, DH and Bilinear-map based protocol etc. for metering data aggregation services with no privacy disclosure. In [22], Li *et al*. proposed a privacy preservation scheme for smart home in smart grids based on hybrid group key scheme.

These privacy preservation solutions relying on cryptographic schemes (except GDOI) cannot secure group communication. The reason is because they are designed for privacy of an individual device or unicast communications. Invoking them in multicast settings cannot be scalable.

Battery: McLaughlin, McDaniel, and Aiello [9] propose the Non-Intrusive Load Leveling (NILL), a new class of algorithms and systems to mask the appliance's fine-grained power usage signature. Ten particular *deep-cycle* batteries are deployed. However, there are still a few privacy leakages after deploying extra batteries. Furthermore, they show expensive installment and maintenance cost.

ID Anonymization: In [28], Efthymiou and Kalogridis proposed a trusted key escrow service to enhance privacy during services such as smart metering data collection, billing service, etc. The approach anonymizes frequent

readings with pseudonymous IDs along with randomized time intervals.

Disturbance: Li *et al.* [8] proposed a compressed meter reading approach that enhances its privacy through the use of random sequence. This solution integrates with pseudo-random spreading codes and channel gains from smart meters to the Access Points (AP). However, AP is assumed never to be compromised.

7. Conclusions

The privacy preservation in smart grids over multicast communication is a challenging task. The well-known group key scheme cannot be directly used to protect the privacy of multicast service. The central issues are the reliability and efficiency considering that the prompt restoration and the minimum overall fault times are highly demanded in smart grids. Previous solutions are not appropriate for smart grid settings because of heavyweight rekeying operations, poor scalability or single-point failure architecture.

This paper presents the design and specification of a fault-tolerant and efficient group key agreement to safeguard the privacy of multicast messages in smart grids. The performance result demonstrates that our scheme is efficient and acceptable. It satisfies smart grid system's reliability and efficiency requirement.

REFERENCES

[1] T. Vijayapriya and D. P. Kothari, "Smart Grid: An Overview," *Smart Grid and Renewable Energy*, Vol. 2, No. 4, 2011, pp. 305-311. doi:10.4236/sgre.2011.24035

[2] D. Li, Z. Aung, J. Williams and A. Sanchez, "Efficient Authentication Scheme for Data Aggregation in Smart Grid with Fault Tolerance and Fault Diagnosis," *IEEE Power and Energy Society Conference on Innovative Smart Grid Technologies*, Washington DC, 19-22 February 2012, pp. 1-8.

[3] H. Y. Tung, K. F. Tsang, H. C. Tung, V. Rakocevic, K. T. Chui and Y. W. Leung, "A WiFi-ZigBee Building Area Network Design of High Traffics AMI for Smart Grid," *Smart Grid and Renewable Energy*, Vol. 3, No. 4, 2012, pp. 253-259. doi:10.4236/sgre.2012.34043

[4] NIST, "Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid," NISTIR 7628, August 2010.

[5] E. L. Quinn, "Privacy and the New Energy Infrastructure," Social Science Research Network (SSRN), 2009. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1370731

[6] F. Li, B. Luo and P. Liu, "Secure Information Aggregation for Smart Grids Using Homomorphic Encryption," *IEEE International Smart Grid Communications*, New York, 4-6 October 2010, pp. 327-332.

[7] J. Zhang and C. A. Gunter, "Application-Aware Secure Multicast for Power Grid Communication," *IEEE Conference on Smart Grid Communications*, New York, 4-6 October 2010, pp. 339-344.

[8] H. Li, R. Mao, L. Lai and R. C. Qiu, "Compressed Meter Reading for Delay-Sensitive and Secure Load Report in Smart Grid," *IEEE International Conference on Smart Grid Communications*, New York, 4-6 October 2010, pp. 114-119.

[9] S. Mclauhlin, P. Mcdaniel and W. Aiello, "Protecting Consumer Privacy from Electric Load Monitoring," 18*th ACM Computer and Communication Security Conference*, Chicago, 17-21 October 2011, pp. 87-98.

[10] http://www.zigbee.org/

[11] http://www.wi-fi.org/

[12] SmartGridNews, "IBM Consumer Survey Reveals Where Utilities Are Still Getting It Wrong," 2011. http://www.smartgridnews.com/artman/publish/Business_Stratgy/IBM-consumer-survey-reveals-where-utilities-are-still-getting-it-wrong-3944.html

[13] NS2, "The Network Simulator," 2013. http://www.isi.edu/nsnam/ns

[14] B. Akyol, H. Kirham, S. Clements and M. Hadley, "A Survey of Wireless Communications for the Electric Power System," US Department of Energy, 2010, in press. doi:10.2172/986700

[15] N. Liu, J. Chen, L. Zhu, J. Zhang and Y. He, "A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid," *IEEE Transactions on Industrial Electronics*, Vol. 60, No. 10, 2012, pp. 4746-4756.

[16] C. K. Wong, G. Gouda and S. S. Lam, "Secure Group Communications Using Key Graphs," *IEEE/ACM Transactions on Networking*, Vol. 8, No. 1, 2000, pp. 16-30. doi:10.1109/90.836475

[17] Y. Kim, A. Perrig and G. Tsudik, "Simple and Fault-Tolerant Key Agreement for Dynamic Collaborative Groups," 7*th ACM Computer and Communication Security Conference*, Athens, 1-4 November 2000, pp. 235-244.

[18] E. Okamoto and K. Tanaka, "Key Distribution System Based on Identification Information," *IEEE Journal of Selected Areas in Communications*, Vol. 7, No. 4, 1989, pp. 481-485. doi:10.1109/49.17711

[19] F. D. Garcia and B. Jacobs, "Privacy-Friendly Energy-Metering via Homomorphic Encryption," 6*th International Conference on Security and Trust Management*, Athens, 23-24 September 2010, pp. 226-238.

[20] A. Rail and G. Danezis, "Privacy-Preserving Smart Meteringm," *ACM CCS Workshop on Privacy in the Electronic Society*, Chicago, 17-21 October 2011, pp. 49-60.

[21] M. A. Lisovich, D. K. Mulligan and S. B. Wicker, "Inferring Personal Information from Demand-Response Systems," *IEEE Security & Privacy*, Vol. 8, No. 1, 2010, pp. 11-20. doi:10.1109/MSP.2010.40

[22] D. Li, Z. Aung, S. Sampalli, J. Williams and A. Sanchez, "Privacy Preservation for Smart Grid Multicast via Hybrid Group Key Scheme," *International Conference on Electrical Engineering and Computer Science*, Shanghai, 17 August 2012, pp. 62-69.

[23] B. Lynn, "The Stanford Pairing Based Crypto Library,"

2013. http://crypto.stanford.edu/pbc/

[24] GNU, "The GNU Multiple Precision Arithmetic Library," 2013. http://gmplib.org/

[25] K. C. Ameroth, "A Long-Term Analysis of Growth and Usage Patterns in the Multicast Backbone (MBone)," *IEEE Conference on Computer Communications*, Tel Aviv, 26-30 March 2000, pp. 824-833.

[26] Network Working Group, "IETF RFC 3547, the Group Domain of Interpretation," 2003. http://tools.ietf.org/html/rfc3547#section-1.1

[27] K. Kursawe, G. Danezis and M. Kohlweiss, "Privacy-Friendly Aggregation for the Smart-Grid," *Privacy Enhancing Technologies*, *Lecture Notes in Computer Science*, Vol. 6794, 2011, pp. 175-191.

[28] C. Efthymiou and G. Kaogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," *IEEE International Smart Grid Communications*, New York, 4-6 October 2010, pp. 238-243.

