An Application of IEEE 802.15.4 Standard for Advanced Metering Infrastructure with Enhanced Security and Privacy Considerations

Pan Deng and Liuqing Yang
Department of Electrical and Computer Engineering
Colorado State University

Abstract

Smart grid is the next-generation power grid which outperforms the current grid in intelligence, efficiency and reliability. As a core component of the smart grid, Advanced Metering Infrastructure (AMI) collects and analyzes energy usage data through a two-way communication network and interconnected smart meters. It is a significant task to choose an appropriate underlying communication technology for an AMI network. In this paper, we investigate the advantages of applying IEEE 802.15.4 based protocols to AMI. In addition, we propose a data communication scheme to protect data security as well as customer privacy in an AMI network with the help of homomorphic encryption. Security analysis shows the resistance of our proposed scheme to typical cyber-attacks.

I. Introduction

THE existing power grid has been serving both industry and daily life well for a long time. However, its limitations in efficiency and reliability are gradually to be reached. For example, if the grid were just 5% more efficient, the resultant energy savings would be sufficient to offset the fuel and greenhouse gas emissions from 53 million cars. Today's electricity system is 99.97% reliable, which still allows power outages and interruptions that cost the United States at least $150 billion each year [1]. There have been five massive outages over the past 40 years while three of which have occurred in the past nine years. In such a situation, there is a strong need for a more intelligent, efficient and reliable next-generation power grid – the smart grid.

Smart grid is different from the legacy power grid in that grid components are interconnected via a two-way communication network. The system that collects, measures and analyzes energy usage data through this network and connected smart meters is often referred to as Advanced Metering Infrastructure (AMI). Smart meters play a key role in AMI. These next-generation electricity meters can monitor power consumption in more detail than conventional meters. A smart meter is able to collect data at a frequency as high as every minute, while old meters only record data hourly or monthly [2]. Smart meters communicate information back to the local utility for real-time monitoring and management purposes such as demand side response. Meanwhile, they can receive data from the local utility through the AMI network, which renders the grid consumer-interactive. For example, consumers can adjust their power load according to the time-varying price of the power supply, which is received from smart meters. With the help of smart

meters, customers can always charge their electric vehicles in off-peak periods and introduce distributed power generation in peak periods to save cost and reduce peak load.

There are two major proposals for AMI network architecture: Power Line Carrier (PLC) and Fixed Wireless Network [3]. Here we will consider the latter, as shown in Fig. 1. In this hybrid architecture, smart meters form a wireless mesh network which provides high reliability and extensive range. A collector device with a wired backhaul connection to the utility acts as a gateway between smart meters and the utility. The main advantage of using wireless communication technology here is that there is no need to build new communication infrastructure for smart meters. A critical issue for this approach is to choose an appropriate wireless communication protocol for smart meters. For example, Zigbee protocol [4] based on IEEE 802.15.4 standard [5] is widely considered a competitive candidate because of its attractive features such as low cost, low power consumption and network flexibility.

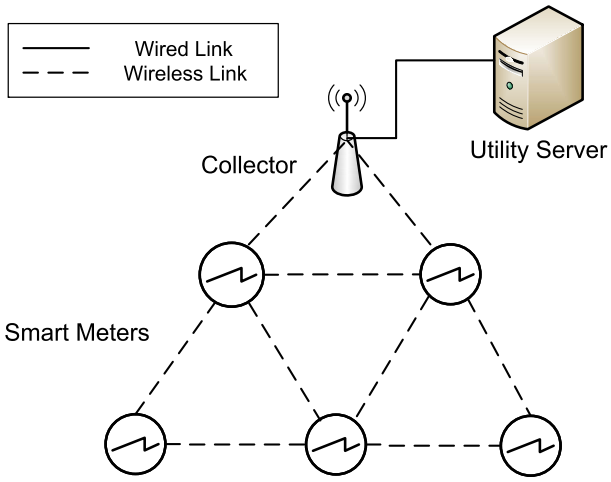

Fig. 1. AMI Network Architecture

While AMI brings great benefit to smart grid, concerns about potential security and privacy threats have been raised. Attackers might inject false data in the AMI network to degrade system performance or even cause power outages at a large scale. Smart meters might be compromised since they are not installed in physically secure locations. Users' energy use data might be eavesdropped and analyzed to deduce private information, such as what kind of electric appliances are operating in the home. If attackers deliberately collect and analyze a large amount of such data from a victim, they might even learn about the victim's daily activities and habits and use that information for malicious purposes. In an extreme case, customers might not trust the utility and they may require that even the utility is not able to correlate their energy use information with their identities. Therefore, it is essential to protect data security and maintain customer privacy, while collecting their daily power usage data with an AMI network.

In the 802.15.4 standard, MAC sublayer can offer some basic security services, like data confidentiality and authenticity, on specified incoming and outgoing frames when requested to do so by the higher layers. However, this is not sufficient in an AMI network since the privacy leakage problem is not addressed. To the best of our knowledge, currently only very few independent research works have been done on the smart grid security and privacy problem. The authors of [6] develop an in-network collaborative communication scheme for secure and reliable AMI communications but the privacy issue is not touched

upon. In [7], the authors assign two IDs to each smart meter and make the ID for high-frequency sensitive data anonymous through a third party escrow service. In [8], the authors attempt to make the appliance load signature undetectable using a rechargeable battery to mitigate any significant change in real-time power consumption. The feasibility of this technology, however, heavily hinges upon the energy efficiency and cost-effectiveness of batteries. A secure information aggregation method, using homomorphic encryption, is proposed in [9]. This method protects the identity of users but lacks enough security mechanisms.

In this paper, we propose a secure and privacy-preserving AMI communication scheme based on the idea of end-to-end data aggregation. Our scheme has enhanced security mechanisms by taking advantage of Paillier cryptosystem [10], which is a homomorphic public key cryptosystem. A homomorphic encryption is a form of encryption where a specific algebraic operation performed on the plaintext is equivalent to a (possibly different) algebraic operation performed on the ciphertext. As for Paillier cryptosystem, we have

$$D(E(m_1)E(m_2) \bmod n^2) = m_1 + m_2 \bmod n$$

for any plaintexts m_1, m_2, where n is the public key and E, D represent the encryption and decryption functions respectively. In our scheme, we first build an initial device registration procedure with strong authentication requirements to ensure that unauthorized devices cannot join the network. Homomorphic encryption is adopted for sensitive metering data to ensure data confidentiality and meanwhile preserve customer privacy. Differing from [9], we also attach a digital signature to each message for integrity and authenticity of the metering data.

The rest of this paper is organized as follows. Section II briefly introduces IEEE 802.15.4 standard and demonstrates its feasibility in an AMI environment. Section III describes our secure communication scheme in detail. Security analysis is presented in Section IV. Finally, Section V concludes the paper.

II. IEEE 802.15.4 STANDARD

A. Overview

A low-rate wireless personal area network (LR-WPAN) is a simple, low-cost communication network that allows wireless connectivity in applications with limited power and relaxed throughput requirements. The main objectives of an LR-WPAN, while maintaining a simple and flexible protocol, are ease of installation, reliable data transfer, extremely low cost and a reasonable battery life. IEEE 802.15.4 standard defines the physical layer (PHY) and medium access control (MAC) sublayer specifications for LR-WPANs [5].

The physical layer defines the means of transmitting raw bits over a physical link connecting network nodes. It is responsible for tasks like activation and deactivation of the radio transceiver, energy detection and channel frequency selection. In the standard, several different symbol modulation scheme are defined, including O-QPSK, BPSK, ASK, etc.. All of them have individual parameters on operating bands and data rate. This diversity is the basis for various applications of the standard.

The MAC sublayer handles all access to the physical radio channel and enables the transmission of MAC frames through the use of the physical channel. It is responsible for tasks like beacon management, channel access management, frame validation, acknowledged frame delivery, association, and disassociation. The

standard employs various mechanisms to improve the probability of successful data transmission, including carrier sense multiple access with collision avoidance (CSMA-CA) mechanism, ALOHA mechanism, frame acknowledgment and data verification.

Other higher-level layers and inter-operability sublayers are not defined in the standard. In contrast, all existing protocols based on this standard like ZigBee, ISA100.11a, WirelessHART and MiWi have developed their own particular upper layer specifications for various application scenarios.

B. Feasibility Study

Many features of IEEE 802.15.4 standard contribute to its feasibility for AMI network nodes, mostly smart meters. We will list a few here.

1) Monetary Cost: Since a huge amount of smart meters will be produced and deployed, it is preferable to use an inexpensive communication module for cost control. This need is well fit by the standard. From the very beginning, the goal of the standard is to provide a low cost wireless communication solution among inexpensive devices. Zigbee can be a paradigm here: as of 2006, the retail price of a Zigbee-compliant transceiver is approaching $1, and the price for one radio, processor and memory package is about $3 [11].

2) Power Consumption: For smart meters with wireless communication capability, power consumption is expected to be at a very low level due to both energy saving and health concern. This is again a main objective of an LR-WPAN. For Zigbee devices, the output power of the radios is generally 0 dBm (1 mW) [4]. The output power can be further reduced, in practice, when the transmission range of a smart meter is carefully controlled.

3) Network Topology: Depending on the application requirements, an IEEE 802.15.4 LR-WPAN operates in one of two topologies: the star topology or the peer-to-peer topology [5]. In either topology, a PAN coordinator serves as a primary controller of the PAN which can be used to initiate, terminate or route communication around the network. In the star topology, communication is established between devices and the PAN coordinator. The peer-to-peer topology is different from the star topology in that any device is able to communicate with any other device, as long as they are in range of one another. Thus, when the peer-to-peer topology is employed, we can implement a mesh network of smart meters efficiently where the collector device plays the role of PAN coordinator.

4) Data Rate: The data rate defined by the standard ranges from 20kbps to 250kbps. Since the data sent by smart meters typically only include hourly power usage readings, which are light-weighted and do not have strict real-time requirements, the relatively low date rate should suffice in our application.

5) Transmission range: In a mesh network, it is important to guarantee link connectivity among neighboring nodes. The typical transmission range of a device is between 10 and 75 meters when Zigbee modules are employed [4]. Considering that the distance between neighboring homes is usually on the magnitude of tens of meters, the network connectivity would not be an issue here.

III. Secure Communication Scheme

A. Design Objectives

As we have seen, IEEE 802.15.4 standard fits well with AMI networks. However, the security features provided by the MAC sublayer are not quite sufficient. Therefore, we propose a communication scheme

which deals with potential security and privacy threats in the application layer. The following security requirements are considered for our scheme:

1) Device Authentication: Any smart meter's identity must be securely authenticated before it can join the AMI network and exchange data with other devices.
2) Data Confidentiality: All data packets exchanged in the network, including meter readings and control messages, must be kept confidential so that only authorized entities, with corresponding credentials, are allowed to access specific sets of data.
3) Message Integrity and Authenticity: When a message arrives at its destination, the recipient should be able to verify whether the message remains unaltered and if it comes from the sender it claims.
4) Privacy Protection: Any sensitive data, which might be used to deduce private information, should only be known to their owner.

B. Device Registration

Each newly installed smart meter should register with the utility before it can start various services. During the registration process, its identity must be authenticated, which is the very first step to ensure the security of the whole AMI system. In our scheme, Paillier cryptosystem is adopted at all smart devices. We assume that each smart meter holds its built-in private key while the authentication server of the utility knows the meter's ID and public key, which can be provided beforehand by smart meter manufacturers.

Fig.2 illustrates the data flow of the device registration process. Specifically, this process takes place in the following steps:

1) The newcomer smart meter initializes a registration request message. The message body consists of the smart meter's ID and request content in a pre-defined format. The entire message is signed by the smart meter's private key.
2) The smart meter passes the message to the collector with other smart meters possibly used as repeaters on the way. The collector then forwards the message to the authentication server of the utility.
3) The authentication server finds the smart meter's public key, according to the ID contained in the message, and verifies the signature. If the signature is valid, it replies to the collector with an "Accept" message and the smart meter's public key; otherwise it replies with "Decline".
4) The collector checks the received response. If the response is "Accept", it sends an acknowledgement message and its own public key to the smart meter and adds a new entry to its registered device list. This list records the IDs and public keys of all successfully registered devices. Otherwise, it notifies the meter that the request is declined.

After registration completes, the smart meter and the collector know the public key of each other. Therefore, they are always able to set up a secure communication session later on. Also, by recording all repeaters' information in the registration request message, the collector can gather all necessary topology information of this multi-hop smart meter wireless network when all smart meters are successfully registered. Then it can generate a virtual routing backbone with some existing algorithms [12][13] and assign each smart meter a routing table for future communications.

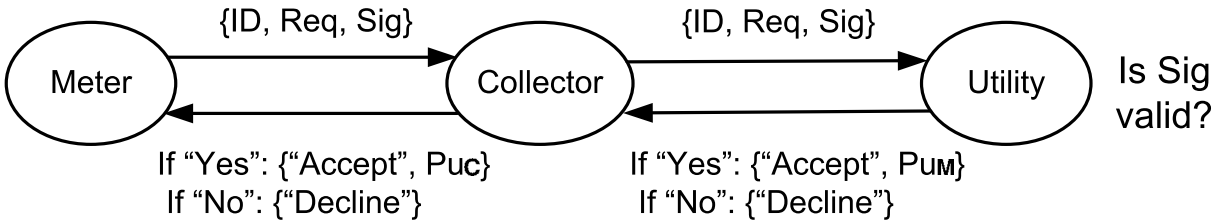

Fig. 2. Device Registration Process

C. Non-sensitive Data Communication

Some data in AMI network do not involve information that might disclose user privacy. This type of data mainly includes monthly or quarterly metering readings, which are usually required for billing purposes and management control messages, sent by the headquarters of the utility. For these data, common methods of secure communication are applicable. Particularly, each message will be encrypted by the recipient's public key and signed by the sender's private key.

D. Sensitive Data Communication

High-frequency (HF) metering data [7] are finer-grained meter readings. They are required for efficient power network monitoring and management and will likely be collected every few minutes. Customer privacy issues essentially arise from the collection of HF data, since it is possible to extract private information, like domestic appliance usage, from these data. Aggregation is a useful way to tackle this problem, assuming that the utility or distribution substation which collects HF data only needs to know the total power usage of a residential area but not the power usage of a specific home. The traditional data aggregation method, in which each smart meter sends its data to the collector separately, is not applicable here, since the collector is able to access the data of any specific user. Instead, we use an in-network aggregation scheme [9] to protect customer privacy. In this scheme, the intermediate aggregation results are calculated along the way and the collector always receives a summation of all smart meters' readings. Any sensitive data directly related to private information are only readable by their owners.

We first need to build an aggregation path which covers all registered smart meters in the neighborhood. If we view the smart meter network as a graph where all devices are vertices and available wireless links between any two devices are edges, then such a path naturally forms a spanning tree of the graph, which is called an aggregation tree [9]. It is convenient to view the path in a top-down manner as a rooted tree, where the collector node is the root, as shown in Fig.3. The data are passed from the bottom to the top along the tree edges during the aggregation process. Since the collector is aware of the network structure as well as a routing backbone, it can construct an aggregation tree based on the routing backbone by simply connecting non-backbone nodes. When necessary, the collector can adjust the structure of the tree according to the two criterions mentioned in [9] for better performance. When the aggregation tree is finally determined, the collector notifies each smart meter of the necessary information for aggregation, respectively. For a single smart meter, it only needs to know: 1) The IDs and public keys of its children nodes; 2) The ID and network address of its parent node.

The aggregation process is supposed to occur at a fixed frequency every day. We assume all smart meters are equipped with synchronized clocks such that they can initialize the aggregation simultaneously

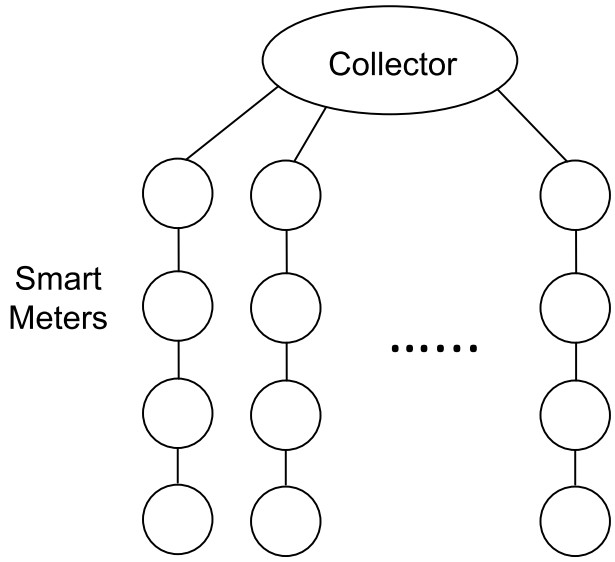

Fig. 3. An example of aggregation tree

when aggregation time arrive. The operations for each smart meter are essentially the same:

1) Encrypt its power usage data with the public key of the collector.
2) Wait for the data from its children (if any). When the data arrives, verify the integrity of the data received using public keys of the children.
3) Calculate intermediate aggregated result by multiplying its own data with the received data (if any).
4) Generate a digital signature with the intermediate aggregated result and current timestamp. The timestamp is a one-time bit sequence which indicates current aggregation time. It is unique and different for each aggregation process.
5) Send the aggregated result combined with the signature to its parent.

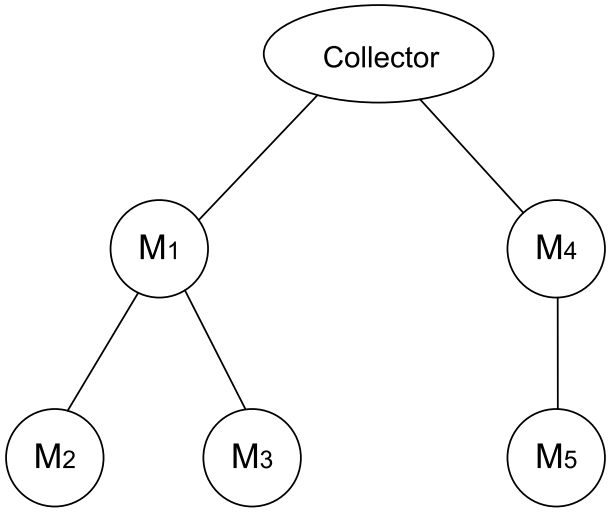

Fig. 4. A simplified aggregation tree

We use a simplified aggregation tree as shown in Fig.4 to give an illustrative example. The tree consists of the collector node as the root and five communication nodes which represent smart meters

M_1, M_2, M_3, M_4 and M_5. Available communication links are indicated by edges of the tree. All notations involved are given in the Table I.

When a pre-defined aggregation time arrives, the process begins in a bottom-up manner. We mainly discuss the operations of the left branch of the tree which includes M_1, M_2 and M_3 here, while the operations of the right part are essentially the same.

1) The nodes at the lowest level, i.e., M_2 and M_3 encrypt their raw data with the public key of the collector and generate the signatures with their private keys:

$$C_2 = E(D_2), S_2 = S(C_2||TS)$$
$$C_3 = E(D_3), S_3 = S(C_3||TS)$$

Here '||' means concatenation. Meanwhile, M_1 just calculate C_1 but not the signature since it need to wait for data from its children.

2) M_2 and M_3 send their encrypted data with signatures to their parent, M_1:

$$M_2 \rightarrow M_1 : \{C_2, S_2\}$$
$$M_3 \rightarrow M_1 : \{C_3, S_3\}$$

3) M_1 receives the data and verifies them with the public keys of M_2 and M_3 it already knows; if the signatures are valid, it calculates its intermediate aggregation result and signature:

$$I_1 = C_1 * C_2 * C_3 \bmod n^2$$
$$S_1 = S(I_1||TS)$$

4) M_1 sends its signed intermediate aggregation result to its parent, the collector:

$$M_1 \rightarrow \text{Collector} : \{I_1, S_1\}$$

Similarly, another intermediate aggregation result $I_4 = C_4 * C_5$ is calculated at M_4 and sent to the collector.

5) The collector receives I_1 and I_4 and verifies their integrity; then it aggregates them and decrypt it with its private key to get the total power usage data of the network:

$$D_{final} = D(I_1 * I_4) = \sum_{i=1}^{5} D_i \bmod n = \sum_{i=1}^{5} D_i$$

The modular n operation can be removed because we can carefully choose the bit length of $D_i s$ and n such that $\sum_i D_i \ll n$.

Now we can see clearly during the whole aggregation process, sensitive data $D_i s$ are encrypted and aggregated along the way. Only the collector has the key to decrypt them. However, it will only receive an aggregated result but not any separate D_i. Therefore, the private information of customers associated with $D_i s$ are effectively protected.

Notation	Definition
D_i	Raw power usage data of M_i
C_i	Encrypted power usage data of M_i
I_i	Intermediate aggregation result of M_i
S_i	Digital Signature generated by M_i
D_{final}	Total power usage data of the network
TS	Current timestamp

TABLE I
NOTATIONS USED IN THE EXAMPLE

IV. SECURITY ANALYSIS

This section analyzes the security properties of our scheme and discusses its resistance to several common attacks.

A. Security Level

We say a probabilistic asymmetric key encryption algorithm has *indistinguishability under chosen plaintext attack* (IND-CPA) property if a polynomial time adversary has only a negligible "advantage" over random guessing. Formally, that means: the adversary chooses two plaintexts, and we select at random one plaintext and provide to the adversary the corresponding ciphertext. The adversary is free to perform any number of additional computations or encryptions with the public key we used, then the adversary must guess which plaintext we chose. If the best success probability the adversary can achieve is $1/2+\epsilon$, where ϵ is a negligibly small number, we say the encryption is IND-CPA. In other words, the encryption is *semantically secure*: the knowledge of a ciphertext does not give any useful information on the plaintext to a adversary with reasonable computation power. The Paillier cryptosystem we adopt is indeed IND-CPA. Due to the nature of homomorphic encryption, this is also the highest security level a homomorphic scheme can reach [14].

B. Possible Attacks

1) False Data Attack: False data attack means the adversary tries to inject false data into the AMI network to disturb normal system operations. One possibility is that the adversary pretends itself to be a smart meter and joins the network. However, since we require device authentication at the registration stage, this is not likely to happen if the adversary cannot get a usable private key by compromising a smart meter. The other possibility is that the adversary intercepts network traffic and maliciously modifies the data and retransmits them. Again, the adversary is not able to generate a valid digital signature without a valid private key, if we can guarantee that all private keys are securely embedded in smart meters. In either case, we have to note that the physical and software security of smart meters themselves are essential for our scheme. This is another important research topic which is beyond the scope of this paper.

2) Replay Attack: A deliberate attacker might initialize a replay attack by eavesdropping on communications first and grabbing some data packets. Then the attacker retransmits them at a later time as if it comes from a real smart meter. This kind of attack does not require the knowledge of any private keys.

Our scheme is resistant to replay attack since we use timestamp as an additional input to generate a digital signature. Thus any outdated data packets will be easily detected and rejected.

V. Conclusion

Smart grid is the next-generation power grid which greatly benefits from the two-way communication network of AMI. Among different solutions for AMI communications, IEEE 802.15.4 standard is a natural fit. However, some security and privacy challenges about AMI still need to be properly addressed. In this paper, we first investigate the suitability of IEEE 802.15.4 standard in an AMI environment. Then, we propose a secure and privacy-preserving communication scheme for AMI which leverages Paillier cryptosystem. Security analysis shows that our scheme is resistant to some common attacks.

Acknowledgment

The authors would like to thank Mr. Robert Griffin for his helpful opinions on English writing.

References

[1] U.S. Department of Energy, "The Smart Grid: An Introduction," 2008.

[2] H. Khurana, M. Hadley, N. Lu, and D. Frincke, "Smart-Grid Security Issues," *IEEE Security and Privacy*, vol. 8, no. 1, pp. 81–85, Feb. 2010.

[3] A. van Engelen and J. Collins, "Choices for smart grid implementation," in *Proceedings of the 43rd Hawaii International Conference on System Sciences*, Poipu, Kauai, Hawaii, USA, Jan. 5-8, 2010, pp. 1–8.

[4] http://en.wikipedia.org/wiki/Zigbee.

[5] IEEE Standard for Local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs).

[6] Y. Yan, Y. Qian, and H. Sharif, "A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid," in *Proceedings of Wireless Communications and Networking Conference (WCNC)*, Quintana-Roo, Mexico, March 28-31, 2011, pp. 909–914.

[7] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proceedings of First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Gaithersburg, MD, USA, Oct. 4-6, 2010, pp. 238–243.

[8] G. Kalogridis, C. Efthymiou, S. Denic, T. Lewis, and R. Cepeda, "Privacy for smart meters: towards undetectable appliance load signatures," in *Proceedings of First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Gaithersburg, MD, USA, Oct. 4-6, 2010, pp. 232–237.

[9] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Proceedings of First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Gaithersburg, MD, USA, Oct. 4-6, 2010, pp. 327–332.

[10] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT'99)*, Prague, Czech Republic, May 2-6, 1999, pp. 223–238.

[11] J. Adams and B. Heile, "Busy as a Zigbee," *IEEE Spectrum*, Oct 2006.

[12] Y. Wang, W. Wang, and X. Li, "Distributed low-cost backbone formation for wireless ad hoc networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Urbana-Champaign, IL, USA, May 25-28, 2005, pp. 2–13.

[13] H. Guo, Y. Qian, K. Lu, and N. Moayeri, "Backbone construction for heterogeneous wireless ad hoc networks," in *Proceedings of IEEE International Conference on Communications (ICC)*, Dresden, Germany, Jun. 14-18, 2009, pp. 1–5.

[14] C. Fontaine and F. Galand, "A survey of homomorphic encryption for nonspecialists," *EURASIP Journal on Information Security*, vol. 2007, pp. 1–15, Jan. 2007.