A SECURE AND COMPROMISE-RESILIENT ARCHITECTURE FOR ADVANCED METERING INFRASTRUCTURE

by

Khalid Alfaheid

A Thesis Submitted in Partial Fulfillment

of the Requirements for the Degree of

Master of Applied Science (MASc)

In

Electrical and Computer Engineering

Faculty of Engineering and Applied Science

University of Ontario Institute of Technology (UOIT)

Oshawa, Ontario, Canada

March, 2011

Abstract

In recent years, the Smart Grid has grown to be the solution for future electrical energy that promises to avoid blackouts as well as to be energy efficient, environmentally and customer-friendly. In Smart Grid, the customer-friendly applications are a key element that provides the feature for recognizing the active expenditure of current energy via an Advanced Metering Infrastructure (AMI) subsystem. In fact, the smart meter, as a major part of AMI that is installed in residences, which provides more details about a consumer's usage. The smart meter measures hour-by-hour usage of a house, and then instantly transmits the record to the utility via two-way communications, unlike the previous electrical system that collects all usage monthly. However, the live measurement of the usage creates a potential privacy leak since each electrical usage records the behaviour of consumers in the home. Therefore, any communication channel between customers and utility should have some sort of confidentiality which protects consumer privacy. In reality, smart meters are generally located in an insecure area of the house (outside), therefore anyone can potentially tamper with the device, noting the fact that it is low-end device. As a result, there is a great possibility of compromising the smart meter, resulting in disclosure of consumer usage. Actually, the nature of a smart meter, and the cost constraints, create a challenge to secure the network. Therefore, the dual motivating problems are the protection of consumer privacy as well as achieving cost efficiency. In this research, we propose a new secure and compromise resilient architecture that continues two major components: a smart meters compromise attack detection scheme and a secure usage reporting protocol. Firstly, the smart meters compromise attack detection scheme improves the security of the smart meter, preventing an adversary from compromising the smart meter. Secondly, the secure usage reporting protocol improves the security of communication between the smart meter and the utility, preventing an adversary from identifying each household's usage reported by smart meters.

Acknowledgements

To ALLAH

I would like to express my deepest gratitude to my supervisor Prof. Xiaodong Lin, who has been a great source of inspiration and encouragement to me. I learned a lot about research styles from him, as well as how to organize the research. His remarkable dedication and knowledge have inspired me to work harder as I continue in the field.

I would like also to express my deepest gratitude to my co-supervisor Prof. Ali Grami, who has been a great source of support guidance.

I would like to thank my mother, as well as my family, for their support throughout the years. I owe to them everything I have ever accomplished.

Table of Contents

List of Figures

List of Tables

List of Acronyms

AES	Advanced Encrypt Standard
AMI	Advanced Metering Infrastructure
AMS	Advance Meter System
CCM	Counter Cipher Block Chaining Message Authentications Code
DSA	The Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECMQV	Elliptic Curve Menezes Qu Vanstone
HAN	Home Area Network
JTAG	Joint Test Action Group
KW	kilowatt
MDM	Meter Data Management system
NAN	Neighbourhood Area Network
PKI	Public Key Infrastructure
RSA	Rivest, Shamir and Adleman
SKKE	Symmetric Key Key Exchanges
SUN	Smart Energy Utility Network
TOU	Time-Of-Use

Chapter 1

Introduction

1.1 Introduction

In recent years, the Smart Grid has grown to be the solution for future electrical energy system that promises to avoid blackouts, while being energy efficient, environmentally and customer-friendly [1]. In fact, the current electric grid system has had a great deal of impact on the economy. For example, in 2003 six billion dollars were lost because of blackouts in the Northeast United States [2]. A great number of American states and Canadian provinces, as well as other countries around the world have been moving towards a Smart Grid; Ontario aims to complete its new system by the end of 2025 [3]. In short, a Smart Grid being developed today will improve the reliability of the current energy system.

The Smart Grid system consists of a great number of subsystems; one of the core systems is the Advanced Metering Infrastructure (AMI). The AMI system is responsible for communicating between the consumers and utilities via two-way communications, in order to collect, store, and analyze energy usage data. Generally, an AMI system has three elements: smart meters at consumers' homes, a metering communication infrastructure between the consumers' homes and utilities, and a Meter Data Management system (MDM). The growth of Smart Grid technology in both industry and academic circles calls for written standards and specifications, but only little effort has been made

which creates a terminology issue. For example, AMI could refer to either the Smart Grid or the Advance Meter System (AMS) [4].

A transition from the traditional energy metering system to the AMI system, requires several enabling technologies. One important technology is the smart meter, which is an electrical device attached to houses to collect consumer energy usages, and then sends the data to the utility company for billing. In fact, the feature of measuring power consumption in real-time is a key element that offers benefits for governments, industries, and consumers [5]. Firstly, governments will benefit from this feature by being able to predict energy use; therefore, they will be able to control energy systems in an effective way, e.g. avoiding blackouts.

Secondly, the industries will have more detailed data about consumer usage via Time-Of-Use (TOU). Typically, TOU means the smart meter measures hour-by-hour energy usage of a house, and then transmits the record to utility providers via two-way communications. Therefore, the industries with current data are able to accurately manage actual energy consumption for each region. Moreover, the utility providers will charge according to the time of the day, with the objective of reducing energy consumption (e.g. at peak time, the cost being higher than off-peak).

Finally, customer-friendly applications are the key elements that benefit the customers by consistently monitoring the active expenditure of energy. In fact, the smart meter

facilitates new applications such as Smart Home [1]. This opens the road for applications to decrease the price of the bill, to manage energy consumption, and to control the devices at residences.

The smart meters have several advantages that make consumers' lives more convenient. For example, as shown in Figure.1, smart meters will provide a clear feedback to consumers, via tracking the spending of energy for each electrical device, such as air conditioners and dishwashers, encouraging consumers to turn off unnecessary devices during peak time with the purpose of reducing cost [5]. Moreover, the smart meter will also control electrical usage in the home, so that each electrical device will send the data to it, as shown in Figure.1. As a result, the smart meter will notify the consumer when s/he forgets to close an electrical device that may harm the consumer in the home. For instance, the smart meter will communicate with the security sensor at home, and then send an alarm to the consumer about possible open window or door.

In short, the AMI offers new applications that develop the energy system through measuring the dynamic spending of energy and permitting a decision to be made; for example, during the peak time consumers may be encouraged to turn off unnecessary electrical devices. Furthermore, the smart meter is a key element in the AMI that has the ability to meter the usage of energy, and then send the data to the utility.

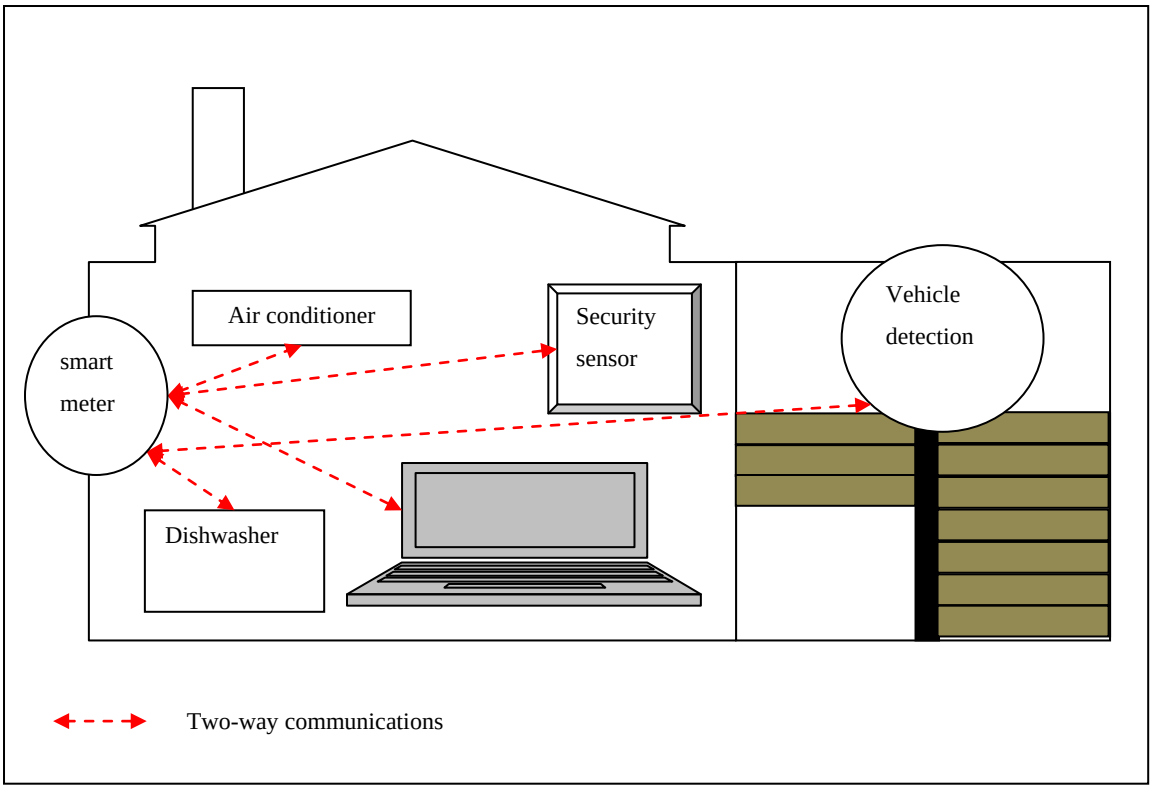

Figure. 1. Smart meter inside the house

While the AMI provides reliability and efficiency for the energy system, it also creates many challenges, in particular security and privacy concerns. For instance, the smart meter, as a part of AMI, collects consumers' hour-by-hour energy usage and then instantly sends the data to the utility, including the individual usage for each electrical device as well as the total usage. Unlike the current energy system that collectively records the general monthly usage of all devices, the way of how the smart meter records and reports the electrical usage could present a record of specific consumer behaviour in the home. For example, anyone can recognize when the consumer leaves home and returns every day by observing the usage of the garage door that is recorded in the smart meter. In addition, it can be recognized when the consumer retires in the evening and

arises in the morning by observing the usage of lights. Hence, knowledge of patterns of behaviour could be an opportunity for an invasion of privacy [5].

A number of studies [6-8] demonstrate the risks that are associated with extract energy consumption from the smart meter, and then applying some kind of analysis such as off-the-shelf statistical methods to determine the lifestyle of the consumer. As a result, once the energy consumption is known, anyone can easily produce a collection of information about the consumer, as shown in Figure. 2.

In summary, the smart meters have detailed information about consumers; therefore, an adversary can distinguish consumer activity and behaviour at home by analyzing the usage that is stored in the smart meter, which creates a critical privacy issue. Therefore, it is essential to ensure that only authorized persons can observe the data.

1.2 Motivation and Objective

In reality, smart meters are generally located in insecure area of the house (outside), so anyone can potentially tamper with the device, depicting the fact that smart meters are low-end devices [9]. In other words, there is great possibility of compromising the smart meter, leading to disclosure of consumer usage. An adversary for example, can recover an encryption key via a physical compromise attack by a programming board connected to smart meters, or by the use of other techniques. For instance, an open-source tool, called KillerBee, can discover the encryption keys in the smart meter which uses ZigBee technology for communication [10]. In fact, the ZigBee is a standard for low-rate

communication that is widely implemented in AMI via mesh network [11]. As a result, when a smart meter is compromised or its data recovered, an adversary can monitor consumer activity and behaviour.

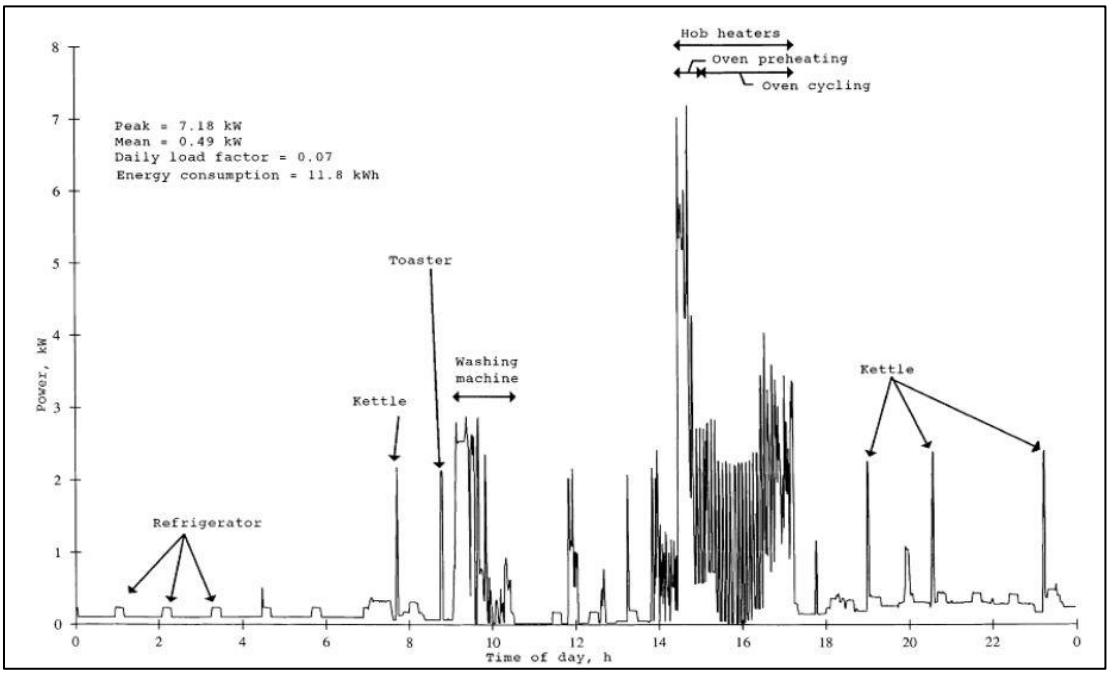

Figure. 2. Household electricity demand profile recorded on a one-minute time from [8]

When an adversary is aware of usage consumption, s/he can use this data to further harm consumers in several ways. First, an adversary can know the consumer's habits and lifestyle because most activities at home require using electrical devices. For example, by observing the reported energy usage, an adversary can distinguish what time a consumer watches television, uses a microwave or oven, and retires in the evening. Secondly, an adversary can use this data in serious crimes such as breaking into and burglarizing a

home, since; an adversary can recognize whether the residents are at home or not. Finally, besides consumer privacy leakage, another concern arises about the selling of consumer data to third parties. For example, a study from the University of Colorado at Boulder demonstrates the risks that are associated with disclosing data from smart meters [12]. The study shows that analysis of specific data from smart meters will represent the lifestyle of consumers; thus, some parties are willing to buy such data, as shown Table. 1. As a result, it could be argued the risks that are associated with disclosing the data in the smart meter are too high. Therefore, any communication channel between customers and the utility should have strict confidentiality which protects consumer privacy.

However, manufacturers that produce smart meters do not pay critical attention to solving the privacy issue. The major functionalities in smart meters are to read the usage, save the data, and then send it via two-way communications. In addition, the manufactures assume the encryption of communication will solve the issue, but this is not the case. Since smart meters are low-end devices, the encryption techniques that are implemented must require low computing. Basically, applying a high encryption approach, such as Public Key Infrastructure (PKI), in smart meters will improve privacy. On the other hand, it does require adding some security hardware for encryption/decryption that increases the price of smart meters and has not yet been attempted as a solution. Since a great number of consumers will purchase it, the cost of a smart meter is quite important due to the fact that the consumer is very sensitive to price [9].

Table. 1. An example of usage analysis

Usage data record	Analysis data	People interested in data
Doors, security sensor	When consumer is away from home	Nefarious
Television	When and how long the consumer watches television	Targeted Marketing
Curling iron, stove range	How often the consumer leaves electrical devices on at home	Insurance Adjusting

The AMI consists of a large number of smart meters that are low-end devices which communicate through a wireless mesh network. The nature of a smart meter and cost constraints, create a challenge to secure the network. In fact, the AMI system suffers from the same challenges and issues as a Sensor Network [4]. However, the risk that is associated with data disclosure in AMI communicating is too high, unlike the usual Wireless Sensor Network. Thus, the two-fold motivations of this research are to protect the privacy of the consumer, as well as to achieve cost efficiency. The objectives of this study are listed below:

- Protecting the communication channel between smart meters and utility collector: an adversary can easily eavesdrop on packets between smart meters and utility; however, we aim to prevent an adversary from recovering and tracing packets.
- Building up a compromise-resilient architecture to protect smart meters: we aim to protect the consumer's privacy on stored memory in a smart meter. Similar to neighborhood watch [13], which is widely used around the world to prevent crime

and vandalism within a neighborhood, we present a scheme that actively monitors smart meters in a neighborhood with the aim of preventing an adversary from compromising the smart meters.

- Achieving cost efficiency by applying the Rabin cryptosystem [14]: we aim to take advantage of a unique feature of Rabin cryptosystem, where fast encryption can be performed in a smart meter and computationally intensive decryption in utility equipment.

1.3 Methodology

In this research, we propose a new secure and compromise-resilient architecture to address the security and privacy issue in AMI. The scheme has two components; the smart meters compromise attack detection scheme and secure usage reporting protocol. The smart meters compromise attack detection scheme improves security by preventing an adversary from compromising the smart meter. The secure usage reporting protocol improves security of communication between the smart meter and the utility with the purpose of prevents an adversary from identifying each household's energy usage. This scheme uses the current smart meters (low-end) devices and protects consumer privacy without needing any additional hardwires.

In fact, we consider the imbalance in the computing power of smart meters and utility equipment; therefore, we move most of the computing tasks to utility equipment instead of the smart meter. The Rabin cryptosystem is notably characterised by its asymmetric computational cost for encryption (or signature verification) operation and decryption (or

signature) operation, where its encryption process is very rapid but decryption process is comparably slow and computationally intensive [14]. The secure usage reporting protocol addresses this feature through applying the Rabin cryptosystem that uses low-computing for encrypting and high-computing for decrypting. Thus, the smart meter will encrypt (low-computing) each household's usage before reporting it to the utility, and the utility equipment will decrypt the encrypted usage messages it receives (high-computing). Moreover, even if the secure usage reporting protocol can protect consumer privacy during the communication channel, an adversary can still easily attack the smart meter device directly and obtain the data since smart meters usually are low-end devices with little protection. Therefore, we further address the smart meters compromise attack detection issue by building couples among smart meters to early detect a compromise attack by actively monitoring each other. The smart meters in the couples will be aware when their partners are under attack.

Protecting consumer privacy in each and every Smart Grid element seems a challenge due to the different levels of consumer privacy in the Smart Grid, including reviewing the bill online, calculating the bills, and collecting the usage data from smart meters. Moreover, the Smart Grid contains a number of subsystems including the Distribution System, Transmission System, and Generator System. In this work, we mainly focus on the privacy of the communication channel between smart meters and the Data Concentrators in the phase of collecting data from smart meters. Also, there are many ways to communicate between the consumer and the utility, including wire and wireless

techniques, such as wireless LAN, WiMAX, 3G/4G cellular, and ZigBee. However, the current research considers the wireless mode in sending data from a meter to a utility, as shown in Figure 3, which is one of commonly used methods.

1.4 Research Contributions

This thesis demonstrates the specific AMI privacy challenges. In order to address these security and privacy issues, we propose a secure and compromise-resilient architecture for AMI. The major contributions of this thesis are listed below:

- Due to the fact that the smart meter is a low-end device located in insecure neighborhood, it prevents us from utilizing sophisticated security mechanisms to ensure security and privacy. As well, it can be easily compromised due to limited protection. We design a secure and compromise-resilient architecture to address this problem by adapting two techniques, Rabin cryptosystem [14] and neighborhood watch [13]. First, we design a new security protocol using Rabin cryptosystem, where at smart meters side only low-computing operations are performed and computationally expensive operations are performed at the utility collectors, which are considered computational powerful devices. Secondly, we propose a novel detection technique likewise the idea of neighbourhood watch, which allows smart meters to monitor each other to detect any smart meter compromise attempts in the early stage. As a result, it can significantly improve security when the smart meter is under physical attack.

- We have designed a secure usage reporting protocol for collecting consumption usages from smart meters to a utility collector by adopting Rabin cryptosystem [14]. We utilize an encryption Token-Ring with specific structural design that guarantees the security and privacy even though the smart meter and utility collector located in insecure neighbourhood.
- Extensive analysis on security and privacy of the proposed secure and compromise-resilient architecture is conducted. The results demonstrate the effectiveness and security of the proposed architecture.

1.5 Thesis Organization

The remainder of the thesis is structured as follows. Chapter 2 describes the background of the architecture of the smart meter and its current security provisions. It also surveys state of the art of ensuring the security or privacy of the smart meter. Chapter 3 presents the proposed scheme and the assumptions including network model, attack model, and design goals. Chapter 4 discuses the potential attacks and how the proposed scheme resists the attacks. The last chapter concludes this research and discusses future work in this area.

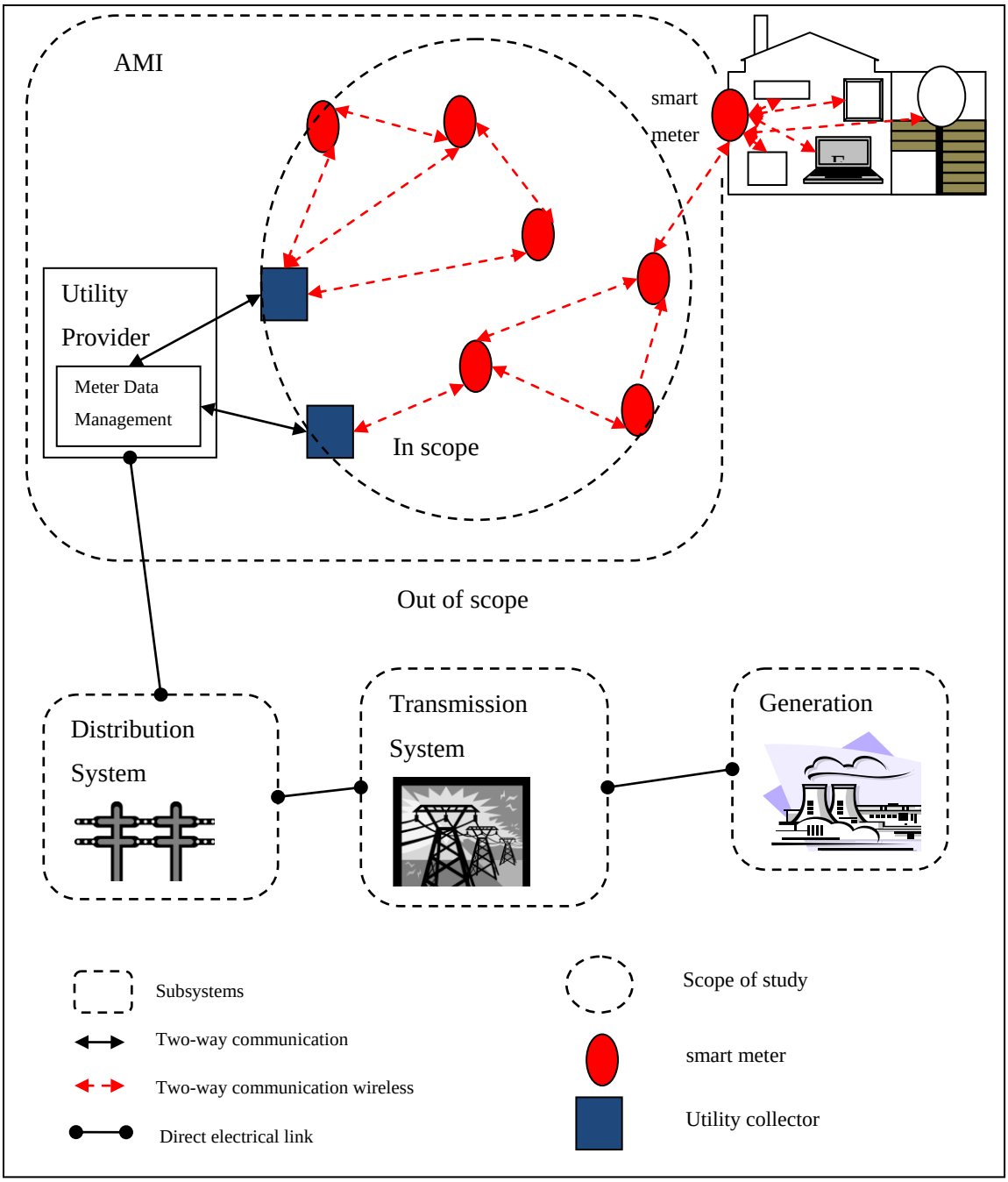

Figure. 3. High overview of smart grid

Chapter 2

Literature Review

2.1 Background

In this section, we will discuss the architecture of the smart meter and the current security conditions that could lead to an attack in the AMI system. First, we will provide the general smart meter architecture, and then we will review the state of the art of AMI.

2.1.1 The Smart Meter Architecture

A smart meter consists of three majors modules, as shown in Figure. 4, 1) microprocessors, 8, 16, or 32-bit microcontrollers (MCUs), such as the Cortex CPU M series and Cirrus Logic's CS7401xx series, which have limited RAM or flash memory, and 2) sensors module that is measuring the consumption of energy. 3) communicating modules, either wire or wireless or both; however, the ZigBee wireless communication is widely used. It may have an additional option of the LCD display that shows the consumption [15]. For example, the MCU CS7401xx uses ARM7TDMI™ 16/32-bit RISC CPU, and from 32kB to 128kB On-chip Flash Memory, and 8 kB On-chip RAM. The CS7401xx has Joint Test Action Group (JTAG) Interface for fixed debug. In short, the smart meter builds on microprocessors that have limited memory and computing capability.

This study considers the current hardware limitations of the smart meter. In fact, adding new hardware or modifying an existing smart meter with the purpose of improving

security would be very costly for two reasons. Firstly, a great number of smart meters have already been installed around the world, e.g. Hydro Corporation was responsible for installing 1.3 million smart meters by the end of 2010 in Ontario [16]. Therefore, recalling these devices and re-installing them will be costly. Secondly, the price of smart meters will increase due to the powerful processors necessary to improve the computing power and memory. Briefly, the new proposed scheme will protect privacy without the necessity of adding new hardware that provides high computing and memory.

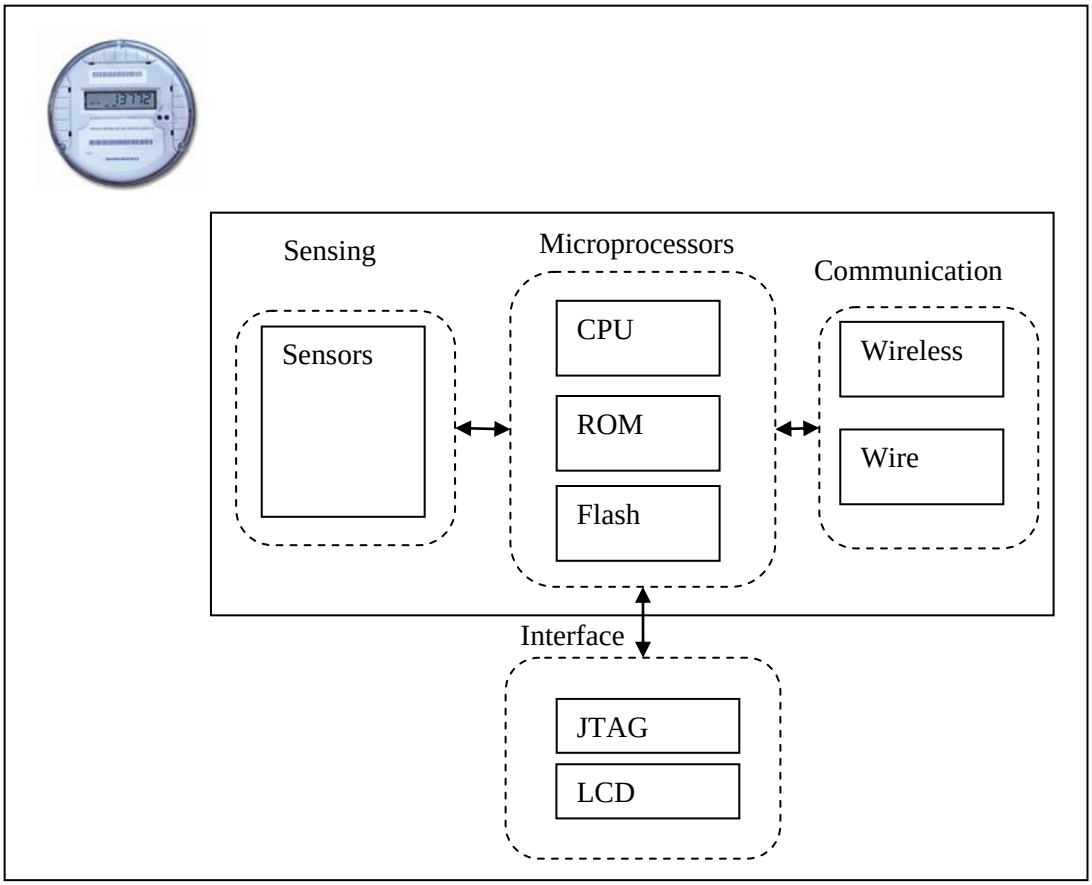

Figure. 4. The smart meter architecture

2.1.2 Security of Current Smart Meter Technology

In this section, we will evaluate the current security of the smart meter including the AMI and the network. Then, some considerations and requirements to secure the smart meter will be reviewed.

2.1.2.1 Smart Meter Security

AMI is an important element in the Smart Grid; therefore some effort has been made to review security and related issues [17]. In fact, the open Smart Grid Users Group published a security specification [18] and Security Implementation Guide [19] for the AMI; nevertheless, the AMI still has security concerns. It has been shown that smart meters have a high risk of being compromised in view of the fact that all devices are installed in insecure neighbourhoods. As a result, an adversary can easily launch a physical attack. Furthermore, a compromised single device might lead to the compromise of others. Another study shows that the AMI presents a threat with data transfer because the smart meter is a low-end device. In fact, it has shown a number of successful attacks to compromise the low-end via the JTAG interface [10] and [20]. Briefly, a number of standards have been published in order to secure the AMI, even though it still has vulnerabilities.

2.1.2.2 Wireless Network Security

Most smart meters are deployed using a wireless network over other choices because it is self-organizing and low-cost. A number of AMI implementations utilize mesh network among wireless devices that offer self-adapting, multi-path, and multi-hop communications between the AMI devices. Examples of a wireless mesh network

standard include ISA 100.11a, Wireless HART, and ZigBee, all of which have been widely implemented. However, all of these standards need more time to improve security, yet there are already vulnerabilities such as denial-of-service attack on IEEE 802.14.4. In fact, the AMI wireless technology is insecure, despite the vendors' claim simply because the vendors were under the initial pressure of marketing, and paid little attention to the issue of security [17].

In summary, an adversary can compromise a smart meter by using various tools such as KillerBee [10], which will break consumer privacy. Until now, the security specifications [18] and security implementation guidelines do not succeed in protecting security and privacy. As a result, there is a need to improve the security defensive in order to protect the privacy which the current study is attempting to achieve.

2.1.3 Smart Meter Security Requirements and Constraints

The smart meter as a part of AMI has specific characteristics that make it difficult to secure; however, any attempt at solutions to secure it without considering these characteristics will be unsuccessful. As this study attempts to protect consumer privacy; this section will review these requirements.

Cleveland [9] analyzes the privacy issue in the smart meter and recommends that there should be security techniques which can prevent unauthorized access to discover the consumption of energy either on the smart meter or on the communication channel.

However, these techniques have restrictions that should be considered when else is possible [9].

Firstly, a great number of consumers will purchase a smart meter, so the cost is quite important. Adding memory or a processor to secure the smart meter will increase the price. As a result, the security technique that attempts to secure the smart meter should not need to increase the price by adding hardware, e.g. for encryption/decryption. Furthermore, the smart meters are placed in insecure locations, so they can be easily accessed. As a result, a physical detection such as wall or glass cannot secure the smart meter, so there is need for other techniques.

Secondly, the majority of communications between the elements in the AMI are based on low bandwidth, such as ZigBee and WiFi. Therefore, a security approach requiring a high bandwidth to secure the AMI (such as sending a large certificate), will be impracticable. Moreover, a number of the AMI elements will communicate via the public telecommunications services, so that perhaps eliminates the security approaches that could be implemented.

The current study considers the [9] effort. In fact, the new scheme does not require adding new hardware for protecting privacy. Moreover, it will consider the weakness of physical detection, so it will protect the device even when physical protection fails, such

as if the glass is broken. Also, the new scheme will be based on low-rate transition, and it does not require transfer a large data for security.

2.2 Related Work

This section will review approaches that attempt to improve the security or privacy of the smart meter. Three areas are evaluated: communication, privacy, and security detection.

2.2.1 Smart Meter Communication

As the Smart Grid is growing today, it is supported by academic research and industry, which need to define a standard; however, little effort has been made. In Canada, the US, and Europe a number of standards have begun to be developed. An example of such standards is the "Government of Ontario IT Standard Advanced Metering Infrastructure" [11]. This considers determining each element in the AMI that could be out of the scope of current study, which protects consumer privacy, not in each and every element in the system; specifically, the communication between smart meters with utilities, or smart meter with smart meter.

One of the standards [11] is Wireless Personal Area Network (ZigBee) that is recommended for low-rate transmission in smart meters. The ZigBee standard offers security methods that protect the network and applications layers. The network layer applies the Advanced Encrypt Standard (AES) with the Counter Cipher Block Chaining Message Authentications Code (CCM) that guarantees authenticity and privacy which is central to current research. In fact, the ZigBee meets all requirements and polices for

[11]; moreover, it meets all requirements for Open HAN Network System Requirements (NSRS) [21] that are being developed in the US. Briefly, most current utilities use ZigBee, which meets the standard.

Shah *et al.* [22] presents an analysis of power management by using the ZigBee wireless that is based on cost saving. ZigBee has several advantages, as such has made it a standard. In fact, the ZigBee is an open standard, developed by the ZigBee Alliance, so it reduces the cost of licenses. Moreover, it supports a mesh network; hence, the meters can communicate directly with each other. As is shown in [22] implemented ZigBee in smart meters has advantages over Bluetooth. In this research not only the cost efficiency is considered, but also protection of consumer privacy by securing the communication between the meters is investigated. Up to date standards do not address security issues. For instance, Joshua Wright has shown an attack against ZigBee that can sniffer the data and get the Key [10]. Thus, the current research will address the privacy of consumers. In a word, the ZigBee could apply to other techniques of encryption to achieve both cost efficiency and privacy; however, current implementation achieves only cost efficiency.

Yang [23] reviews the Security in the Wireless Sensor Network based on the ZigBee standard; consequently, the ZigBee has several issues including channel interference, address conflict, and weakness in ASE repudiation. The cause of the weakness in ASE is a symmetric key encryption. As a result, the two nodes should exchange the key before they communicate; consequently during key exchanges any adversary can potentally

eavesdrop. The adversary can then simply use the key in order to compromise the nodes. Actually, the National Institute of Standards and Technology considered AES-128 encryption will be secure until 2036; nevertheless, up to the present, it has been broken only in a five minute attack. Furthermore, symmetric key encryption has issues with key management when the number of nodes becomes huge. As Yang [23] suggests applying Elliptic Curve Cryptography (ECC) might solve the issues since it is asymmetric authentication and key exchange [24].

Blaser [24] demonstrates that the ZigBee standard is ideal for a low wireless network since it meets all of the requirements of manufacturers and businesses including a number of advantages such as saving power and cost. In addition, it supports security in different layers. However, Blaser identifies the security issue in ZigBee that is using Symmetric Key Key Exchanges (SKKE). SKKE is fast and has low-cost implementation; on the other hand, it has security issues such as key exchange. As [24] suggests applying public key algorithms based on ECC could solve the issue. The advantages of using ECC are scalability and non-repudiation, while ECC uses one key instead of many. Additionally, ECC has advantages over the traditional public key system which are faster computations and less significant key size. For instance, Rivest, Shamir and Adleman (RSA), The Digital Signature Algorithm (DSA), and Diffie-Hellman are not good systems because those require large key and huge computing. As shown in [24] using the ZigBee with ECC will improve the security of communication, and it can fit more than the traditional public key system.

In fact, [24] applies Elliptic Curve Menezes Qu Vanstone (ECMQV) as a key establishment mechanism for ZigBee. However, ECMQV is not approved and has been dropped from the National Security Agency's cryptographic standards. The reason behind that is ECMQV uses signed Diffie-Hellman although, which is vulnerable to a man-in-the-middle attack.

Jincheol Kim [4] *et al.* proposes a solution to secure communication between the AMI and Smart energy Utility Network (SUN). Due to improved security in standard protocol, IEEE 802.15.4 and ZigBee Alliance that uses SKKE is a recommended protocol for Key establishment and management. This proposal is based on public key cryptography, and as is shown in [4]; the algorithm depends on four phases: Key establishment, data encryption/decryption, key and trust data update, and finally orphan node management. As [4] concludes, the proposed algorithm gets better than the SKKE algorithm when the number of hops is more than 2 hops. However, this research aims to discover a secure communication algorithm in order to protect the privacy of the consumer as long as it maintains cost efficiency. In fact [4] does not provide the computing power necessary to archive the public key algorithm which is assumed higher than SKKE.

In summary, several approaches have been provided to secure a communication channel between smart meters and utilities collectors. However, these approaches have concerns either in the security or cost efficiency. First the issue of security means the approach has been shown insecure or broken. Secondly cost efficiency means the approach might be

secure, but requires adding some functionality that increases the cost of smart meters rather significantly. Unlike the above mentioned approaches, the proposed scheme achieves both privacy and cost efficiency.

2.2.2 Smart Meter Privacy

The smart meter privacy concern is ability to obtain the consumption of energy data either on stored memory or on the communication channel. Since the smart meter has valuable information about consumers that could be used to explore the consumers' lifestyle, this section will review a number of proposed schemes that aim to protect privacy in smart meters.

Efthymiou *et al.* [25] review the issue of privacy in the Smart Grid; specifically, during the transmission of data from the smart meter to the utility every few minutes. Typically, the data can identify the lifestyle of the consumer since the smart meter data can easily link to householder location by observing the sender of data. Consequently an adversary is able to analyze the data frequently. In order to prevent the issue, Efthymiou *et al.* suggests applying anonymization of smart metering data.

Accordingly, the smart meter sends data anonymously; in other words, without associating the data with the real identity of the smart meter that refers to the identity of the householder. It instead uses an anonymous identity. The utility collects the data from the smart meter with an anonymous identity and then authenticates the data via an escrow

service. As only the escrow service is aware of the two identities of the smart meter, the service must be a trusted party between the consumer and the utility provider.

The effort of [25] relies on a trustworthy third party escrow service; nevertheless, that could be an issue if the third party does not establish trust. The whole system in this case would be unsuccessful. Furthermore, [25] does not provide the technique that prevents an adversary from observing the usage of energy. It only blocks the identities of the consumers, preventing the adversary from linking the usage with identified consumers. When an adversary continues to observe the usage of a small group of smart meters over a long period of time, it is possible to link the data. This work protects privacy, including the usage, by applying the encryption technique that prevents an adversary from observing the identity and the usage.

Fengjun *et al.* [26] proposes a solution to protect privacy on the communication channel between the smart meter and the utility collector, so that an adversary who eavesdrops the messages is not able to distinguish between the usage of each smart meter. As a result, the proposal will also protect the consumers' privacy.

The contribution of [26] applies data aggregation for the usage data with homomorphic encryption passing through an aggregation tree when the smart meter transfers the data to the utility collector. This means that each smart meter sends the usage data to neighborhood's smart meter, uses homomorphic encryption to protect the data, and then

transfers the data results to the next smart meter continually, until the data reaches the collector. As a result, only the utility collectors are able to identify the usage of each smart meter; yet an adversary may still capture the sum total data for smart meters in a neighbourhood.

The effort of [26] relies on accurate data from smart meters, and Fengjun *et al.* assumes that physical security must be improved in order to prevent fabricated data. However, this study will improve physical security in order to protect consumer privacy. Furthermore, Fengjun *et al.* uses homomorphic encryption on each smart meter that increases the computing power, and they assume the encryption computation will not be an issue from the overhead prospect since they apply asymmetric encryption. However, it will be an issue from the computing power perspective. This study will consider the imbalance in computing power that the smart meter and the collector have. Therefore, the new scheme will move most of the computing power to the utility collector as a powerful device, unlike the smart meter that is low-end.

Kalogridis *et al.* [27] propose a solution to protect the privacy of the data that is stored in the smart meter, so they obfuscate the energy usage. They achieve the goal of protecting privacy by avoiding the identify of the consumption of each electrical device; as a result, the data that is stored in the smart meter cannot determine the habits of consumers.

The contribution of [27] applies the "load signature moderation" that combines the consumption of energy from the utility with a rechargeable battery. For example, "a kettle drawing 2kW of power when switched on; the power router could be configured so that 1kW is supplied from a solar panel, 0.5kW from a battery, and 0.5kW from the mains electricity supply [27]". As a result, when an adversary observes the usage data from the smart meter, s/he cannot recognize the behavior of consumers, thus protecting privacy.

Actually [27] has two issues with the rechargeable battery. First, it will be costly to provide each resident with a rechargeable battery; second, the rechargeable battery charges from the electricity supply, so that will in fact be wasting instead of saving energy. However, the motivation of this study is to protect the privacy of consumers as well as achieving cost-efficiency. The new scheme does not require adding new equipment to protect privacy.

2.2.3 Smart Meter Security Detection

Several approaches have been provided to protect privacy in the smart meter. They could be applied to different schemes to improve privacy; however, they cannot stand alone. Improving privacy without improving security in the smart meter device will not make the grade schemes that protect privacy. Actually, it does not matter how much the scheme can protect privacy when an adversary can easily attack the device directly, and then obtain the data. Therefore, the current research will initially improve the security in order to protect privacy. This section will review some techniques to improve security on the smart meter.

Xiaodong [28] proposes a solution to protect sensor nodes from compromise, so that the scheme will notify any attempt of physical attack by an adversary. The proposal is to protect the sensor node compromise attack in the early stage, which is the first effort to address this issue.

The contribution of [28] applies a couple-based scheme to detect potential physical attack. This means that each sensor node builds couples with a neighborhood sensor, then the couples monitors each other. As a result, any attempt to compromise the node can be detected.

We will consider the effort of [28], and utilize a similar scheme to improve the security of smart meters in the network. However, the scheme in [28] will send an alarm when anyone tries to connect to a sensor including an authorized person, thus increasing the potential from false-positive alarm; however [28] does not provide a scheme to clear a false-alarm once it has occurred. This will be an issue for the AMI because the utility provider is responsible for performing maintenance and repairs on smart meters. Consequently, the smart meter will send an alarm to the couple each time the utility provider performs maintenance; nevertheless, this study will also address this issue by proposing a false alarm clearance.

Chapter 3

Secure and Compromise-Resilient Architecture for Advanced Metering Infrastructure (AMI)

In this chapter, we introduce a new couple-based scheme to detect the smart meter compromise attack. Also, we will present a secure usage reporting protocol to further defend against several threats on information transmitted between the smart meters and the utility collector.

3.1 Preliminaries

In this section, a brief review on the basis of Rabin cryptosystem is given, which serves as important background of the proposed secure and compromise-resilient architecture for advanced metering infrastructure.

3.1.1 Rabin Cryptosystem

To illustrate the Rabin cryptosystem, as shown in Figure. 5, Alice sends an encrypted message to Bob, Alice and Bob will follow the steps below [14].

1- Key generations: Bob generates two keys one to encrypt (public) and the other to decrypt (private).

   a. Generate two random prime numbers p and q that are the matching size.

   b. Compute n =q*p.

   c. The public key is n and the private key is (p,q).

2- Encryption: Alice receives the public key of Bob that is n, and then encrypts the message M for Bob.

a. Express the message plaintext as a number.

b. Compute the cipher text $C \equiv m^2 mod\ n, c \in N$.

c. Send *C* to Bob.

3- Decryption: Bob receives the *C* from Alice.

a. Recover the 4 message plaintexts m1,m2,m3,m4 then $m_i^2 \equiv c\ mod\ n$, i1,4.

b. Distinguish the plantext from four message.

c. Recover the original messages m.

Rabin encryption operation is faster than the decryption operation because the encryption is just modular squaring. Nevertheless, the Rabin decryption operation has speed similar to the RSA operation. Moreover, the Rabin scheme relies on the hard problem of factoring large integers; for more specific information see [29].

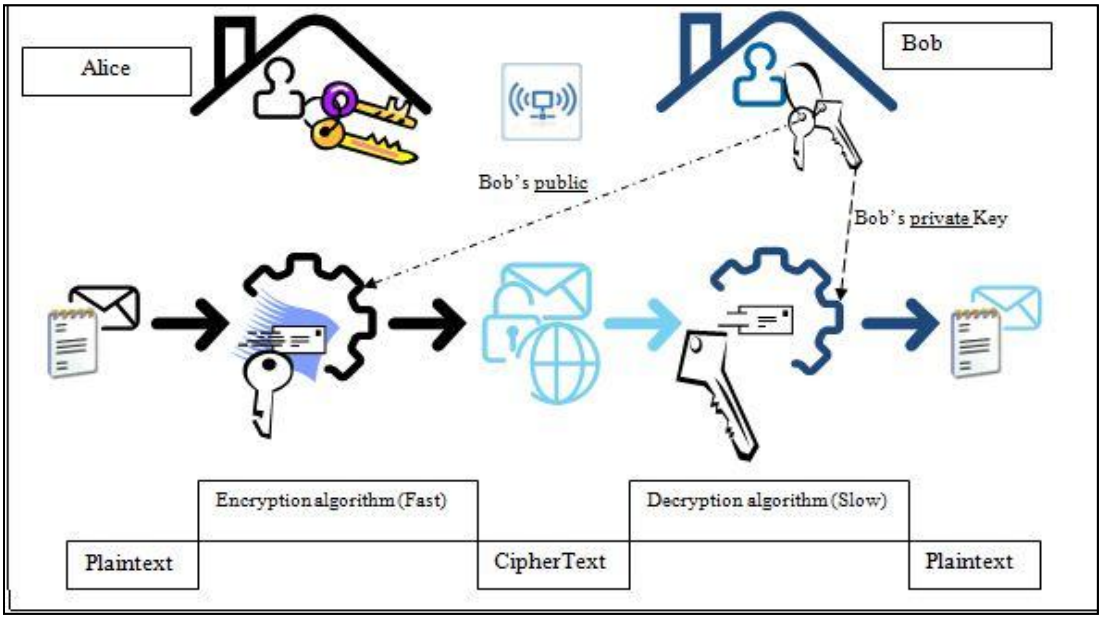

Figure. 5. Rabin cryptosystem

3.2 System Model and Design Goals

In this section, we will give details about the network model, the attack model, and the design goals. For clarity of discussion, the notations throughout this section are listed in Table. 2.

3.2.1 System Model

We assume the utility provider is responsible for deploying and installing smart meters in each residence along with a Neighbourhood Area Network (NAN). Therefore, each region has numerous houses and one utility collector, and where each house has one smart meter; this denotes a community.

Table. 2. Notations

Notations	Descriptions
S_i:	the i-th smart meter
UC_i:	the i-th utility collector
M_i:	the i-th maintenance device
Y_i :	the public key of i
x_i :	the private key of i
K_i :	a key shared between S_i and a S_j
TS_i :	A timestamp that records the current time when S_i sends message
σS_i(m) :	i's digital signature on m, where σ as the Naccache-Stern signature
RE_Y(m):	Encrypt the message m with a Rabin public key algorithm scheme, where Y is the public key of UC

Notations	Descriptions
$RS_x(\mathrm{m})$:	Signature on message m with Rabin signature scheme, where x is the private key of M
$\|\|$:	Message concatenation operation, which appends several message together in a special format

The smart meter only reports usage device, and it may provide unsophisticated functions such as sending an alarm and interacting with smart appliances at home. However, the smart meter does not provide network services, which mean it is not vulnerable to typical network based attacks. As a result, an adversary cannot lunch remote malicious attacks by exchanging directly a message with the smart meter. In our design, the smart meter actively monitors the power consumed by electrical devices in Home Area Network (HAN), and forwards the data to the utility provider, accordingly; all devices in the HAN send their usages to the smart meter at the home via low-rate wireless.

The utility provider manages the entire NAN, so it amasses all of the usage data from smart meters via a utility collector. The utility collector is a powerful and trustworthy device that collects all usage from every smart meter in a neighbourhood via the mesh network model in NAN, then transmits the data to the utility billing system. By way of transferring the usage from the smart meter to the utility collectors, the smart meter communicates through two-way communications; each smart meter can send and receive the data only from neighbours with low-rate wireless communication, as shown in Figure. 7. After transferring the data from each smart meter to the utility collector, each smart

meter will resend the data from the neighbourhood meter until the packages reach the utility collector. All communications and routing in the NAN however are driven by the utility provider.

3.2.2 Attack Model

This research will investigate the threats to communication between the smart meters and data concentrators, assuming an adversary has physical access to the smart meters and compromises them, since the smart meter is located in insecure area. Moreover, an adversary can simply perform passive attacks such as eavesdropping with a powerful device. In particular, we consider that an adversary can launch the following attacks to either subvert privacy or degrade the performance of the smart meter.

1. Packet recovery: an adversary can eavesdrop on packets between smart meters, which are received and analyzed in order to recover the content of data. In other words, this will potentially threaten consumer privacy because an adversary can know the lifestyle of the consumer by observing the moment in time and electrical usage of activites such as watching television, or cooking by oven.
2. Packet tracing: an adversary can eavesdrop on packets between smart meters, which are received and analyzed in order to identify the sender of the data. In other words, an adversary can be aware of when and how long the consumer is away from home by observing the particular smart meter activity.
3. Compromising the smart meter: an adversary can launch a direct physical attack by using some sort of tool and then obtaining all of the keys that are stored. For

instance, an adversary can use a programming board and serial cable that are connected with JTAG interface in the smart meter in order to compromise the meter.

3.2.3 Design Goals

This research aims to improve the security and privacy in smart meters by developing a new scheme. With regard to improving security, the outcome of the research will apply a detection scheme in order to avoid a smart meter compromise attack. As a result, each smart meter will be aware when an adversary attempts to launch an attack, so it will send an alarm to other devices and the utility collector. In order to improve privacy, the outcome of the research will propose a new protocol that protects privacy by applying the Rabin public key scheme [14]. A number of considerations are illustrated below.

1. Send data via low-rate communications: each smart meter can send/receive data from a neighbourhood in a secure technique that protects privacy.
2. Cost effectiveness: A great number of people will buy smart meters, so the cost will play a major role in an attempt to achieve privacy. For example, as a promising security infrastructure, PKI will protect consumer privacy; however, it also requires high computing from the smart meter and additional hardware for encryption may need to be added.
3. Privacy of consumer in a communication channel: There are different levels of risk to consumer privacy in the Smart Grid, such as reviewing the bill online or calculating the billing system. However, this research focuses on the privacy of

the communication channel between the smart meter and the Data Concentrators in the phase of data collection from the smart meter.

4. As a result of the imbalance in the computing power which smart meters and utility equipment have, most of computing will move to the utility equipment instead of the smart meter.
5. Other security goals: In terms of security, there are a numbers of goals that should be considered in order to protect information transmitted in the NAN including confidentiality, integrity, authentication, and non-repudiation.

3.3 Proposed Secure and Compromise-Resilient Architecture for Advanced Metering Infrastructure

In this section, we illustrate the proposed secure and compromise-resilient architecture for advanced metering infrastructure, which contains two components including smart meters compromise attack detection scheme and secure usage reporting protocol.

3.3.1 Smart Meters Compromise Attack Detection

The smart meters compromise attack detection scheme has four phases:

1. Smart meters initialization;
2. Couple building;
3. Smart meters compromise detection;
4. False alarm clearance.

The main advantage of this scheme is that it prevents an adversary from launching a direct physical attack by using a programming board and a serial cable that is an easy way to compromise the smart meter. We adopt detection scheme that protects any smart

meter compromise attempts in the early stage. Different from other schemes it also allows authorized connection with a programming board such as maintenance. The Figure. 6 demonstrates the possible situations that could occur on the scheme. We illustrate the proposed scheme in detail in the following.

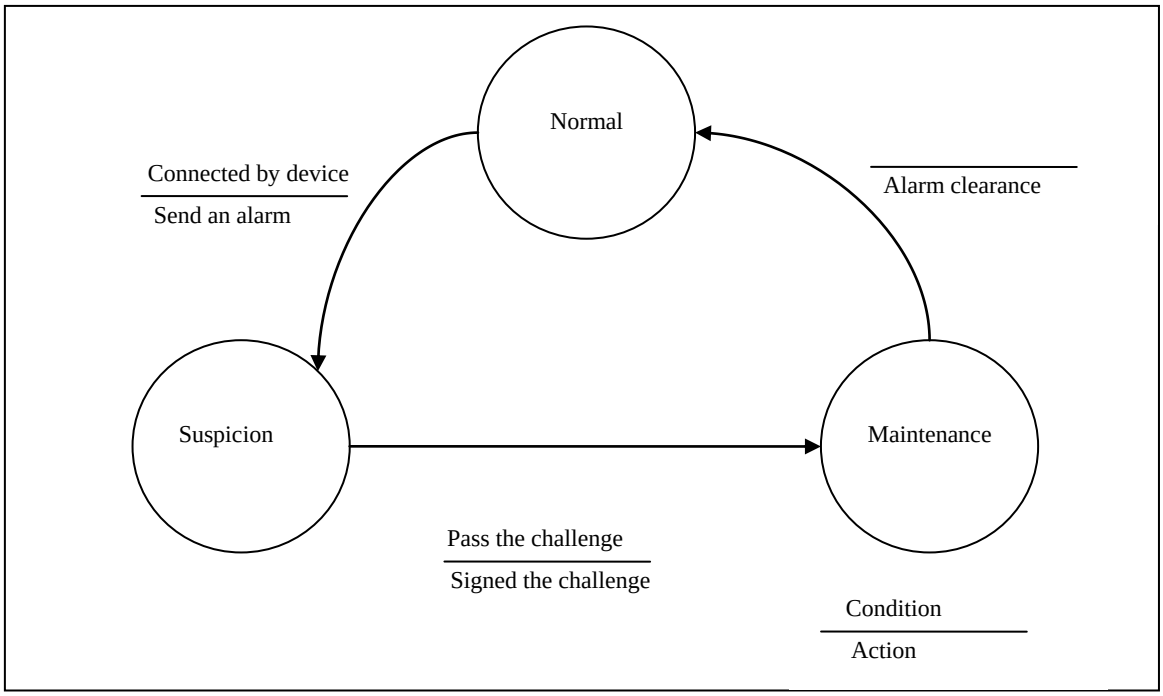

Figure. 6. State-transition diagram of smart meter

Normal to Suspicion: when the smart meter connects with any device, the smart meter sends an alarm to other couple.

Suspicion to Maintenance: when the suspicion device passes the challenge that sends from the smart meter.

Maintenance to Normal: After the smart meter verifies the challenge, it sends alarm clearance to other couple.

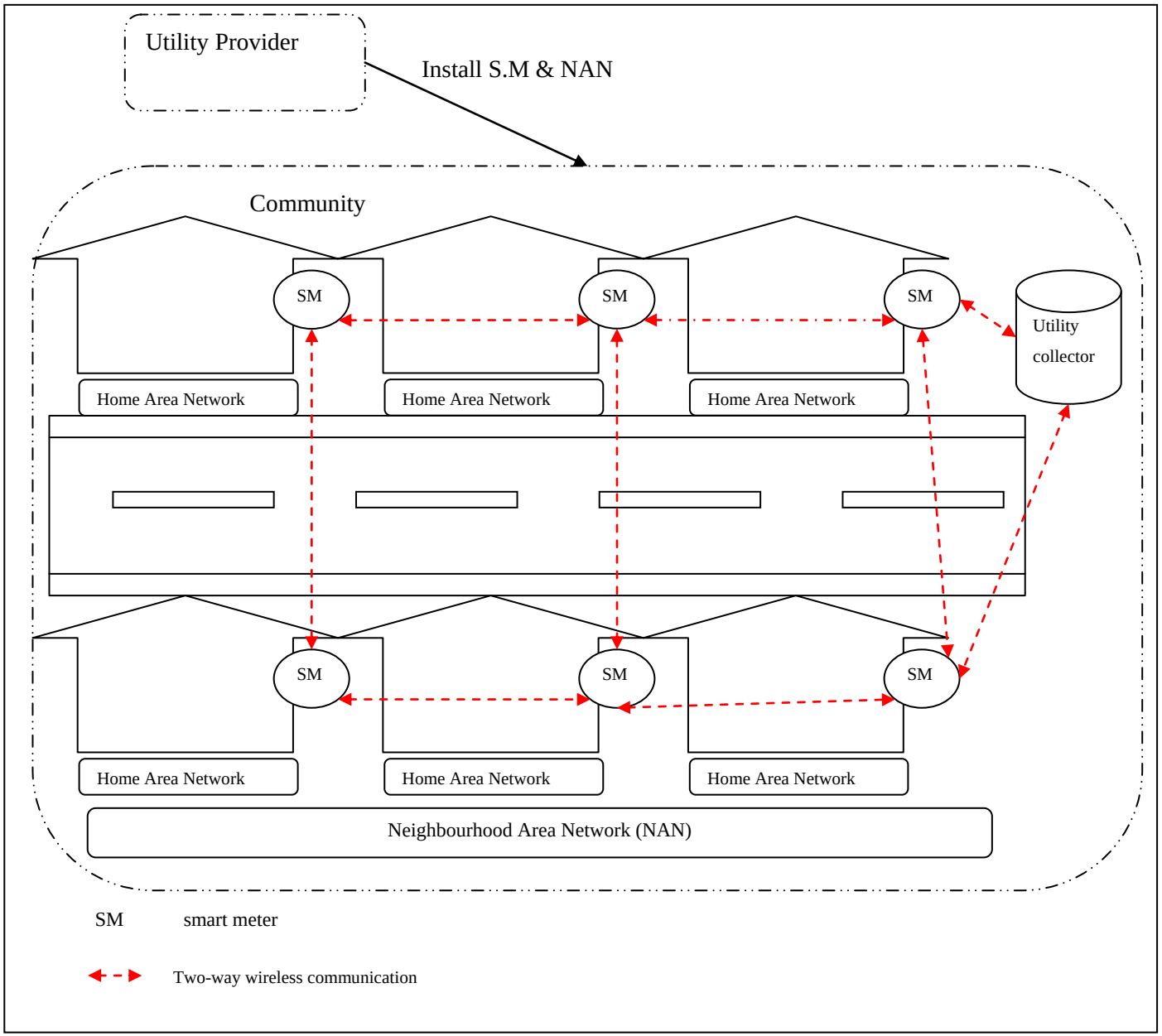

Figure. 7. The smart meter network

3.3.1.1 Smart Meters Initialization and Deployment

The utility collector selects an acceptable elliptic curve E built in Tiny ECC and a base point G of order r in E [30]. Next, the utility collector initializes smart meters $S = \{S_0, S_1, S_2, \ldots, S_n\}$ by applying the Algorithm 1. In the end, the utility collector sets up the initialized smart meters in a neighbourhood via wireless communication. However, the utility provider is responsible for deploying and installing all smart meters; as a result, they will be installed in all houses in the NAN. Therefore, the smart meter S_i may have many neighbors with which it can communicate.

Algorithm 1 Smart Meters Initialization

1: Procedure SMARTMETERSINITIALIZATION
Input: un-initialized smart meters $S = \{S_0, S_1, S_2, \ldots, S_n\}$
Output: initialized $S = \{S_0, S_1, S_2, \ldots, S_n\}$
2: for $i = 0$ to n do
3: randomly choose a private key $x_i \in [1, 1 - r]$
4: compute the corresponding public key $Y_i = x_i \cdot G$
5: preload smart meter S_i with key pair (x_i, Y_i)
6: end for
7: return initialized $S = \{S_0, S_1, S_2, \ldots, S_n\}$
8: end procedure

3.3.1.2 Couples Building

With the purpose of improving the security in AMI; all smart meters in the same NAN will observe each other in order to detect potential compromised attack. Smart meters can

achieve that by building couples in an *ad hoc* model once they are deployed, so that each one from the couples will be aware when the other smart meter is under attack. As a result, the utility collector will notice the compromise and quickly react to the attack. For example, a pair of smart meters within their transmission range in a NAN build couples, one as **H**-Meter (**H**usband Meter) and the other as **W**-Meter (**W**ife Meter), as shown in Figure. 8. In order to build the couples, the candidate meters will execute the following steps, assuming there are n smart meters, and the candidates Meters are S_i, S_j .

Step 1: S_i selects a random number a ∈ [1,r − 1], computes A = a.G, and sends (S_i,A) to S_j .

Step 2: After receiving (S_i, A), S_j selects another random number b ∈ [1,r − 1] and computes B = b.G. Next, S_j applies the Naccache-Stern signature [31] to create a signature on A||B||S_i as σS_j (A||B||S_i). In the end, S_j sends (S_j, B, σS_j (A||B||S_i)) to S_i .

Step 3: when S_i receive (S_j,B,σS_j(A||B||S_j)), S_i verifies the validity of the signature σS_j (A||B||S_i).when it is valid , S_i creates a signature on B||A||S_j as σS_i (B||A||S_j) and send the signature to S_j. As well, S_i computes the shared key K_i= h(a.B)= h(ab.G), where h: $\{0,1\}^* \rightarrow [1, \mathrm{r} - 1]$ is a secure hash function.

Step 4: when S_j verifies the validity of σS_i (B||A||S_j), S_j also computes the shared key S_j= h(b.A)= h(ab.G).

After the shared Key is calculated, that is $K_i = K_j = \mathrm{h}(\mathrm{ab.\,G})$, S_i and S_j become a couple, responsible to monitor each other, in order to detect compromise attacks. After couples have been built, each couple will send and receive the beacon information during

synchronization time between the Husband Meter and the Wife Meter. As a result, when couple meter does not receive beacon information or incorrect beacon information from its partner, it will assume the other meter is under compromise attack. For example, S_i computes $K_i = K_i + 1$ each interval of time, then it sends $\text{Beacon}_i = h(k_i||S_i||1)$ to S_j. When S_j receives the broadcast (S_i , Beacon_i), it will compute $K_j = K_j + 1$ first, then compare the result with $\text{Beacon}_i = h(k_j||S_i||1)$. If they match, that means S_i is normal; otherwise it means that it is compromised.

3.3.1.3 Smart Meter Compromise Attack Detection

There are four notifications in the detection scheme that are sent between the couples (S_i, S_j) during each interval time. The first is the normal situation, where S_i computes $K_i = K_i + 1$, then it sends $\text{Beacon}_i = h(k_i||S_i||1)$ to S_j. The second is the detect situation, where S_i computes $K_i = K_i + 1$, then it sends $\text{Beacon}_i = h(k_i||S_i||0)$ to S_j. The third is the fake beacon or unreserved beacon, where S_j does not receive valid beacon from S_i. Finally, is the maintenance situation, where S_i computes $K_i = K_i + 1$, and then sends $\text{Beacon}_i = h(k_i||S_i||2)$ to S_j. As a result, the couple smart meter S_j can recognize the situation by the Algorithm 2. Therefore, once the adversary connects with S_i in order to compromise the smart meter, the S_j will receive $h(k_i||S_i||0)$. As a result, Exception II occurs; that means the S_i connected with the adversary. Similarly, Exception I occurs as soon as the S_j does not receive the Beacon_i, which means the adversary has shut down the S_i. Also, Exception III occurs when the maintenance device M signs the challenge from S_i, so S_i expects physical connection by a programming board during $\boldsymbol{T_t}$, then S_i will

send a clear alarm beacon to S_j. In the end, the utility collector will receive a report about each smart meter in the NAN, and will initiate a reaction to it.

Algorithm 2 Detect Smart Meter Compromise Attack

```
1: procedure DETECTSMARTMETERCOMPROMISEATTACK
2:     if S_j receives a valid beacon Beacon_i from S_i every a predefined
       period T_t then
3:         S_j = S_j +1
4:         if Beacon_i = = h(k_j||S_i||1) then
5:             return Normal
6:         else if Beacon_i == h(k_j||S_i||0) then
7:             return Exception II
8:         else if Beacon_i == h(k_j||S_i||2) then
9:             return Exception III
10:        end if
11:    else if S_j doesn't receive a valid beacon Beaconi from S_i every a
predefined period T_t then
12:        return Exception I
13:    else
14:        return Exception I
15:    end if
16: end procedure
```

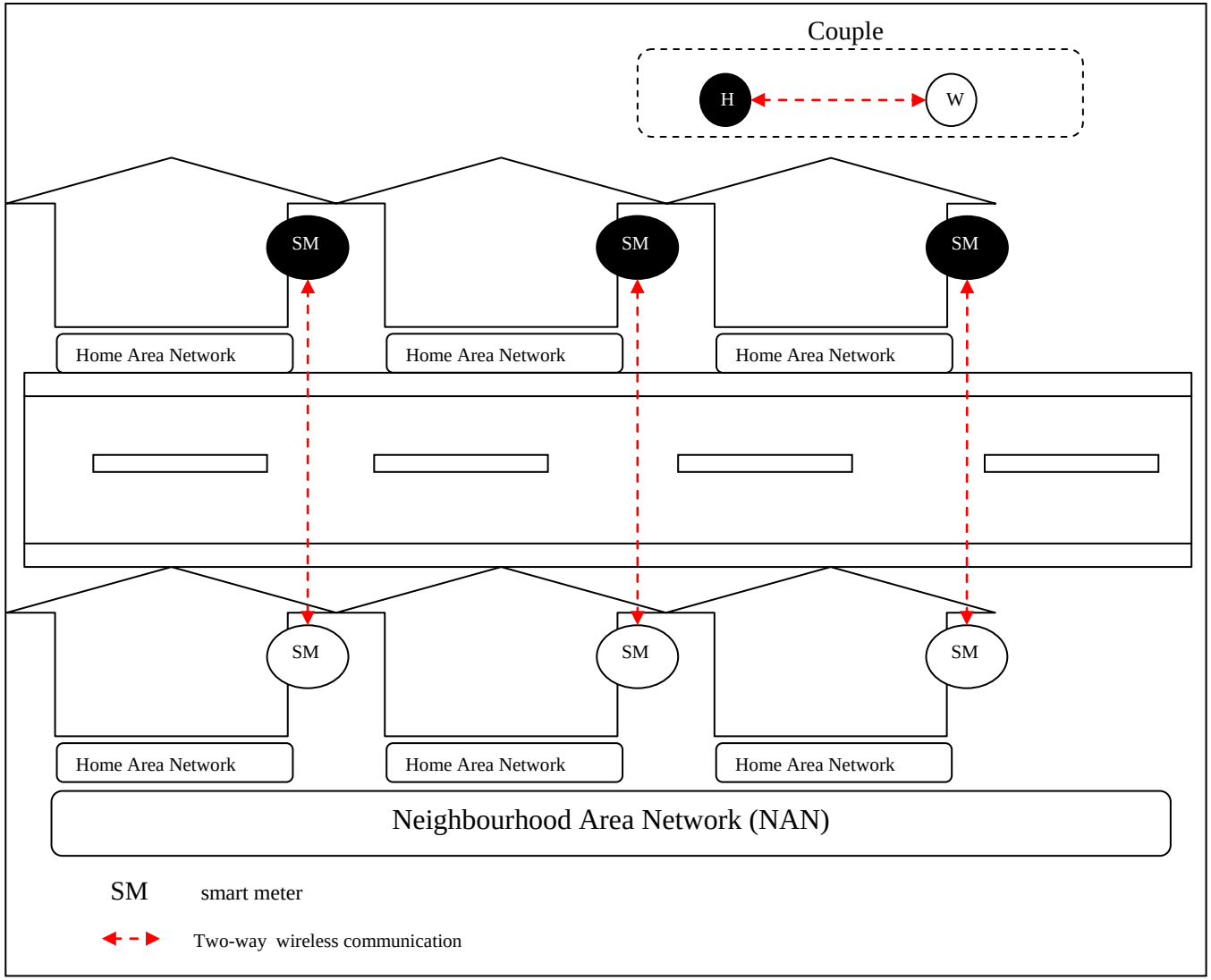

Figure. 8. An example of building smart meter couples in NAN

3.3.1.4 False Alarm Clearance

In some situations, a smart meter may be connected due to maintenance performed by an authorized person, such as the utility company. This may trigger the smart meter compromise attack detection scheme described above, but is a false-positive alarm. Hence, we need to distinguish it from other possible abnormal situations. To avoid a false-positive alarm, the maintenance device will sign the challenge from the smart meter, which will then verify it; next, it will send an alarm clearance message to its partner to clear the false alarm which was caused by maintenance (Exception III). Considering the imbalance in computing power that the smart meter and maintenance equipment may have, we will adopt the Rabin public-key signature scheme to develop a challenge and response identification.

The Rabin signature scheme is ideal for this challenge because it offers the most secure signature as long as the asymmetric cost of computing fits together effectively in the current system situation. Firstly, the Rabin scheme provides a secure signature as public key implementation, which prevents the attacker from generating a private key. As a result, the attacker cannot pass the challenge, guaranteeing the security. Secondly, the asymmetric cost which is fast verification in a smart meter and computationally intensive signing in the utility maintenance device. The challenge and response signature algorithm is based on four steps, as shown in Table. 3. A maintenance device M, that holds the public key (Y_m) and private key (x_m) pair wants to connect with smart meter S_i; Figure. 9. The following steps should be executed:

Step 1: A maintenance device connects to S_i;

Step 2: S_i generates a random R_i and Timestamp TS_i. Then S_i computes the challenge $(TS_i||R_i)$, and sends it to the maintenance device;

Step 3: the maintenance device signs the challenge with x_m by applying the Rabin public key signature. Then, M sends to S_i the signed challenge $RS_x(TS_i||R_i)$;

Step 4: S_i verifies the $RS_x(TS_i||R_i)$ which means that it has passed the challenge; then S_i will send Exception III to S_j to clear the false alarm caused by maintenance.

Table. 3. Challenge to clear the alarm

S_i		M_i
generates R_i, TS_i		
sends $(TS_i\|\|R_i)$	----------►	$(TS_i\|\|R_i)$
verifies the $RS_x(TS_i\|\|R_i)$	◄----------	$RS_x(TS_i\|\|R_i)$

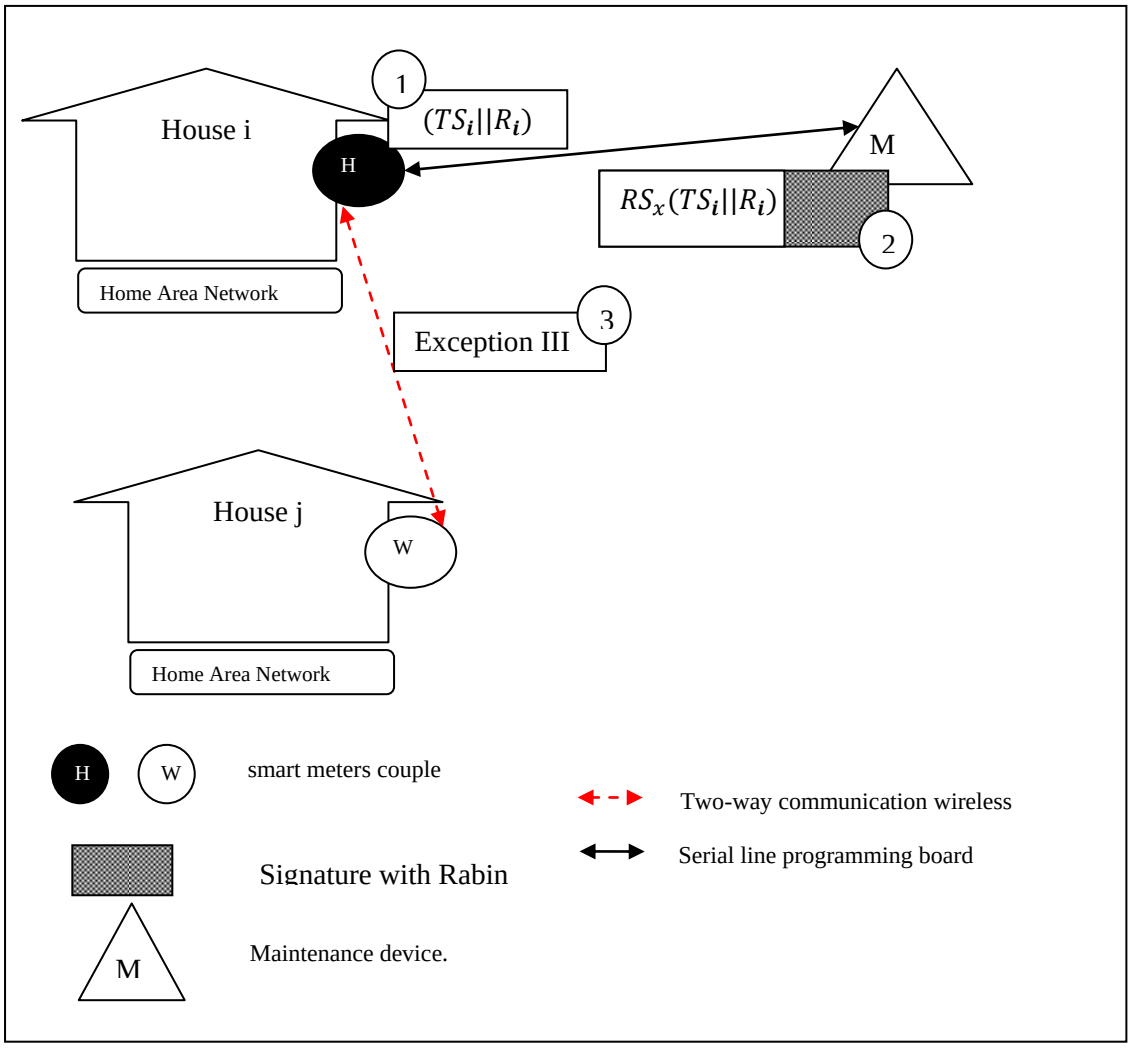

Figure. 9. Clear an alarm scheme

3.3.2 Secure Usage Reporting Protocol

The secure usage reporting protocol has three phases:

1. Token initialization.
2. Appending usage to Token.
3. Smart meter privacy protection.

The main advantage of this protocol is that it prevents an adversary from eavesdropping the messages sent between the smart meter and utility collector, by using an encryption Token-Ring. It also allows the smart meter to transfer the usage data securely. Considering the imbalance in computing power that the smart meter and equipment for utility collectors have, we will adopt the Rabin public key cryptosystem to develop secure usage reporting protocol [14]. It is important to point out that this protocol differs from the other approaches in that designs with particular aspects to ensure the security and the privacy of consumers.

The Rabin cryptosystem is ideal for this protocol because it offers the most secure communication as long as the asymmetric cost fits together effectively in the current system situation. Firstly, it secures communications since it is the public key implementation that protects the attacker from eavesdropping. Secondly asymmetric cost that is encryption requires low-power, and the decryption is similar to the RSA; therefore, a great number of smart meters will encrypt the usage data at low-cost and then send it; only a few powerful utility collector devices will decrypt at a high-cost. We will illustrate the protocol in detail in the following.

3.3.2.1 Token Initialization

The utility providers generate the public and private keys for each utility collector based on the Rabin public key encryption. Next, the utility invokes the Utility Collector (UC) $UC = \{UC_0, UC_1, UC_2, \ldots., UC_n\}$ by applying the Algorithm 4. Finally, the utility collector broadcasts the public key Y_i to all smart meters in the community. In fact, the

utility provider is responsible to deploy and install all utility collectors in the community, so it may invoke offline, prior to installation. As a result, each utility collector has a pair of keys (public and private), and it broadcasts the public key for each smart meter in the community.

The utility collector encrypts the token with the private key and sends it to the smart meters at the Ring. In fact, the utility provider controls and manages the NHN, so that the utility collector will be aware of the NHN graph of the smart meter. Therefore, the network routing in the NHN will be static, and the utility collector can easily build the Token-Ring path. As a result, smart meters do not need to establish the Token-Ring or construct the routing ring; they only need to replay the Token from the utility collector. Without loss of generality, the utility collector encrypts the Token, then sends it to smart meters which are located in the community ring. Each smart meter transfers the data to the Token, and then resends the Token to the next smart meter, until the Token reaches the utility collector, as shown in Figure. 10.

3.3.2.2 Appending Usage to Token

With the purpose of improving the privacy in AMI, all smart meters in the same NAN will report the consumption of energy to the encrypted Token, in order to detect potential eavesdropping. They can achieve this by appending their encrypted data once the Token passes through, so that each smart meter will encrypt the usage with the utility collector's public key. As a result, the utility collector will decrypt the Token and obtain the usage for each smart meter; see Figure. 11.

Algorithm 4 Utility Collector Invoke Keys

Procedure UTILITYCOLLECTORINVOKE

Input: un-invoke Utility collector $UC = \{UC_0, UC_1, UC_2, \ldots, UC_n\}$

Output: invoked $UC = \{UC_0, UC_1, UC_2, \ldots, UC_n\}$

for $i = 0\ to\ n$ do

randomly generate two large prime number a private key $x_i(p, q)$

compute the corresponding public key $Y_i = p \cdot q$

preload utility collector UC_i with key pair (x_i, Y_i)

end for

return invoked $UC = \{UC_0, UC_1, UC_2, \ldots, UC_n\}$

end procedure

In order to append the usage to the Token, the candidate meters will execute the following steps when the Token is received. Assuming there are n smart meters, and the candidate meter is S_i:

Step 1: S_i reports the current Usage U_i with the TimestampTS_i.

Step 2: Next generates a random number R_i

Step 3: S_i obtains Utility Collector (UC)'s authentic public key Y_{uc}

Step 4: S_i encrypts the Data D_i $(ID_i||U_i||TS_i||R_i)$ with Y_{uc}, S_i computes $RE_Y(D_i) = D_i^2 \bmod Y_{uc}$.

Step 5: S_i append the $RE_Y(D_i)$ to the Token T.

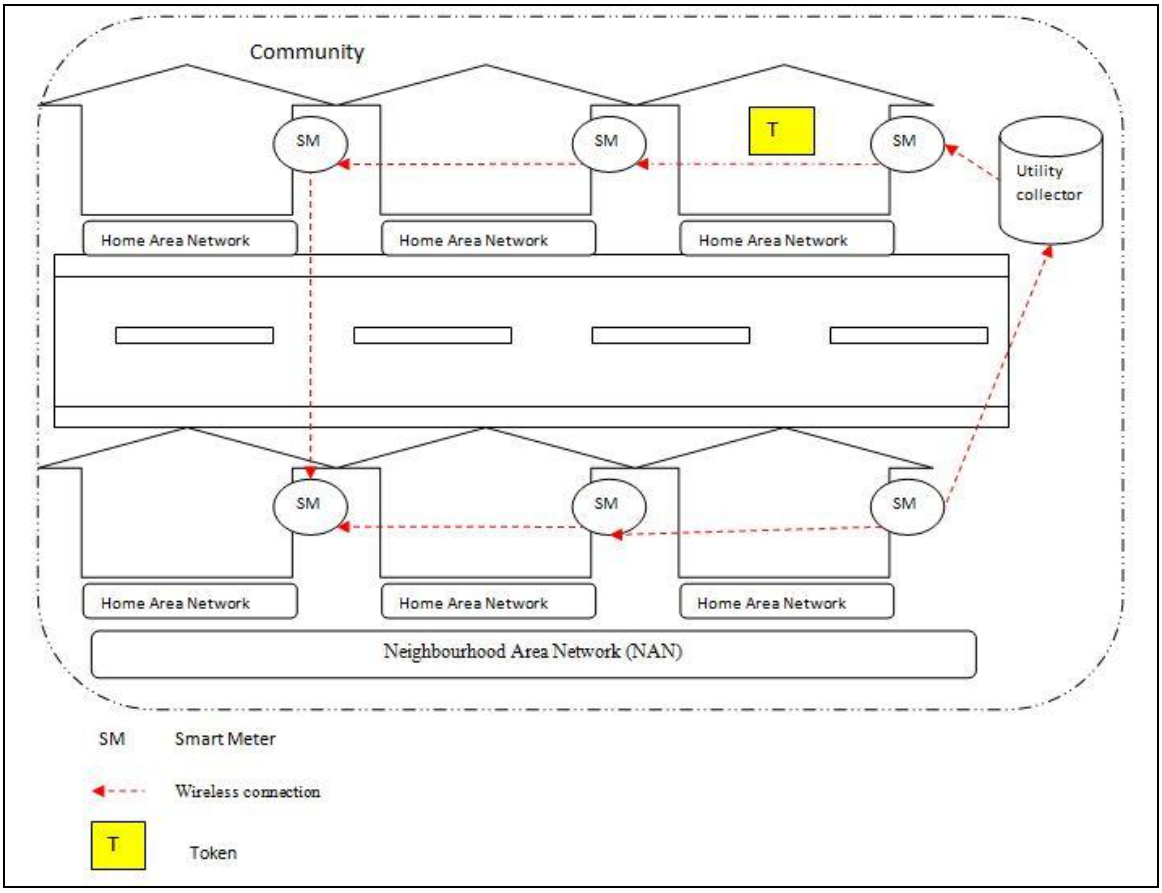

Figure. 10. Token-ring in NAN

After S_i appends the $RE_Y(D_i)$ to the T, S_i resends the Token to the next smart meter. The utility collector is responsible for monitoring the Token in order to collect the usage from the community, including routing the Token-ring and establishing the Token. Due to collecting the usage, the utility collector will send and receive the Token during the travel time between them e.g. five minutes, daily, weekly, monthly. As a result, when the smart meter does not receive the Token, it will not send the usage or establish the Token that will keep the usage hidden from an eavesdropping adversary.

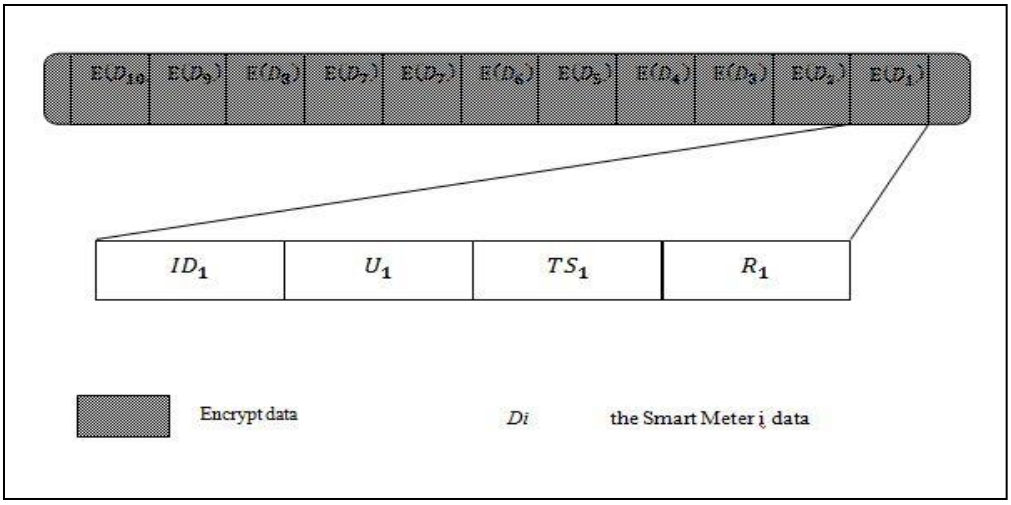

Figure. 11. Token format

3.3.2.3 Smart Meter Privacy Protecting

There are three elements in the secure usage reporting protocol that ensure privacy. Firstly the Token is encrypted by the utility collector's public key, so that only the utility collector is able to decrypt it. Moreover, an adversary cannot establish a Token, and then send it to the smart meters since the smart meters report only to an authenticated Token which is sent by the utility collector. Secondly, when the S_i encrypts the D_i $(ID_i||U_i||TS_i||R_i)$ with RE_Y, this prevents an adversary from recognizing the consumption of usage. In fact, adding the R_i to the D_i will avoid an adversary from launching a dictionary attack, because the utility collector's public key could be known by the adversary, and the amount of energy consumption to report every time is also limited. As a result, an adversary may succeed in launching a dictionary attack; however, encryption with R_i will prevent this. Finally, all smart meters must wait and report for the encrypted Token, even if there is no energy consumption. The main benefit of this is that it blocks

the data from the view of an adversary who eavesdrops on the community; however, all feasible attacks and the detection will be discussed in detail in the Security Analysis section. In short, the proposed secure usage reporting protocol will protect the privacy of consumers by an encrypted Token and achieve cost-efficiency by the Rabin cryptosystem.

Chapter 4

Security and Privacy Analysis

In this chapter we will analyze the types of attacks an adversary could launch, and evaluate the security of the proposed scheme, particularly on consumer privacy. For this analysis, we assume an adversary has a powerful device with full access to sniffer communication data. In fact, there are no limitations regarding the computational or memory sources that are available to an adversary. Therefore, we will discuss the security involved in available attacks, and then we will explain how the proposed scheme will offer resistance.

4.1 Dictionary Attack

This attack will be different from known dictionary attack while an adversary can guess the potential plan text. As a result, an adversary encrypts known data, and then tests out with cipher text that is captured. Once the combination matches, this means the attack will succeed. In our case, there is a high possibility for this to occur in view of the fact that an adversary has a powerful device and there is several possibilities of data to encrypt. Specifically, once the smart meter encrypts the usage data (limited range) with the utility's public key, it then sends it to the utility collector. However, the proposed secure usage reporting protocol resists the attack by adding a random number.

In reality, it may happen that an adversary knows the possible range of data which is reporting every time, since the smart meter reports to the utility collector every short

period, and typical consumers in residences use small amount of energy every short period, which is usually a few hundred kilowatt (kw). In fact, an adversary might very well estimate a list of usages consumption, which should have the actual consumption. In order to make a good guess, an adversary will need to find the threshold consumption of energy that is publicly known, or use a different technique to guess the range of consumption during a short period. For example, the Ontario Energy Board sets a threshold of 600 kilowatt hours per month during the summer and 1,000 kilowatt hours per month during the winter [32]. As a result, depending on threshold consumption, an adversary can simply pre-compute all possible energy consumption during the short period, e.g. from 0 kw to 600 kw which is a limited range. Moreover, an adversary can simply know the public key of the utility collector, and the time of collecting packages, since the schedule of usage reporting could be easily predicted when an adversary eavesdrops in the NHN. Thus, a dictionary attack is possible, if we do not add a random number in the encryption data.

To create the attack without considering a random number, an adversary can compare the pattern of encrypted data with a known array of usage consumption, as shown in Figure. 12. The following steps would be executed in order to launch the dictionary attack:

Step 1: an adversary pre-computes all possible usage consumption $U_{\mathbf{0-n}}$ {0,1,2, … , n}.

Step 2: an adversary captures the Utility collector public key Y_{uc} .

Step 3: an adversary captures the time of sending the Token.

Step 4: an adversary captures the Encryption Data E$(D_i)\{ID_i||U_i||TS_i\}$; then stored at table.

Step5: an adversary encrypts each possible usage withY_{uc}, and the TS; which are then stored at an indexed table.

Step 6: an adversary runs a look-up method to find matched fields; an attack is successful when the look-up returns the index value.

Accordingly, when the look-up method returns the field value, the adversary can simply note the consumption usage by checking the value of the field before the encryption.

However, in the proposed scheme the smart meter S_i encrypts the consumption usage with a utility's public key in order to make the dictionary attack insignificant; we appended a random number R_i with the data. Thus the Encryption Data $E(D_i)$ will be $(ID_i||U_i||TS_i||R_i)$ which reports to the utility every time. Consequently, the R_i will make the $E(D_i)$ very complex to guess, so the dictionary attack will not be significant enough to succeed.

In summary, even if the adversary knows the possible range of consumption, s/he cannot launch a dictionary attack. The proposed scheme resists the dictionary attack by adding a random number into the encryption data.

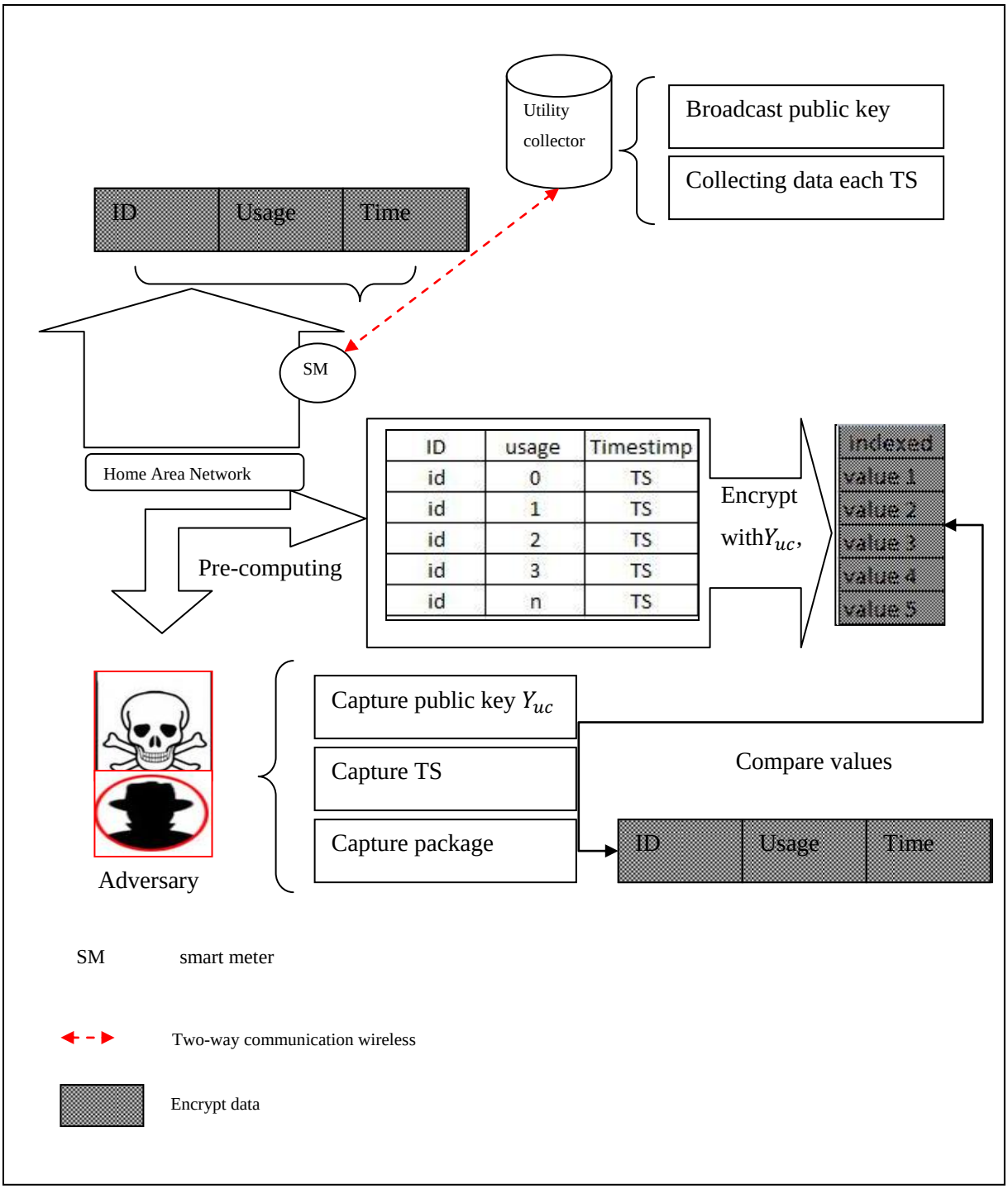

Figure. 12. Launching the dictionary attack

4.2 Message Replay Attack

This attack attempts to bypass the authentication method by resending the authenticated message. An adversary, who eavesdrops on the network, captures the authentication messages, e.g. a challenge and response between two parties. Then the message of the authorized party is replayed to the other end, e.g. the response of the authorized party that will pass the challenge. In fact, an adversary does not need to know the encryption key or the content of the message but need only replay the message of authentication. However, in our scheme the replay- message attack could occur in two parts of the detection attack scheme, either on a replay the beacon message between the couples or on the clearance alarm message between the smart meters and maintenance device.

Firstly, the couple based detection scheme can resist the replay beacon attack. In fact, without the proposal scheme an adversary might attempt to compromise the **H**-Meter via a physical attack and keep the other **W**-Meter unaware about the attack; as shown in Figure. 13. The following steps should apply in order to succeed:

Step1: an adversary captures the beacon message between the couple (H-W).

Step2: an adversary connects to the **H**-Meter via a JTAG in order to compromise the smart meter.

Step3: an adversary resends the beacon message within a normal situation in order to avoid the **W**-Meter sending an alarm to the utility collector.

When an adversary completes these steps, this means the adversary can simply compromise the smart meter, and it is a matter of time before the second one is compromised. In fact, the detection attack scheme will resist this attack because just the couple of smart meters S_i, S_j can compute the shared ab.G; also, the one-way hash function h(ab.G) is difficult to break. Then if an adversary replays the beacon, the other couple can detect the attack. As a result, an adversary cannot launch the replay-message attack.

Secondly, with a replay the clearance alarm attack an adversary replays, the signed challenge message in order to appear as a maintenance device when s/he connects to the smart meter. Without the TS_i which included in the clearance alarm, an adversary might attempt to appear as a maintenance device; therefore, an adversary can connect to the JTAG without sending an alarm; see Figure. 14. The following steps should be executed:

Step1: an adversary captures the signed challenge RS_x message between the smart meter and a maintenance device.

Step 2: an adversary connects with smart meter via a JTAG in order to compromise the smart meter S_i.

Step 3: an adversary receives the challenge that is generated by S_i.

Step 4: an adversary resends the signed challenge RS_x message; to deceive the smart meter S_i for sending the clearance alarm message to S_j.

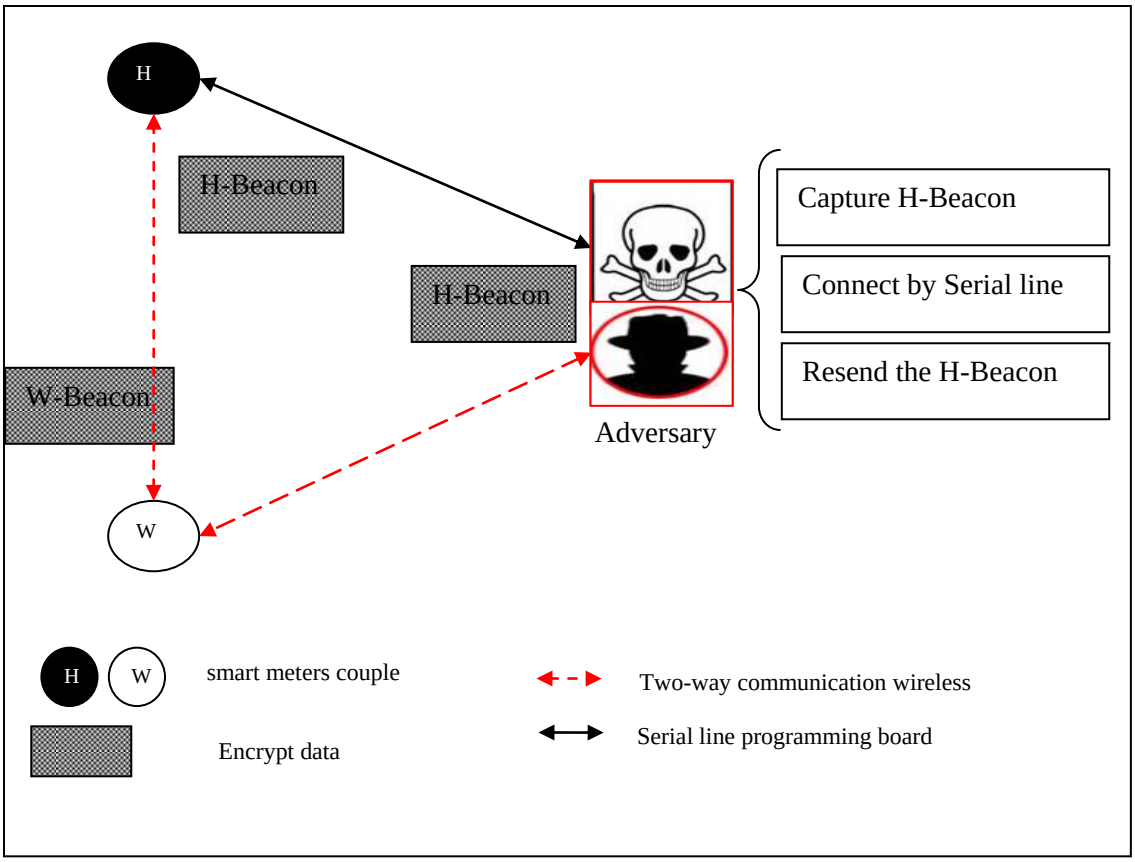

Figure. 13. Replay the beacon Attack

Clearly, it cannot work in the the false alarm clearance scheme because of the Timestamp TS_i added in Step 2 of Table 3. If the same Timestamp TS_i included in the signed challenge $RS_x(TS_i||R_i)$ is not reasonable, the smart meter will simply reject the signature. As a result, an adversary cannot launch a replay-message attack as this message is valid only for a specific moment of time.

In summary, the difficulty of computing the shared ab.G, and the one-way hash function h(ab.G) has been used in the proposed scheme in order to prevent the replay beacon message in first situation. As well, the Timestamp TS_i included in signed challenge

prevents a reply false alarm clearance message. Therefore, the scheme can resist the replay attack in both situations.

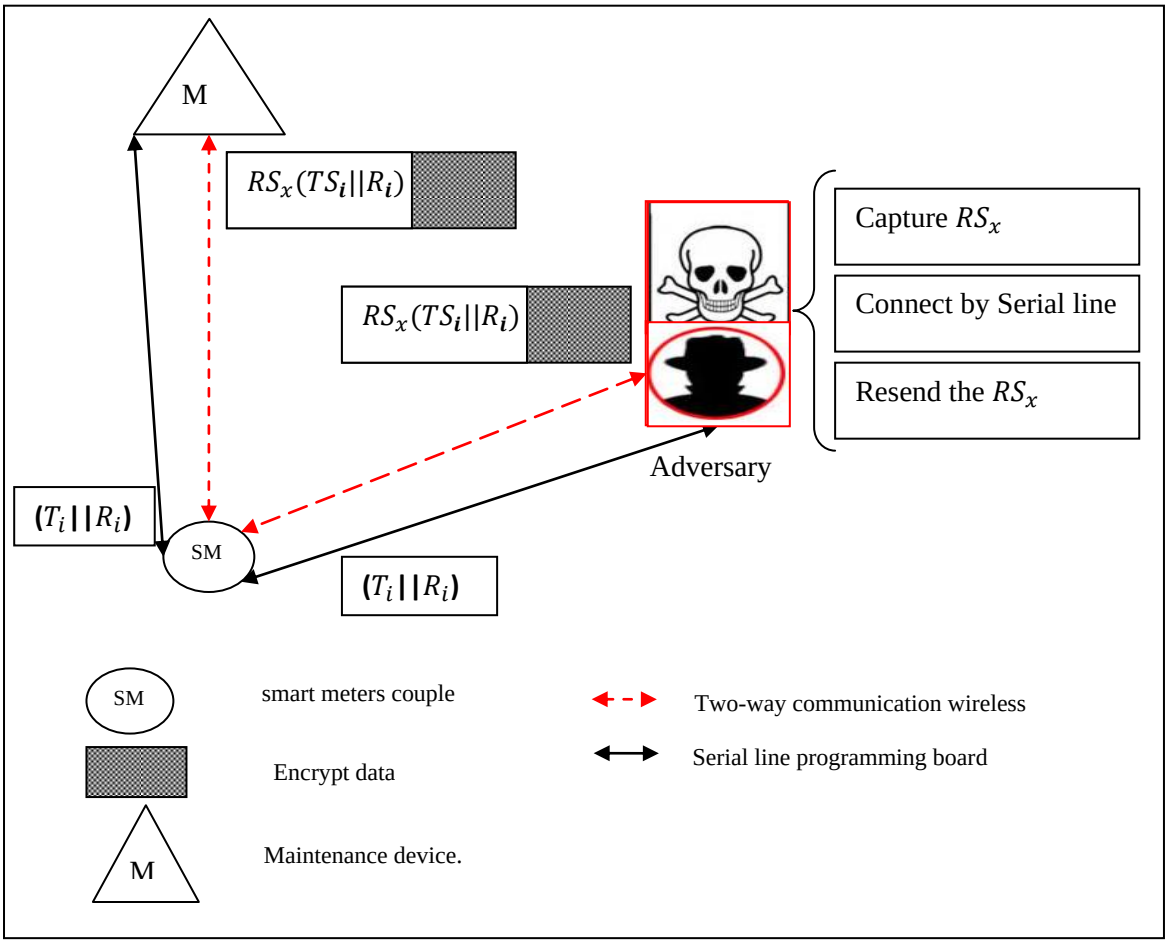

Figure. 14. Replay the clearance alarm attack

4.3 Traffic Analysis

This attack aims to assemble all communication activities of a specific node in order to produce the patterns of activities. An attacker is incapable of knowing the message contents by decrypting; instead, the attacker will observe the time the smart meter sent

data to the utility. The proposed scheme can resist this attack; in fact, all smart meters must report to the encrypted Token, even if there is no energy consumption.

Without reporting to the utility each time, the traffic analysis attacks against usage reporting protocol, will violate the consumers' privacy. In fact, the attacker can recognize what time the householders are in-home or out-of-home by observing the messages which are sent from the smart meter even if encrypted, see Figure. 15. The attacker can carry out the following steps to launch the attack:

Step1: the attacker chooses a smart meter to observe, e.g. S_i.

Step 2: the attacker creates a timetable with event reporting.

Step3: when S_i sends a message, the attacker reports with the time event.

Step 4: after a period of time (e.g. week/month) the attacker can determine the pattern of activities of S_i, which is evidence of the householder being absent from the residence.

However, the proposal scheme can resist this attack by secure usage reporting protocol; specifically, every single smart meter will report to the encrypted Token even if there is no energy consumption at the particular moment once the Token is received. For instance, the Token will send from the utility collector every travel time, and smart meters will report the usage consumption e.g. 100 kw or the value '0'. As a result, an attacker is not able to distinguish the pattern activities of a specific smart meter, since all smart meters report to Token every time; thus, the analysis of the attack traffic will be resisted.

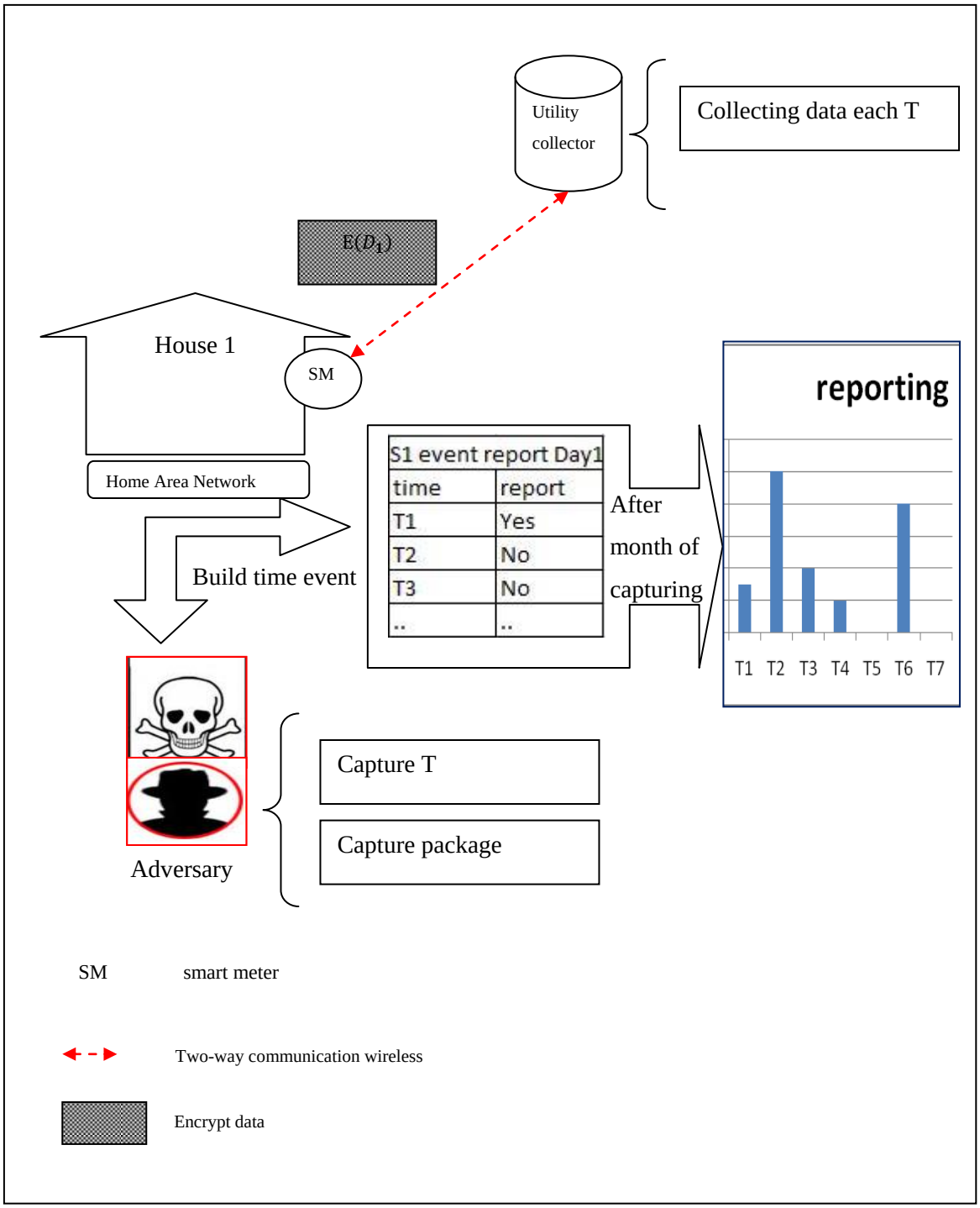

Figure. 15. Traffic analysis attack

4.4 Physical Attack

This attack aims to compromise the smart meter by using a programming board and a serial cable. However, the proposed detection scheme resists this attack by building a couple that is monitoring each other.

In fact, this attack is easy to launch since the smart meter is located outside the home, and it has a JTAG; moreover, most smart meters use ZigBee with a symmetric key ASE-128. As a result, the attacker can connect to the smart meter, and then obtain all of the keys within one minute when the smart meter is being compromised; the attacker has full control of a smart meter, thus affecting the consumers' privacy. The attacker can simply follow the steps of a KillerBee Toolkit [10].

However, the proposed scheme resists a physical attack through the smart meters compromise attack detection scheme. In fact, all smart meters in the NHN are building a couple that is monitoring each other, e.g.(S_i S_j); see Figure. 16. Therefore, when an adversary A connects to a smart meter S_i with the purpose of compromise, the other couple S_j will be aware of this and send an alarm to the utility collector. For example, when an adversary A connects to a smart meter S_i, the S_i will send the Exception II to S_j, which means the smart meter is connected with an adversary. Moreover, the adversary cannot respond with a correct signature for challenge; hence, S_i will not send a clearance alarm message to S_j (Exception III). Furthermore, when an adversary shuts down a smart meter S_i in order to compromise, the other couple S_j will not receive the Beacon_i. As a

result the S_j will consider S_i is under attack and send the Exception I to utility collector. In summary, with all which is possible to compromise the smart meter, the couple based detection scheme is able to detect the physical attack.

4.5 Impersonation Attack

This attack aims to impersonate the authorized party in the network in order to deceive the victim. An adversary places a fake smart meter in the network, which will then communicate with the victim smart meter to potentially affect privacy by analyzing the packages. However, in our scheme the Impersonation attack can be directed either to the building couple or to the reporting protocol, which is resisted in both situations.

Firstly, an adversary cannot build a couple in the NAN even if s/he has inserted a fake Smart meter. However, without the scheme considerations an adversary can impersonate the smart meter, and the fake smart meter will keep the other couple unaware about the attack. For example, an adversary attempts to impersonate the **H**-Meter and keep the other **W**-Meter unaware about the actual condition of the **H**-Meter; after that, an adversary compromises the **H**-Meter via a physical attack; see Figure. 17. Attacker *A* can carry out the following steps to launch the attack:

Step1: the attacker gets hold of the shared key (*ab.G)* between the **H**-Meter and the **W**-Meter.

Step2: the attacker shuts down the **H**-Meter in order to compromise.

Step3: the attacker sends the normal situation beacon to the **W**-Meter.

When an adversary completes these steps successfully, s/he can simply compromise the **H**-Meter, and it is a matter of time before the second one is compromised.

However, in order for an attack to occur, the adversary requires to either obtain the shared key directly from one of the couples or compute the shared key (*ab.G)* between the couple. In fact, the scheme resists both possibilities. It has been shown in Figure. 16 how the scheme prevents the key being obtained directly by detecting a physical attack. Moreover, the difficulty of the elliptic curve computational Diffie-Hellman problem resists the attackers' computation of the shared key. As a result, the shared key (*ab.G)* can only compute by the couple S_i, S_j, which uses the Naccache-Stern signature [31] during building. Hence, an adversary cannot build a couple with any smart meter in the NHN.

Secondly, the proposal for secure usage reporting protocol, prevents an impersonation of the utility collector. It may occur that an adversary inserts a fake utility collector into the NHN. However, the smart meters report only to approve the Token that is encrypted by the utility collector's private key. Even if the adversary sends a fake Token to collect the usage from smart meters in the community, it still cannot forge a utility collector's private key. In order for an attack to occur, the adversary needs to compute the private key of the utility collector that is $x_i(p, q)$, then encrypt the Token. In fact, the difficulty of factorization of the Rabin public key prevents an adversary from achieving a forged key. As a result, the private key can only be computed by the utility collector.

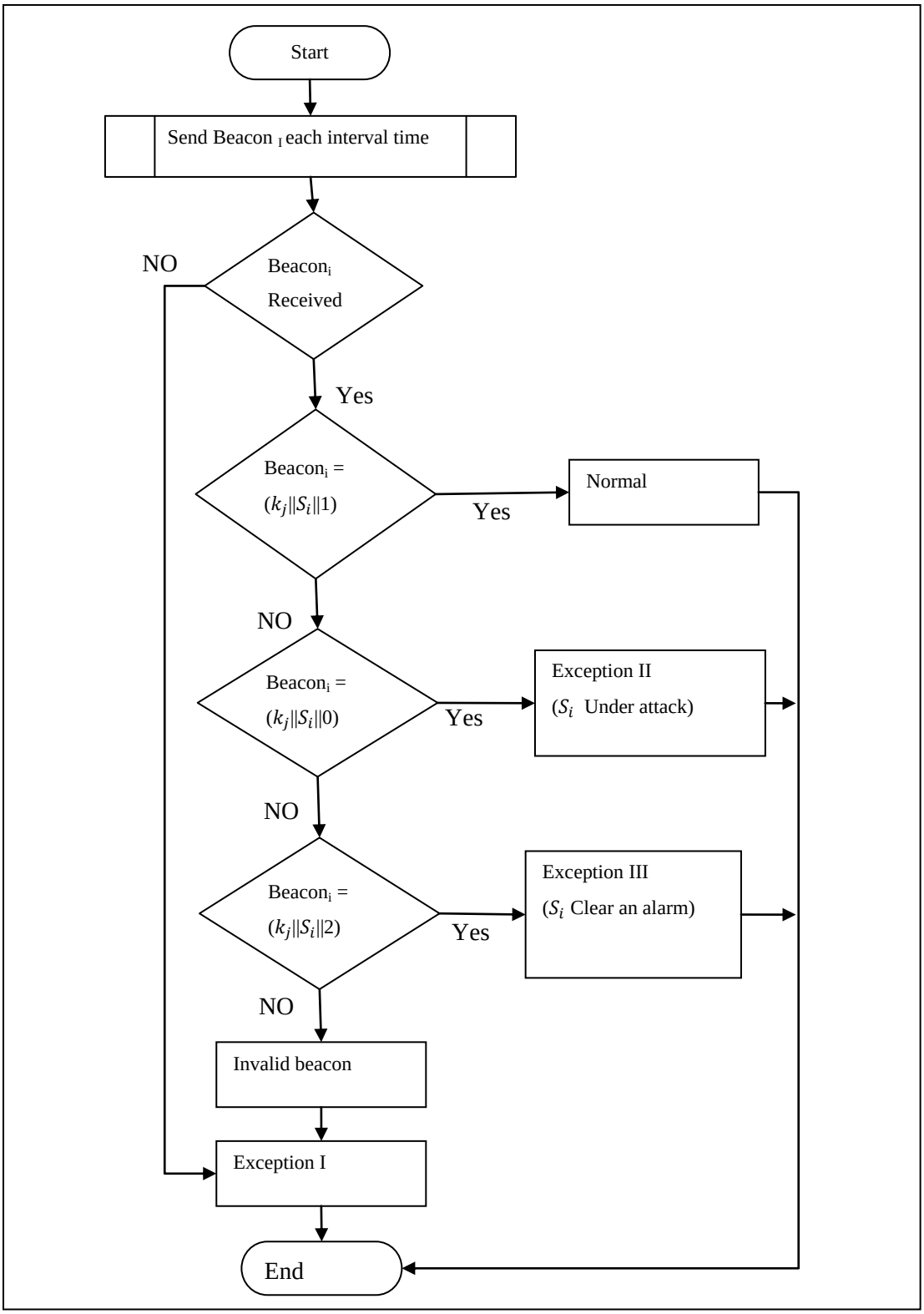

Figure. 16. Couple S_j monitoring flow diagram

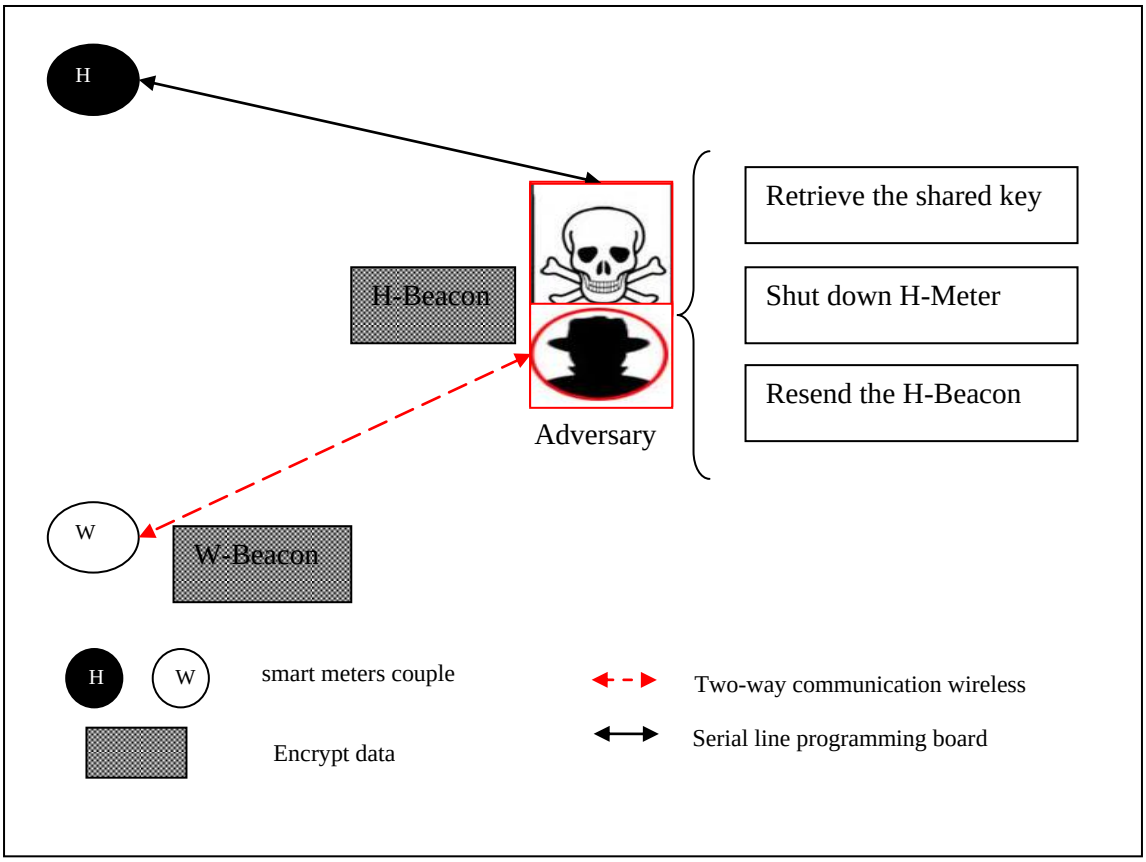

Figure. 17. Impersonate the H-Meter

In summary, the difficulty of computing the shared key (*ab.G)* in the building a couple phase in the proposed scheme prevents the impersonation attack in first situation; the difficulty of the factorization of the Rabin public key prevents an adversary from achieving a similar result in the second situation. Thus, the Impersonation attack can be resisted by the proposed scheme.

4.6 Eavesdropping Attack

Eavesdropping is known as a passive attack; an adversary can simply capture the communications packages in the wireless network radiation range between the smart meters and utility collectors. Subsequently, an adversary attempts to analyze the packages in order to obtain the in content. However, this attack is highly possible to occur since all smart meters in the NHN communicate with low-rate wireless. Consequently, any adversary who is in the range of the wireless communication can capture the packages quite simply. Therefore, once an adversary can obtain the content of packages the consumer privacy is violated as shown in Figure. 18.

In fact, the proposed scheme can resist this violation by encrypting all wireless communication with a strong encryption scheme, which is Rabin public key. The communication between the smart meters and the utility collector are encrypted by the utility collector public key Y_{uc}, such that an adversary cannot know the content without knowledge of the utility collectors' private key. An adversary can capture the communication packages between the utility collector and a smart meter, but s/he cannot decrypt them. In fact, computing the private key relies on the complexity of factorization, which is considered to be difficult. As a result, the adversary needs to have knowledge or be able to compute the private key of the utility collector with the purpose of analyzing the packages. In summary, an adversary can simply capture the encryption packages; on the other hand, they are too difficult to decrypt, which results in privacy protection.

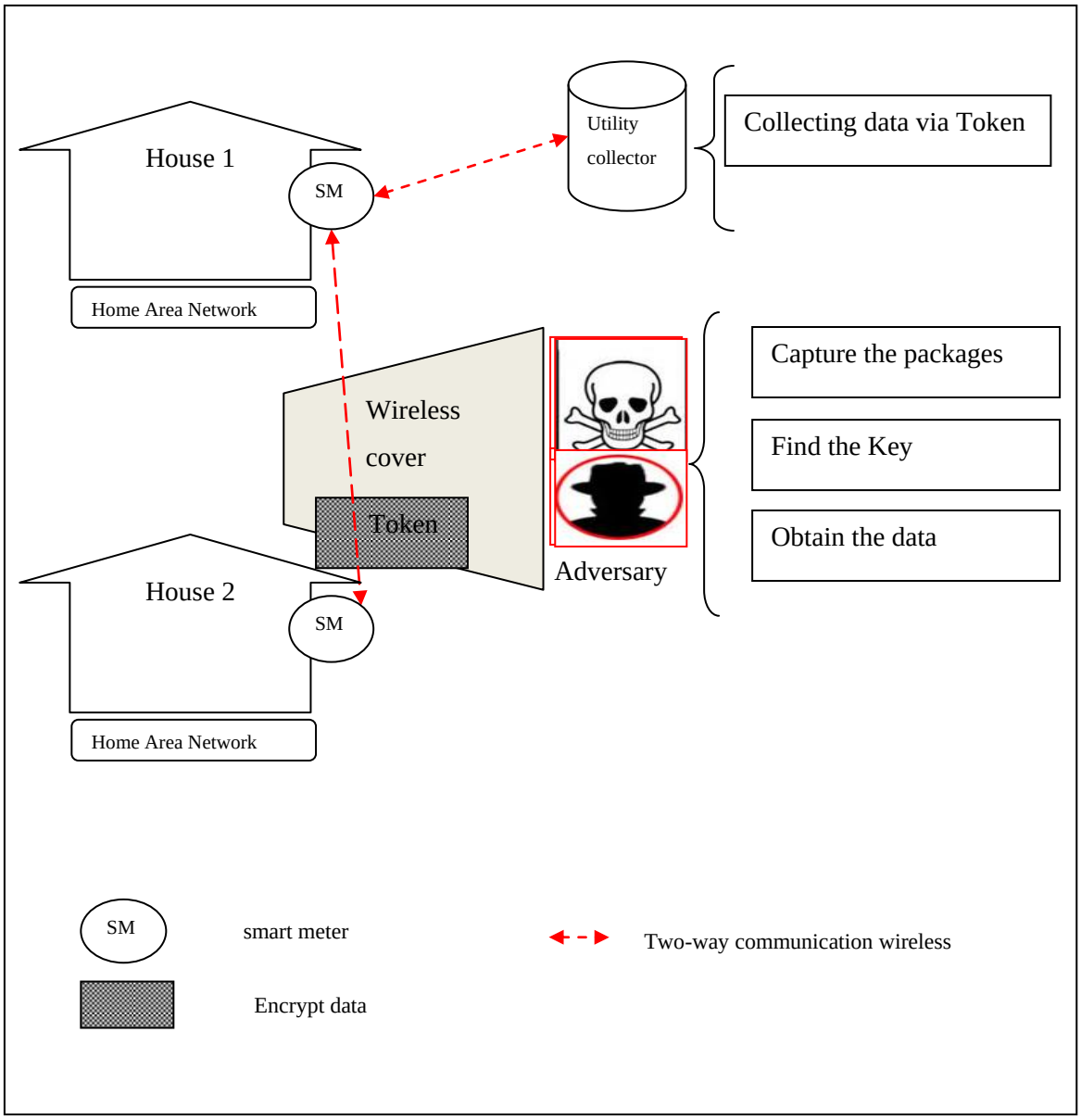

Figure. 18. Eavesdropping attack

In summary, in this section we evaluate the proposed scheme by discussing a possible attack against a consumer's privacy. It has been shown that the proposed scheme can resist all potential attacks. Firstly, the Rabin public key encryption scheme ensures the confidentiality of the packages. Secondly, the couple built detection scheme prevents the smart meter gaining compromise. Table. 4 provides a summary of all potential attacks.

Table. 4. AMI targeted attacks

Attack Name	Attack details	Take Place	Attack Resist
Dictionary Attack	Compares a list of pre-computing encrypted usage with a capture package to identify the consumption	Encrypts the usage data	Appends a random number R_i with the data
Message Replay Attack	Passes the authentication method	Replaying the beacon between couples	The one-way hash function h(ab.G) is hard to break
		Replaying the clearance alarm between the maintenance device and smart meter	Signed the challenge with Timestamp TS_i $RS_x(TS_i \| \| R_i)$
Traffic Analysis	Assembles all communication activities of a specific smart meter	Secure Usage reporting protocol	Report the usage consumption or '0' every trivial time to Token
Physical Attack	Compromises the smart meter by using a programming board and a serial cable	In the smart meter JTAG interface	Building a couple in NHN
Impersonation Attack	Impersonates the authorized party in the network in order to deceive the victim party	Impersonates the smart meter to build the couple	The difficulty of elliptic curve computational Diffie-Hellman problem to compute the shared key
		Impersonate the utility collector to collect the usage	The difficulty of factorization of the Rabin public key

Attack Name	Attack details	Take Place	Attack Resist
Eavesdropping Attack	Capture the communications packages in order to obtain the content of the packages	The NHN communicate with low-rate wireless	The difficulty of factorization of the Rabin public key

Chapter 5

Conclusions and Future Work

5.1 Conclusions

In summary, a great number of countries around the world have been moving towards energy efficient, environmentally and customer-friendly Smart Grid which promises to avoid blackouts. The AMI subsystem addresses these features through recognition of the dynamic expenditure of energy. The AMI controls communication between consumers and utilities by two-way communications, in order to collect, store, and analyze energy usage data. Typically, the AMI system consists of smart meters in a consumer's home, a metering communication infrastructure between the consumer's home and utilities, and the MDM. The key element of AMI is the smart meter which is an electrical device installed outside a house that collects the consumer energy usages, and then sends the data to the utility company for billing. The smart meter provides more details about consumers' usage via TOU that measures hour-by-hour usage of each electrical device at home; different from the current system which collects the total of the monthly energy consumption. Briefly, a Smart Grid being developed today will improve the reliability of the current energy system by recognizing the dynamic expenditure of power.

The Smart Grid offers reliability and efficiency for the energy system; on the other hand, it presents a new challenge in the consumer's privacy. Specifically, the smart meter assembles the usage data of each electrical device at home, then instantaneously sends the data with the total usage to the utility. When the smart meter records the electrical usage,

each electrical usage presents the behaviour of consumers in the home. For instance, the smart meter records the time and the consumption usage of every electrical device in the residence such as watching television, using a microwave, oven, and so on. Thus, the risks that are associated with disclosing the data in the smart meter are too high as it could turn out to be attractive for attacks.

In fact, an adversary can distinguish the consumer activity and behaviour by compromising a smart meter or recovering a record of usage during the communication between the smart meter and utility collector. Therefore, any communication channel between customers and the utility should have a standard of confidentiality which protects consumer privacy. On the other hand, the smart meter is located in insecure areas, and it does not provide a secure encrypted algorithm. For example, the open-source tool KillerBee can break the encryption keys in the smart meter. The smart meters are actually low-end, therefore applying high encryption techniques for the security requires additional hardware. Nevertheless, the cost constraints create a challenge to secure the smart meter without significant additional cost. Moreover, several standards have been published with the aim of securing the AMI, although it still has vulnerabilities as a low-cost device. Therefore, there is a need to improve the security defenses in order to protect the privacy, which the current study achieves. Thus, the objectives of this research are to protect the privacy of the consumer as well as achieve cost efficiency.

This research focuses on the privacy of the communication channel between smart meters and the utility collector in the phase of collecting usage from smart meters via a wireless

mode. In addition, we consider protection privacy either on stored memory in the smart meter or on the communication channel. Furthermore, this research improves the security with the intention of protecting privacy. Firstly, with the intention of improving security, we propose a detection scheme that protects the smart meter from a compromise attack. Secondly, with the intention of improving privacy, we propose a new protocol that protects privacy by applying the Rabin public key scheme.

As shown in the security analysis chapter, the scheme can protect the consumer's privacy either on stored memory in the smart meter or on the communication channel. Specifically, an adversary, who is eavesdropping with a powerful device in NHN, cannot recover the packages, trace the packages, and compromise the smart meter.

5.2 Summary

We propose a new scheme to secure the AMI that has two components: the smart meter compromise attack detection and secure usage reporting protocol. In fact, we consider the imbalance of the computing power of the smart meters and utility equipment, so we shift most of computing to utility equipment instead of the smart meter. Consequently, we apply an imbalanced encryption technique between the utility collector and smart meter that is the Rabin public key. Thus, we successfully achieve both security and cost-efficiency.

Firstly, the smart meters compromise attack detection scheme resists an adversary to compromise the smart meter by an easily launched physical attack. We achieve this by

building couples, in order that every single smart meter in the NAN will monitor another smart meter with the purpose of detecting a potential compromise attack. As a result, when an adversary attempts to compromise one of the couples, the other couple will become aware and send an alarm to the utility collector. There are three situations: a normal situation, a detection situation, and a maintenance situation that are sent between the couples at each interval time. All of these situations are sent by Beacon message that is encrypted with a hash function. Moreover, we apply the Rabin public key signature scheme to a false alarm clearance once the utility provider repairs a smart meter which offers the most secure signature as long as the asymmetric cost of computing.

Secondly, the secure usage reporting protocol resists an adversary from identifying the message that is sent between the smart meter and utility collector, which is protecting consumer privacy. We consider the imbalance in the computing power that the smart meter and equipment for utility collectors have, so we adopt the Rabin public key cryptosystem to develop reporting protocol usage. As a result, the utility collector sends an encryption Token every time with the aim of collecting the usages. The smart meter then transfers the usage data to the Token securely, which encrypts the data with the utility public key. Briefly, the protocol protects the privacy of consumers by an encrypted Token and achieves cost-efficiency by the Rabin cryptosystem.

In summary, it has been shown that the proposed scheme can resist all potential attacks against the consumer's privacy, which are the dictionary attack, the replay attack, the traffic analysis attack, the physical attack, the impersonation attack, and the

eavesdropping attack. Therefore, the schema protects the privacy of the AMI either in the confidentiality of the packages by the Rabin public key encryption scheme or in the memory of the smart meter by the couple built in detection scheme.

5.3 Future Research

Consumer privacy concerns are an important focus of Smart Grid. In this work, we mainly focused on the privacy of the communication channel between smart meters and the Data Concentrators in the phase of collecting data from smart meters. However, consumer privacy can be easily breached in many areas of Smart Grid. As for future research plans, we will be investigating techniques to protect the privacy once the usage is stored at the Meter Data Management system. We will involve addressing the privacy in the data base of the utility provider, in order that no individual will be able to link the usage data with consumer identity, even including the utility provider employees. As a result, the AMI privacy concerns will be well protected.

References

[1] A. Ipakchi and F. Albuyeh, "Grid of the future," *IEEE Power and Energy Magazine*, vol. 7, no. 2, pp. 52–62, Mar/Apr, 2009.

[2] U.S. Department of Energy, *The Smart Grid: An Introduction*, 2008. [E-book]. Available:http://www.oe.energy.gov/DocumentsandMedia/DOE_SG_Book_Single_Pages%281%29.pdf. [last accessed Apr 14, 2011].

[3] Ontario Smart Meter. [Online]. Available: http://www.mei.gov.on.ca/en/energy/conservation/smartmeters/?page=powersmarter_why-smart-meters. [last accessed Apr. 13, 2010].

[4] J. Kim, S. Ahn, Y. Kim, K. Lee, and S. Kim, "Sensor network-based AMI network security," in *Proc. Transmission and Distribution Conference and Exposition*, New Orleans, Louisiana, pp. 658-662, Apr. 2010.

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

[6] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in *Proc. the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building (BuildSys 2010),* Zurich, Switzerland, pp. 61-66, 2010.

[7] E. Quinn, "Smart metering and privacy: existing law and competing policies," A Report for the Colorado Public Utilities Commission, 2009.

[8] E. Quinn, "Privacy and the new energy infrastructure," *Social Science Research Network (SSRN),* February 2009. [Online]. Available: http://ssrn.com/paper=1370731 [last accessed Apr. 13, 2010].

[9] F. Cleveland, "Cyber security issues for advanced metering infrastructure (AMI)," in *Proc. IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, Pittsburgh, Pennsylvania, pp. 1–5, July 2008.

[10] C. Johnny, J. Wright, and V. Liu, *Hacking Exposed Wireless: Wireless Security Secrets & Solutions*, 2nd ed. Osborne: McGraw-Hill, 2010.

[11] Canada, Information Technology Standards, *Government of Ontario IT Standard Advanced Metering Infrastructure*, 2009.

[12] K. Doran, F. Barnes, and P. Pasrich, "Smart grid deployment in colorado: challenges and opportunities," University of Colorado, Boulder, June 2010. [Online]. Available: http://rechargecolorado.com/images/uploads/pdfs/University_of_Colorados_Smart_Grid_White_Paper.pdf. [last accessed Apr. 13, 2010].

[13] Canada, Toronto police service, *Neighbourhood Watch*, 2004. Available: http://www.torontopolice.on.ca/crimeprevention/nwatch.pdf [last accessed Apr. 13, 2010].

[14] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, Florida: CRC Press, October 1996.

[15] T. Khalifa, V. Naik, and A. Nayak, "A Survey of communication protocols for automatic meter reading applications," *IEEE Communications Surveys & Tutorials*, pp.1-15, 2010. Available: http://ieeexplore.ieee.org/stamp/stamp.jsptp=&arnumber=5473879 [last accessed Apr. 14, 2010].

[16] R. Davies, "Hydro one's smart meter initiative paves way for defining the smart grid of the future," in *Proc. IEEE Power and Energy Society General Meeting*, Calgary, Alberta, pp. 1-2, 2009.

[17] W. Boyer and S. McBride, "Study of security attribute of smart grid systems-current cyber security issues," Idaho National Laboratory, Technical Report, Idaho Falls, Idaho, Apr. 2009.

[18] B. Brown, and *et al.*, *AMI System Security Requirements*, AMI-SEC TF, 2008.

[19] B. Brown, and *et al.*, *AMI Security Implementation Guide*, AMI-SEC-ASAP, 2009.

[20] C. Hartung, J. Balasalle, and R. Han, "Node compromise in sensor networks: the need for secure systems," Dept. of Computer Science, Univ. of Colorado, Technical Report CU-CS-990-05, Boulder, Colorado, Jan 2005.

[21] C. Bennett and D. Highfill, "Networking AMI smart meters," in *Proc. IEEE Energy 2030 Conference*, Atlanta, Georgia, pp.1-8, Nov. 2008.

[22] P. Shah, T. Shaikh, K. Ghan, and S. Shilasakar, "Power management using ZigBee wireless sensor network," in *Proc. ICETET '08 First International Conference on Emerging Trends in Engineering and Technology,* Nagpur, India, pp. 242-245, Jul. 2008.

[23] B. Yang, "Study on security of wireless sensor network based on ZigBee standard," in *Proc. International Conference on Computational Intelligence and Security,* Beijing, China, vol. 2, pp. 426-430, Dec. 2009.

[24] M. Blaser, "Industrial-strength security for ZigBee: the case for public-key cryptography," *Embedded Computing Design,* 2005.

[25] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. First IEEE International Conference on Smart Grid Communications*, Gaithersburg, Maryland, pp. 238-243, Oct.2010.

[26] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Proc. First IEEE International Conference on Smart Grid Communications*, Gaithersburg, Maryland, pp. 327-332, Oct. 2010.

[27] G. Kalogridis, C. Efthymiou, S. Denic, T. Lewis, and R. Cepeda, "Privacy for smart meters: towards undetectable appliance load signatures," in *Proc. First IEEE International Conference on Smart Grid Communications*, Gaithersburg, Maryland, pp. 232-237, Oct. 2010.

[28] X. Lin, "CAT: building couples to early detect node compromise attack in wireless sensor networks," in *Proc. IEEE GLOBECOM*, Honolulu, Hawaii, pp. 1–6, Dec. 2009.

[29] X. Lin, R. Lu, P.-H. Ho, X. Shen, and Z. Cao, "TUA: A novel compromise-resilient authentication architecture for wireless mesh networks," *IEEE Transaction on Wireless Communications*, vol. 7, no. 4, pp. 1389–1399, Apr. 2008.

[30] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," in *Proc. International Conference on Information Processing in Sensor Networks (IPSN 2008),* Missouri, USA , pp. 245–256, Apr. 2008.

[31] D. Nacache and J. Stern, "Signing on a postcard," in *Proc. Financial Cryptography - FC 2000,* LNCS 1962, pp. 121-135, Springer-Verlag, 2001.

[32] Ontario Energy Board, Internet: http://www.oeb.gov.on.ca/OEB/Consumers/Electricity/Electricity+Prices, [last accessed Apr. 13, 2010].