SECURE COMMUNICATION GATEWAY DESIGN FOR SMART GRID

By

Xiaochen Tang

A THESIS

Submitted
to Michigan State University
in partial fulfillment of the requirements
for the degree of

MASTER OF SCIENCE

ELECTRICAL ENGINEERING

2012

ABSTRACT

SECURE COMMUNICATION GATEWAY DESIGN FOR SMART GRID

By

Xiaochen Tang

Secure and efficient communication between human being and managed devices is critical for Smart Grid and Smart Home. This thesis considers the architecture and design of a secure access gateway (SAG) for home area networks. The SAG serves as the interface between the remote users and the managed devices, such that real-time secure monitoring and control of the devices can be achieved through a Smart Phone. We try to address the security and capacity challenges using multilayer techniques. Security enhancement is ensured through network layer protocol development, as well as inherently secure physical layer transceiver design, capacity improvement is achieved through dynamic spectrum sharing. We also develop an evaluation platform of our proposed system and implement our secure algorithm on that platform. Remote monitoring and control of home/office devices through a Smart Phone is coming closer to us more than ever before.

To my family and friends.

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my appreciation to my advisor, Dr. Tongtong Li, for her continuous support, guidance and encouragement throughout my master years. She makes a great effort to help me in every aspect, from providing advice on research to personal development and growth. She is more than an advisor, she is a friend, a life mentor.

I want to thank Dr. Jian Ren and Dr. Shantanu Chakrabartty from the Department of Electrical and Computer Engineering for serving on my committee. I am deeply indebted to them for their support, either in the classroom or in all thoughtful correspondences. I would also like to thank Dr. Fangzheng Peng and Dr. John Deller from Department of Electrical and Computer Engineering for their valuable advice and help when I first come to Michigan State University.

I am grateful to all my friends who have made my life at Michigan State University an enjoyable experience. Thanks to my friends from the QBJDLXFD, Zhuo Wang and Yongchao Hao, for treating me like family. I would also like to thank all my friends around the world, Yuzong Liu, Xingguang Qu, Yuan Wei and Qiaoyi Zhang for all the fun times and encouraging conversations. I would like to send a special thank you to my lab mates Dr. Lei Zhang, Dr. Leonard Lightfoot, Ms. Abdelhakim Mai, Mr. Di Tang and Mr. Jian Li, for their valuable discussions on the research issues, as well as their helpful advices on the daily life.

Lastly, I would like to thank my parents, my uncle, my aunt and my extended family for their underlying love and constant support. Many thanks to my special one, who had never shown up in the past three years, without whom makes me so focused in the lab.

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1

INTRODUCTION

1.1 Concept of Smart Grid and Smart Home

1.1.1 Risk of The Current Power Grid

The current power grid was started to build in the 19 century and upgraded based on technology through each decade. Today, it consists of more than 9200 electric generating units with more than 1 million megawatts of generating capacity connected to more than 300,000 miles of transmission lines [1]. However, the limitations of one-way interaction, centralized system make it difficult to response the changing and arising energy demand of the 21 century.

Reliability is one of the modern challenges that our current power grid have not kept pace. As electricity is needed almost everywhere in our daily life, blackouts and brownouts affect more consumers as before, result in huge economic loss today. However, due to lack of real-time and automated response capability, more and more blackouts or brownouts occur in recent decades. What is worse, in most area of the United States, the only way that utility can learn blackouts happen is reported by customer.

Another modern challenge that our current power grid struggling to keep up is peak demand. The energy demand is not stable, but varying. In other words, most time demand for electricity maybe in a normal range. However, sometimes such as a extremely hot summer day, demand for electricity would be driven substantially higher to its peak. As a result, utilities have to spend much money to build new infrastructure and maintain existing infrastructure so that supply for electricity can meet the peak demand. But, due to demand for electricity would not always be in its peak and electricity must be consumed the moment it's generated, the excess generated electricity is wasted.

Besides, the current power grid is also at risk in security. Due to the centralized structure of current grid, once a component in the grid was attacked, the affect may expand to all the interde-

pendent components in the grid which is like a domino effect. As a result, a cascading series of failures may bring serious damage to our nation's banking, communications, traffic, and security systems among others.

Moreover, efficiency, environment risk such as greenhouse gases are also big problem result from our current power grid. To move forward, we need a new kind of electric grid that can increase the reliability, efficiency, flexibility and security of the electricity network in the 21 century.

1.1.2 The Smart Grid Architecture and Key Features

There are already many different definition for Smart Grid. Someone may consider it as an upgrade of existing power grid. Others may see it as a totally different revolution of current power grid. In my point of view, Smart Grid is a combination of current power grid working together with communication technology, advanced automated control algorithm and new energy equipment. The essential improvement is that, with the help of communication technology integration, the Smart Grid will transform one-way interaction, centralized power system into two-way interaction, decentralized power system.

Figure 1.1 shows a conceptyre architecture of Smart Grid system. It is composed of several systems such as power generators, system operator control and data centers, phasor measurement units, distribution systems, transimission systems, consumer domains like home, office and factory, etc. By integrating communication technology and advanced control algorithm, each domain or system can automated communicate and coordinate with others. Under this structure, the Smart Grid will be less decentralized than the current power grid. Hence the Smart Grid will be capable of resisting more malicious attack and natural disasters. Moreover, the two-way communication system offer a two-way visibility and control of energy usage.

The Smart Grid will integrate phasor measurement units (PMU) into every electric delivery system including power genenators, transmission systems, distribution systems and consumer domains. The PMU is a device that measures the volatage and current several times a second at a given location of the grid, comparing the power quality information acquired from system opera-

Figure 1.1: Smart Grid Architecture "For interpretation of the references to color in this and all other figures, the reader is referred to the electronic version of this thesis"

tor control and data center. Hence it provides a wide-area power system monitoring and situation awareness, which makes detection or even prevention of the brownouts or blackouts much easier. It will also increase the possibility of distributed power generation, bring power generation closer to power consumption, which makes the power system more efficient, economical and "green".

In the consumer domain, the Smart Grid will update the legacy electric meter to the advanced metering infrastructure (AMI) The AMI is not a traditional defined meter that only record the consumption of electric energy. It provides an approach to involve consumer affecting utilities, regulators, energy service providers by enable two-way communication between the meter and the central system. Both the utilities and the consumer can get the data of power usage remotely and real-time. The utilities can adjust the price of the energy in real-time based on the data reported by

AMI. For example, the utilities could increase the price during the peak demand time and lower the price when the demand is less than usual to encourage consumers using the energy in different time to lower the peak demand at a instant period. On the other hand, after gathering information processed by AMI, the customers could tailor their energy consumptions in responding to price or environmental concerns. As a result, the peak load burden will be reduced without adding expensive infrastructure.

1.1.3 The Smart Home Concept

The Smart Home has much overlaps and inter-connections with Smart Grid. It communicates with the Smart Grid and enables consumer to manage their electricity usage. The Smart Home is composed of a home area network (HAN), smart meters, smart appliances and home energy management systems. Inside the Smart Home, a home area network (HAN) connects smart appliances and other electrical devices to a energy management system. The smart meters, instead of current mechanical meters, can provide a Smart Grid interface between utility company and consumer home. The smart meters can help utility company better estimates the energy consumption of each consumer by transfering information between consumers and themselves. The smart appliances are devices that can adjust their run schedule to reduce the electricity demand on grid at critical time and lower consumer energy bills. The home energy management system can gather all the energy information coming from utilities and smart appliances, allow householder to monitor real-time information and price signal from utilities, track energy usage in detail and control smart appliances to better save energy from computer or even hand-held device.

1.2 Communication between Human Being and Devices

From the description of Smart Grid and Smart Home, we learned that the Smart Grid is a truely complexty modern power system. There are lots of research fields included in Smart Grid such as efficient power generation and distribution, advanced system monitoring an control. However,

the Smart Grid could not be called "smart" without the real-time, two-way secure communication, etc. In other words, commnucation is involved everywhere into the Smart Grid. For example, the communication between the generation and distribution system, PMU and system data center, the AMI and the utilities or the human being and the Smart Home appliances. Our research focuses on a real-time, secure wireless communication interface between human being and the monitored Smart Home appliances.

1.2.1 Motivation

Along with the rapid development in wireless technologies today, people can receive high speed multimedia information services at any place covered by a communication network. However, while we can talk to people at the other end of the globe through a Smart Phone, we cannot turn off a forgotten light or close an unattended garage door once we are out of the range of the remote controllers. The reality is:

(i) Long distance information exchange through wide area networks (WANs) has largely been limited to phone-to-phone or phone-to-computer communications for pure information transmission or acquisition.

(ii) Development of human-to-device interfaces, such as home automation systems and integrated car-driver interfaces, has largely been limited to local area networks (LANs) or personal area networks (PANs), ranging from 10 to 100 meters.

On the other hand, today's WANs and LANs are on their way to mature development by supporting scalable multimedia services with increasingly *flexible* designs. The advances in WAN and LAN technologies drive for the convergence of wide area wireless systems and localized device networks, which is expected to bring a new wave of revolution to our daily lifestyle, just as in the widespread of the Internet and mobile communications.

Inspired by the observations above, we consider the development of wireless-enabled smart systems that can achieve seamless monitoring and control of localized devices or device networks

with a Smart Phone, through secure two-way communications between the Smart Phone and the managed devices.

1.2.2 Major Challenges

In this thesis, we discuss the design of a reconfigurable framework for mobile-based device monitoring and control, which can be applied to both fixed or moving LAN scenarios, such as vehicle electronics, power and energy systems, etc. We start by identifying the limitations with existing works and the major challenges in the proposed system design.

1.2.2.1 Network Layer Security and Privacy

Security is a key enabler for the prevalence of mobile-based device monitoring and control. It would be totally unacceptable if the devices are monitored or controlled by an adversary, or if the signal received by the mobile device is from, or has been modified by a malicious attacker. Moreover, privacy leakage (including location privacy) can lead to property loss, or even cost of life. That is, security has to be ensured from the aspects of access control, privacy protection, communication integrity, and intrusion detection.

Unfortunately, the security provided by existing systems is far from adequate. In existing systems, the access control at the LAN is either achieved through password-based authentication or biometric-based authentication. As is well-known, the static password-based authentication is vulnerable to eavesdropping attacks and message replay attacks. On the other hand, biometric-based authentication in existing systems has been implemented with inadequate protection to the biometrics. A major risk raised here is that: biometrics are not replaceable; once intercepted, replay attacks can be launched against the authorized user and the access control system. Moreover, communication integrity (i.e. , the received packet is intact), intrusion detection and source/destination privacy have received little attention in existing mobile-based device monitoring and control systems.

Clearly, we need to design advanced cryptographic algorithms, protocols and tools to ensure system security and source privacy. The major challenges here include:

(i) How to design efficient but effective security solutions tailored for mobile-based device monitoring and control in unprotected wireless environments?

(ii) How to track user accountability while preserving privacy protection?

1.2.2.2 Physical Layer Security

In existing systems, security has largely been limited to higher layers, independent of the PHY layer transceiver design. As a result, the PHY layer of most wireless systems does not possess built-in security features. However, all the information exchange activities eventually have to take place in the PHY layer. Without the cooperation of a PHY layer enabled with built-in security, wireless signals are fragile to hostile jamming, detection and interception attacks, in which jamming is the most dangerous threat. This lowers the barrier to PHY layer attacks on user and network information, and also leads to inefficient transmission.

Performance of the PHY layer system is limited by both the self interference caused by time/frequency dispersions and the hostile jamming launched by an adversary. In general, the highly efficient systems developed today mainly focused on self interference mitigation, and have no inherent security features. The only exception is the spread spectrum systems, including CDMA and frequency hopping. Both of them have anti-jamming and anti-interception features by exploiting frequency diversity over a large spectrum, hence have very low spectral efficiency. Moreover, the conventional spread spectrum systems were originally developed for voice-centric communication which only lasts a short period. Their security features are far from adequate for today's high speed multimedia communications. Therefore, the major challenge here is: how to design highly efficient and inherently secure wireless systems for reliable communication under hostile environments?

1.2.2.3 Demand on Capacity

While providing a new class of wireless services, cyber-enabled device monitoring and control also imposes new capacity demand on wireless networks. This is because that: unlike wired networks where new requests on communication services can largely be resolved by adding more transmission lines, in wireless networks, the total available spectrum is mainly limited by the radio frequency (RF) technologies, and has to be *shared* by various users and services at each power defined zone or cell. Once the system is overloaded, network performance and reliability would be lost or greatly degraded. In order to accommodate more users with security sensitive service requests, the wireless systems have to be much more efficient, and at the same time, be much more secure and reliable. However, security and reliability are often achieved at the cost of lower efficiency or capacity. The contradiction between security and capacity raises significant challenges in wireless system design and networking.

In addition to efficient PHY layer transceiver design, we consider capacity improvement through cognitive spectrum sharing. The most recent advance in optimal spectrum utilization is represented by cognitive radio. The cognitive radio technique proposes to improve spectrum utilization by enabling a secondary user (SU) to perform spectrum sensing to a licensed primary user (PU), and then transmits on the bands where the primary user is idle or not fully active. However, while each individual cognitive radio can make flexible decisions, lack of user coordination and network control raises serious issues in efficiency and security:

(i) Traffic collisions between the PU and the SU, or among SUs, lead to low efficiency and reliability.

(ii) Mobile-controlled spectrum sensing enables the SU to perform legitimate traffic analysis of the PU, leading to a *security compromise* of the PU.

(iii) Continuous spectrum sensing and real-time decision making at every terminal causes significant resource waste.

The major challenge here is: how to optimize spectrum utilization through cognitive spectrum sharing, but at the same time resolve the traffic collisions, security drawbacks and device resource waste in conventional cognitive radio?

In summary, we will discuss how to integrate all the corresponding devices into the wide-area wireless network for convenient and secure monitoring and control, by establishing a resilient human-device interface. This will certainly increase human capabilities in remote monitoring and control, but at the same time, raise significant security and capacity challenges to existing wireless networks. These challenges need to be addressed in an efficient and extensible way for system realization today as well as future applications.

1.3 Contributions and Thesis Outline

1.3.1 Contributions

The contributions of my work lists as follow:

(i) Helped design our proposed Smart Home architecture.

(ii) Developed the evaluation platform of our proposed Smart Home architecture.

(iii) Implemented our proposed secure authentication algorithm.

1.3.2 Thesis Outline

We already introduced the background of Smart Grid and Smart Home. Besides we present our research area and the major research challenges. The reminder of this thesis is organized as follow. In Chapter 2, we will introduce our proposed Smart Home system architecture and the theory of our proposed secure authentication and control algorithm in detail. In Chapter 3, we will present the implementation of our proposed system from core software algorithm to overall system prototype and evaluation platform. Finally in Chapter 4, we conclude the thesis and discuss the future work.

Chapter 2

SYSTEM ARCHITECTURE AND SECURITY ALGORITHM

In this chapter, we describe the overall proposed system architecutre and each component consisted in the system. In addition, we present the security algorithm in different layer of the communication system. Finally, we introduce a dynamic resource management protocol about network capacity improvement that complement our proposed system.

2.1 Proposed Smart Home Architecture

The proposed architecture for the mobile-based monitoring and control system is shown in Figure 2.1. The purpose of this system is that providing a reality platform and enviroument of the Smart Home to implement and evaluate the secure authentication and control algorithm. This architecture contains three major components: the remote wireless enabled device (called C-Mobile), the Secure Access Gateway (SAG), and the Smart Home Managed Devices. We will describe each component below.

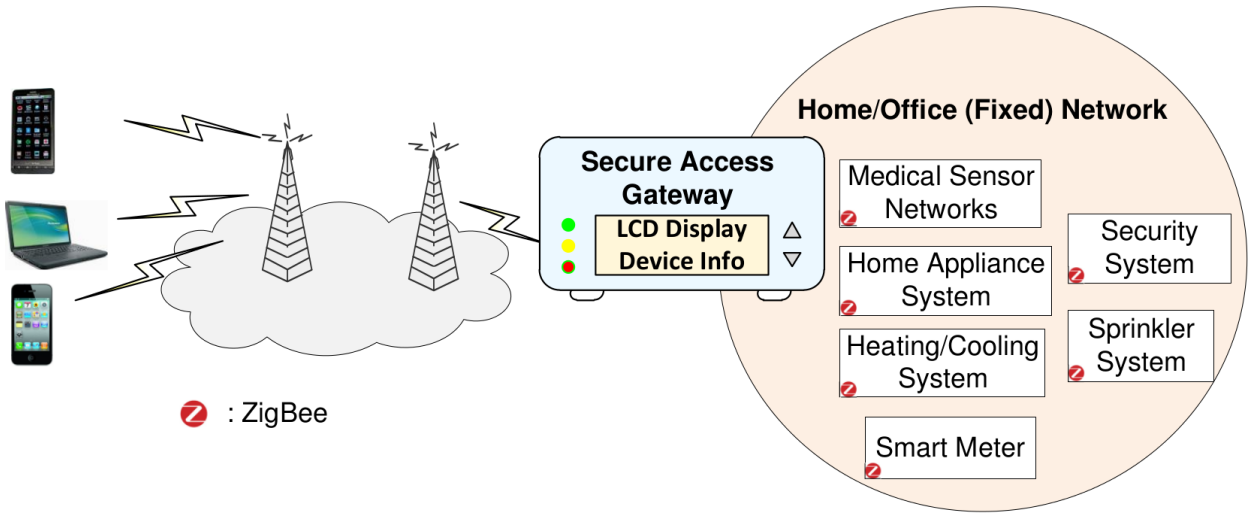

Figure 2.1: Proposed Smart Home Architecture

- C-Mobile: C-Mobile can be any kind of remote terminals or devices (e.g., Smart Phones, notebooks, etc.) gaining services to the Smart Home devices with some kinds of accessing technologies (e.g., GSM/GPRS, 3G/4G, WiFi, etc.).

- SAG: The SAG provides secure protections to the managed Smart Home devices. SAG also enables secure two-way communications be established between the C-Mobile and the managed Smart Home network for secure monitoring and control of Smart Home devices. It also enables Smart Home devices to report alarm. At a higher level, both the C-Mobile and the SAG access the WAN through the base stations.

- Smart Home Managed Devices: The Smart Home Managed Devices can be any kind of ZigBee enabled terminals or devices (e.g., Smart Meter, home appliances, and medical equipment). All the managed devices are connected to the SAG through secure and low power wireless communications over unlicensed spectrum using ZigBee. The SAG is then connected to the C-Mobile through the WAN.

The advantage of using this structure is obvious. Because each network platform has its own package format so that it cannot recognize the data package from other network. By seperating the Smart Home Managed Devices and C-Mobile devices into two different network, it provide a physical barrier of communication between these two type devices. Besides, it allow integrating advanced secure algorithm into the SAG which is less cost than integrating secure algorthm into every Smart Home Managed Devices.

2.2 Network Layer Security

We propose to design efficient cryptographic algorithms, protocols and tools to ensure system security and privacy by exploiting the unique system structure in mobile-based device monitoring and control. The network layer security of this architecture can be imposed by the SAG. As a secure access gateway, the SAG can enforce a number of security services, including access authentication,

access authorization and event tracking. It can also implement some advanced security services such as privacy protection, rule-based intrusion detection and abnormal event alarm.

2.2.1 Access Authentication and Access Control

Ensuring appropriate access permissions only to authorized users is a very challenging task in the open wireless environment. In SAG, a pluggable authentication module (PAM) is proposed to support multiple authentication mechanisms. Existing static password-based access authentication schemes can be easily hacked by replaying/reusing a previously used access credential. To solve this security problem, we propose a one-time password-based (OTP) authentication mechanisms for remote access. In this design, each password is used only once to prevent replay attacks.

The main idea of the proposed OTP secure access authentication is that the C-Mobile and the SAG will share a secret key, k, which can be generated from a strong password. They should also share a linear feedback shift register (LFSR) sequence generator with feedback polynomial $f(x_1, x_2, \cdots, x_n)$, as shown in Figure 2.2, where n is a configurable parameter. The C-Mobile and the SAG can use any segments of the sequence generated from the LFSR as the counters. In order to minimize the possibility for the counters to be repeated, we ensure the period of the sequence to be sufficiently long, which can be guaranteed by selecting the feedback polynomial $f(x_1, x_2, \cdots, x_n)$ to be primitive. The resulted sequence is an m-sequence (maximum length sequence) with period $2^n - 1$. Though the m-sequence has good measurable randomness, it can be easily reconstructed using the Berlekamp-Massey algorithm [4] if a continuous segment of length $2n$ is received. Therefore, the sequence cannot be used directly for user authentication.

In the proposed approach, the m-sequence will only be utilized to generate a sequence of counters with large periods. The counters can be any segment of the m-sequence of the designed length. We can then use a symmetric cipher (such as the Advanced Encryption Standard (AES) [5]) in counter mode to generate a pseudo-random number through encryption of the counter value. The generated pseudo-random number, or a segment of the pseudo-random number, can be used as the OTP for the remote C-Mobile to authenticate to the SAG. That is, the ith OTP_i is given by

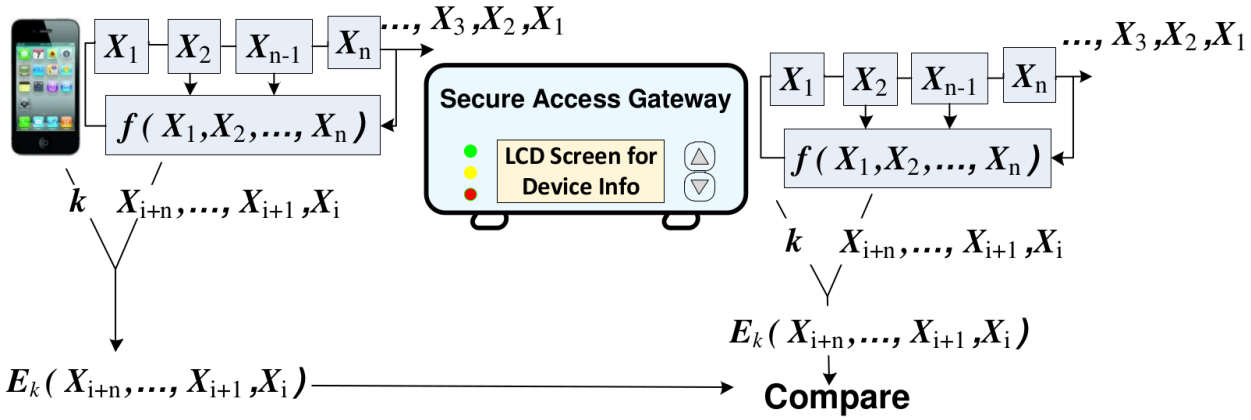

Figure 2.2: Proposed OTP Secure Access Authentication

$OTP_i = AES_k(C_i)$, where E represents the AES encryption algorithm, k is the secret key shared between the C-Mobile and the SAG, and C_i is the ith counter value.

Since each counter value is different, the OTP will be different every time. While the OTP generation is very efficient for both the C-Mobile and the SAG, it is computationally infeasible for any other people to generate the OTP without the shared secret encryption key. In fact, even if the counter initialization is unprotected, it is still infeasible for the adversary to generate the OTP without using the shared secret key. This is ensured by the avalanche effect and security of the AES under known-plaintext attacks. Keeping the counters secret will limit the adversaries to ciphertext-only attacks, which is even more difficult to succeed.

In addition to the security services described above, the communication between the remote device and the SAG can be encrypted to provide communication confidentiality and integrity services.

In SAG, a profile is defined for each C-Mobile, which enables the SAG to support multiple levels of access control for remote access, ranging from system configurations to simple event view. This profile includes an access control list (ACL), resources that can be accessed, operations allowed, and also configurations that cannot be altered. It can also specify the remote access hours, including the days of the week and times of day that the remote access is enabled/disabled.

2.2.2 Event Logging and Alarm

As a security access gateway, the SAG is designed to record all recent logins (including both successful logins and failed logins), their login times and durations. It can also store and analyze the security related events based on the predefined rules, such as unidentified access or access trials that exceed a threshold. The SAG will also record and backup all events periodically. Whenever a predefined event occurs, an alarm can be issued to a pre-configured terminal(s) with an alarm ID and an alarm code. Due to possible traffic collisions and transmission errors, the SAG should be capable of handling multiple access attempts within a threshold defined in the profile, before it issues an alarm and terminates the access.

Even the best access control system may fail sometimes. The SAG will be designed to provide a second line of defense for the controlled systems and devices through the intrusion detection systems (IDS). When a suspicious behavior or an unauthorized access attack is detected, the SAG will terminate the connection and report this event as an alarm to the pre-configured devices.

2.2.3 System Security and Privacy Protection

To prevent identity based security attack, we propose a dynamic ID based secure access. Each terminal/user has to share a secret initial ID and a predetermined secret key k with the SAG. Based on this shared secret, SAG and the terminal will generate an *ID-hash-chain*: $\{id_1, id_2, \cdots, id_n, \cdots\}$, where $id_1 = H(ID\|k), id_2 = H(id_1\|k), \cdots, id_n = H(id_{n-1}\|k, \cdots)$, and H is a one way hash function.

The SAG access authentication will use id_i as its ith login name. Because H is a one-way hash function, the $id_1, id_2, \cdots, id_n$ forms a hash-chain. It is computationally infeasible to compute id_{i+1} from id_i without knowledge of predetermined secret key k. The dynamic login names can prevent the identities from being predetermined, reused and also the attacked. Therefore, it can provide privacy protection to the SAG access.

To make the storage and communication more efficient, the login name can be only part of the hash value (such as 8 characters). Though a short login name could possibly increase the chance for

the login names to repeat, the probability is low. However, since only the C-Mobile and the SAG have the full knowledge of the ID-hash-chain, using short login names can prevent the adversaries from computing the previous login names that leads to link multiple messages transmitted from the same terminal. In this way, adversarial attacks to the SAG can be effectively eliminated and better security protection can be ensured to the terminal device.

From the implementation point of view, both the OTP password and dynamic login names will be executed through an automated process. The users do not need to remember the OTP password and the dynamic login names, which makes the implementation feasible and practical.

2.3 Physical Layer Security

Conventionally, the main task of the physical layer in a communication system is to transmit the information bit stream accurately, timely and efficiently from the source to the destination. The efficiency here including both power efficiency and bandwidth efficiency. In civilian applications, security is generally not taken into consideration for physical layer transceiver design, but mainly left to the network layer, which tries to cover user authentication, access control, confidentiality, accounting, privacy etc. As a result, the PHY layer of most wireless systems (such as OFDM, GSM) does not possess built-in security features. However, all the information exchange activities eventually have to take place in the PHY layer.

Due to the lack of a protective physical boundary, wireless signals are subjected to hostile detection, interception, and intentional jamming. Hostile jamming, in which the authorized user's signal is deliberately interfered by the adversary, is one of the most commonly used techniques for limiting the effectiveness of an opponent's communication, and is the most harmful attack. Along with the wide spread of various wireless devices, especially with the advent of user configurable intelligent devices (such as cognitive radios), physical layer malicious attack is no longer limited to battlefield or military related events, but has become an urgent and serious threat to civilian communications as well. These attacks, especially the jamming attacks, cannot be effectively resolved based solely on higher layer security techniques, but have to be investigated from the

physical layer as well. In other words, we need to design wireless systems with built-in security.

In literature, the only systems that have built-in security features are spread spectrum systems, including direct-sequence CDMA systems and frequency hopping (FH) systems, which were originally developed for secure communications in military applications. Both CDMA and FH systems possess anti-jamming and anti-interception features by exploiting frequency diversity over large spectrum. However, mainly limited by multiuser interference (caused by multipath propagation and asynchronization in CDMA systems and by collision effects in FH systems), the efficiency of existing jamming resistant systems are very low due to inefficient use of the total available bandwidth. Although these systems work reasonably well for voice centric communications which only requires relatively narrow bandwidth, the *security feature* and *information capacity* provided by these systems are far from adequate and acceptable for today's high speed multimedia wireless services. Note that security is generally achieved at the cost of lower spectral efficiency. For secure, especially jamming resistant, wireless system design, the major challenge here is: How to design wireless systems which are highly efficient but at the same time have excellent security features?

2.3.1 Revisit of the Spread Spectrum Systems

Traditionally, both CDMA and FH have been used for secure communication under hostile environments. CDMA is especially robust to narrow band jamming by reducing the jamming power through the despreading process. Moreover, CDMA can hide the signal within the noise floor so that the adversary cannot even detect the existence of the signal. On the other hand, FH system is more robust to wideband jamming, since the signal power can be concentrated on a narrower frequency band during each hopping period. As the carrier hops randomly over a wide range of frequencies, it is hard for the adversary to track or jam the active transmission.

The above understanding for FH is mainly based on slow frequency hopping (SFH), where hopping period is equal to or larger than the symbol period. In a traditional frequency hopping system, as the transmitter hops in a pseudo-random manner among available frequencies according

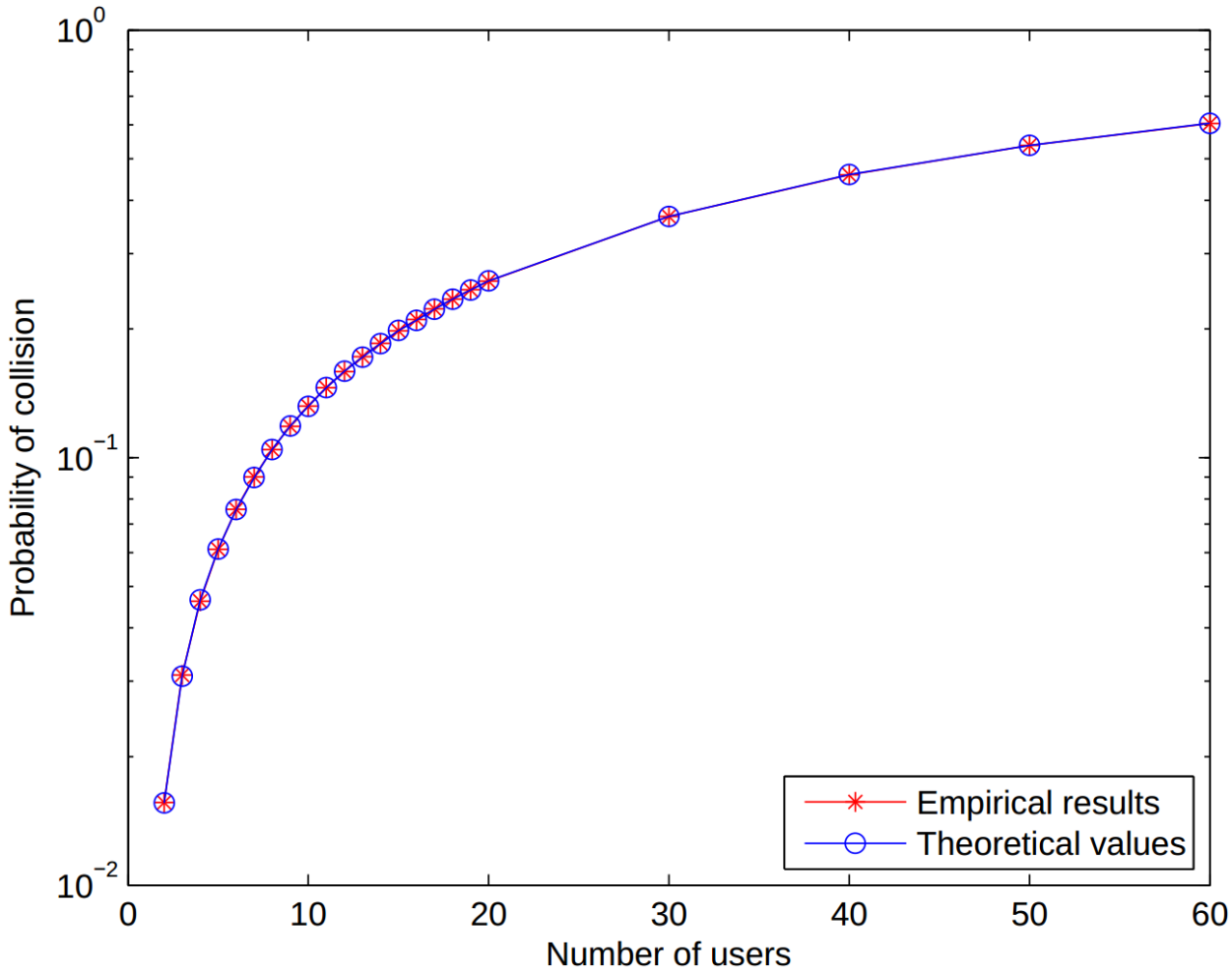

Figure 2.3: Collision Effect in an FH System with 64 Channels

to a pre-specified algorithm, the receiver has to operates in a strict synchronization with the transmitter and remains tuned to the same center frequency. The strict requirement on synchronization directly influences the complexity and performance of the system, and turns out to be a significant challenge in fast hopping system design. For this reason, existing work on FH has mainly been limited to slow hopping systems.

It is interesting to notice that: if we put the strong requirement on frequency acquisition aside and consider the fast frequency hopping (FFH) systems, then we can find that *CDMA is actually a special case of FH*, for which you happen to "hop" just on (actually fixed to) the same band, and during each hopping period or chip period, you transmit either the chip signal itself or its negative version. In other words, CDMA uses only repeated coding, which is the least efficient

channel coding, and CDMA has fixed carrier frequency. Clearly, FH provides a more general and more flexible framework for anti-interception, anti-jamming system design. However, as shown in Figure 2.3, the spectral efficiency of the conventional FH is very low due to the collision effects among different users.

2.3.2 PHY Layer Security Enhancement for OFDM System

Orthogonal frequency division multiplexing (OFDM) is by far the most efficient modulation scheme, and is expected to be used widely for reliable two-way communications in Smart Grid and Smart Home. The basic principle of OFDM is to split a high-rate data stream into a number of lower rate streams that are transmitted simultaneously over a number of orthogonal subcarriers. OFDM can effectively eliminate the intersymbol interference (ISI) caused by the multipath propagation and achieve high spectral efficiency. By assigning subsets of subcarriers to individual users, we then obtain a multi-user version of OFDM, known as orthogonal frequency-division multiple access (OFDMA). Due to its high spectral efficiency and scalability, OFDMA has emerged as one of the prime multiple access schemes for broadband wireless networks. However, OFDMA does not posses any inherent security features and is fragile to hostile jamming and interception.

Motivated by the observation that the efficiency of conventional FH is mainly limited by the collision effect, we investigate a network centric collision-free frequency hopping scheme based on a secure carrier assignment algorithm [6]. The proposed secure subcarrier assignment is achieved through an advanced encryption standard (AES) based secure permutation algorithm, which is designed to ensure that:

(i) Each user hops to a new set of subcarriers in a pseudo-random manner at the beginning of each hopping period.

(ii) Different users always transmit on non-overlapping sets of subcarriers.

(iii) Malicious users cannot determine the hopping pattern of the authorized users, and hence cannot launch follower jamming attacks.

The secure carrier assignment algorithm actually provides an FH based network centric dynamic spectrum access control and management scheme. It can be applied to different multi-carrier systems to prevent unauthorized signal interception and hostile interference. If we apply the proposed collision-free frequency hopping (CFFH) scheme to OFDMA, then we obtain a highly efficient anti-jamming system. The resulted system has both time and frequency diversity, and can effectively mitigate both random jamming and follower jamming. Moreover, it has high spectral efficiency ensured by OFDM, and at the same time can relax the complex frequency synchronization problem suffered by conventional FH systems.

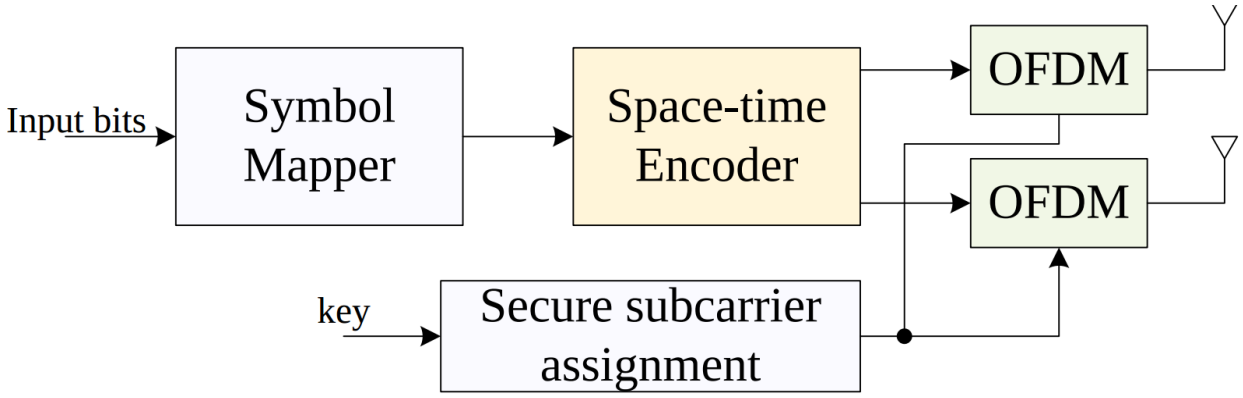

Figure 2.4: STC-CFFH Transmitter

The anti-jamming property of the OFDMA based CFFH can be further enhanced by incorporating space-time coding (STC) [7] (as shown in Figure 2.4), which is a technique that exploits space diversity by transmitting different versions of the same signal through multiple antennas. When there are N_T transmission antennas and N_R receiving antennas, then the system capacity can be increased linearly by a factor of $\min\{N_T, N_R\}$. When incorporated with OFDM, the space-time diversity in space-time coding is then converted to space-frequency diversity. The combination of space-time coding and CFFH is particularly powerful in eliminating channel interference and hostile jamming interference, especially random jamming.

2.4 Capacity Improvement Through Dynamic Resource Management

Cognitive radio has been proposed as a promising technique to promote efficient wireless spectrum allocation [8]. The idea of cognitive radio is motivated by the observation that lots of licensed frequency bands in the spectrum are largely unoccupied or only partially occupied most of the time. This under-utilization of the electromagnetic spectrum leads to the thought that: spectrum utilization can be improved significantly by making it possible for a secondary user (SU) to access a spectrum hole unoccupied by the licensed primary user (PU).

2.4.1 Introducing Cognitive Network

As an exciting concept, cognitive radio emphasizes the power or capability of the *individual* radio devices. However, allowing the radio devices to modify user services and reconfigure RF parameters can raise serious efficiency and security concerns for PUs, operators and regulators, including:

(i) Spectral inefficiency due to traffic collisions between the PU and SU, and among the SUs themselves.

(ii) Serious security fragility evoked by spectrum sensing and denial-of-service attack launched by hostile SUs.

(iii) High terminal costs, as each SU is required to perform continuous spectrum sensing.

Therefore, mandatory network control has to be enforced. Motivated by these observations, we introduce the concept and architecture of *cognitive network*.

By cognitive network, we *mean* an intelligent wireless system that can collect and analyze the current network conditions, and then make real-time changes to network operating parameters (e.g., modulation scheme, transmission power, carrier frequencies, data frame structure, coding schemes, resource allocation in the joint time-frequency-space domain, and security mechanisms) for optimal network performance. The overall goal is to ensure spectrally efficient and secure information exchange among versatile wireless devices, including both the legacy devices and the

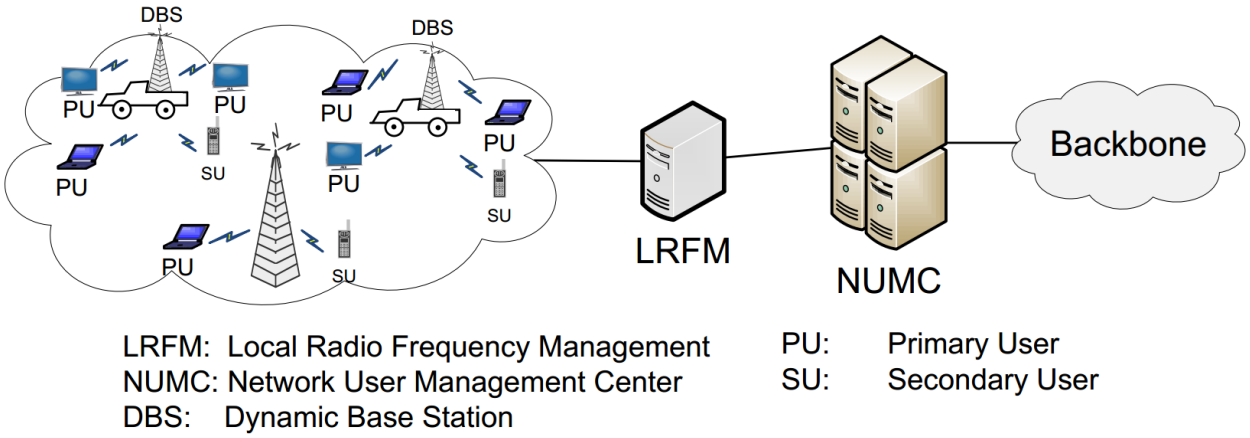

Figure 2.5: Architecture for Cognitive Networks

powerful software-defined radios (SDRs). We propose a novel architecture for cognitive network, as shown in Figure 2.5, with the objective of increasing the spectral efficiency, system reliability, flexibility and scalability.

In this architecture, we allow co-existence of fixed and dynamic BSs and introduce the concept of Local Radio Frequency Management (LRFM) center and Network User Management Center (NUMC). All the users, both PUs and SUs, register with the NUMC to become authorized users. In wireless systems, one spectrum reuse region may contain one or more cells, and is generally referred to as a *cluster*. An LRFM is attached to each cluster. The LRFM is responsible for continuous spectrum sensing, and dynamic resource allocation for collision-free spectrum sharing among all the users within the cluster. Network management tasks, such as user authentication, access control, handover and accounting, are conducted by the NUMC, with assistance of the LRFM. While increasing spectrum efficiency and protecting the privacy of the PUs, this architecture also makes the SUs more feasible and cost efficient since they are no longer required to perform continuous spectrum-sensing. Moreover, the system flexibility and scalability are increased significantly by introducing vehicle mounted dynamic BSs into the fixed infrastructure.

In the following, we will explain how the system works within each cluster, and how the clusters are connected into a network.

- First, the subscribers register with the system through the NUMC. In reality, the system

generally has some fixed PUs, like those involved in TV/radio broadcasting and public safety systems. All the other users access the network in a random manner. An authorized user can request PU service(s) or SU service(s) based on the user's need and resource availability at each communication event. PUs will be granted higher priority and higher Quality of Service (QoS), at a higher service cost. For a time sensitive signal, like a phone conversation, the user can claim itself as a PU. While for a less time sensitive and short delay tolerable signal, like transmitting a short message or email, the user can claim itself as an SU to get a better price deal.

- QoS for PUs will be divided into different levels, with a minimum information rate guarantee for all the PUs. PUs have higher priority for all the unassigned frequency bands. At the same time, the system can still support a considerable number of SUs due to the wide existence of spectrum holes or under-utilization.

- Spectrum allocation for all the users (including both PUs and SUs) within a cluster is managed by the LRFM attached to the BSs. Spectrum sensing of the PUs will be performed by the LRFM, and the detected spectrum holes are distributed among the SUs. Note that the LRFM can be equipped with advanced receivers and strong data processor and controller, and it also has the real-time information of the frequency band occupied by each PU. The LRFM can perform much more accurate spectrum sensing and highly efficient dynamic resource allocation. As a result, transmission collisions can be completely resolved, and each user terminal no longer suffers from the burden of continuous spectrum sensing and access frequency selection.

- When the user is moving from one cluster to another cluster, it will be handed over to the LRFM in the new cluster through the NUMC. NUMC is also responsible for other network management tasks, including user authentication, access control, and accounting (for billing and record tracking purpose) etc.

2.4.2 General Protocols

Note that each cluster has a LRFM, which is responsible for spectrum allocation of all the PUs and SUs in the cluster. Within each cluster, the total available spectrum generally contains numerous frequency bands and services. For maximum spectral efficiency, we will rely on network-controlled software-defined radio (NC-SDR). The frequency shift and transmission rate variation of the mobile set are invoked or controlled by the LRFM. For a rather long period, there will be coexistence of NC-SDRs and legacy devices which can only be used at a fixed frequency band. Generally, legacy devices can only be registered as PUs due to lack of flexibility, since SUs have to be able to shift from band to band and allow variable transmission rates. The NC-SDRs are coordinated with the legacy devices for maximum frequency utilization according to the following rules:

- *NC-SDRs versus legacy devices* When a new user enters the system, the LRFM will first determine whether it is an NC-SDR or a legacy device. If it is an NC-SDR, the LFRM will assign it to the band with the lightest traffic load. If it is a legacy device, the LFRM has to assign it to its designed working band, and move the NC-SDRs to other bands if necessary. In practice, for maximum system capacity, telecommunication carriers often provide free upgraded mobile devices to user to get rid of legacy mobiles.

- *PUs versus SUs* PUs have higher priority on unassigned bands over the SUs. Partially assigned bands are mainly assigned to SUs, a PU will be put on partially assigned bands only if the minimum required transmission rate can be guaranteed for the PU. Except the fixed group of PUs (like TV and radio stations), a primary service request would be accepted only when the requested transmission rate can be ensured by the system, otherwise the user has to be register as an SU.

2.4.3 Network Capacity Evaluation and Cluster Size Control

We first estimate the network capacity from an information theory point of view, and then convert it to the capacity in terms of the number of users that can be supported by the system under a required QoS.

Based on Shannon's channel capacity theory, for an ideal additive white Gaussian noise (AWGN) channel (that is, a flat fading channel) of bandwidth BHz, the channel capacity can be calculated as:

$$C = B\log_2(1+SNR)\ bits/sec \tag{2.1}$$

where SNR is the signal-to-noise ratio. In wireless communications, due to the effect of multipath propagation, different frequency components of the transmitted signal generally experience different fading effects. In other words, we have to deal with non-ideal frequency selective channels, and we need to extend the results for the ideal channel to frequency selective channels. To do this, we divide the bandwidth into small bins of width Δf, where Δf is small enough that the channel transfer function is approximately constant over the range of Δf. The total capacity is then the sum of the subchannel capacities.

Once the network capacity is evaluated, the total number of users that can be supported will be estimated under the required QoS, including data rate, the probability that a call is blocked, and the average delay for queued calls. With these results, cluster size control or the frequency reuse spectrum management plan can be carried out through appropriate transmit power adjustment.

2.4.4 Dynamic Spectrum Sharing

Equal average load criterion In the proposed cognitive network architecture, the LRFM is spectrum aware. It maintains a real-time spectrum usage distribution for all the frequency bands. The spectrum is divided into three categories: white spectrum, gray spectrum and black spectrum. White spectrum denotes the spectrum that is unassigned, or not allocated to any users; gray spectrum denotes the spectrum that is assigned to a user (generally a PU), but is not fully utilized; black

spectrum denotes the spectrum that is fully occupied and utilized by a PU. In order to optimize the system performance, we propose to distribute the traffic uniformly among all the available bands based on the water-pouring criterion, so that a constant average load is maintained over different bands. We name it as the *equal average load criterion*. The realization of this criterion needs to be investigated jointly with dynamic user assignment based on the corresponding multiple access schemes and channel state information. The multiple access techniques used in the network directly impact the spectrum allocation scheme design. In addition to efficiency, we can also take the anti-interference and anti-interception properties of the systems into consideration. When the frequency-hopping (FH) technique is involved for security purpose, spectrum allocation will be more dynamic.

Dynamic Resource Allocation Consider a cognitive network with a centralized base station. Each user has a data rate request and a power constraint. The spectrum is divided into N bands, each consisting of a group of equal-sized channels of bandwidth. The channel impulse responses are assumed to be independent to each other.

The spectrum can be allocated to SUs only when the primary users are absent. It is assumed that the base station has the global knowledge about which channels are occupied by the primary users and which ones are vacant. For $i = 1, \cdots, N$, We define the effective load factor η_i as below to measure the utilization of band i,

$$\eta_i = \frac{\text{active traffic over band } i}{\text{total capacity of band } i} \tag{2.2}$$

Consider the frequency division multiple access (FDMA) scheme, where η_i is equivalent to the ratio between the number of channels occupied by the primary users and the total number of channels in band i.

Through a dedicated feedback channel, SUs provide to the base station information about their maximum transmit power as well as desired data rates, according to which the base station will make the resource allocation [9]. Since the number of available channels varies dynamically in cognitive networks, resource allocation may not guarantee the full satisfaction of users rate re-

quests. For a large spectrum consisting of many channels, it is unrealistic to assume that all the instantaneous channel gains are known for each SU. However, it is not difficult to obtain the mean channel power, which can then be used for channel allocation by the base station.

When a user has a desired rate R_k, we can convert it as a request for a minimum number of channels N_{min}. If the system has an engineering limit on the maximum number of channels that one user can use, N_{limit}, then the number of channels that the system will allocate to this user is $M = \min\{N_{min}, N_{limit}\}$. Load balance can be achieved using the water filling method.

Chapter 3

EVALUATION PLATFORM AND SECURE ALGORITHM IMPLEMENTATION

The purpose of implementing our proposed system is to provide a practical evaluation platform of the Smart Home architecture. Any further research of Smart Home can be implement and evaluate upon this platform. As we have described in Chapter 2, The system includes three component: the C-Mobile devices, the Secure Access Gateway, and the Smart Home Managed Devices. The platform consists of two seperate networks. One is called external network, which is used to provide communication service between C-Mobile devices and the SAG. The other one is called internal network, which is used to provide the communication service between The SAG and the Smart Home Managed Devices. The goal of our implementation is to provide a secure end-to-end two-way communication between the C-mobile devices and the Smart Home Managed Devices through the Secure Access Gateway (SAG). The final practical evaluation platform should have the following functions:

- The C-mobile devices could access the SAG to control the Smart Home Managed Devices or ask for data from Smat Home Managed Devices.
- The Smart Home Managed Devices could report instant alarm or data to the SAG and the SAG is able to forward this report to such C-mobile device.
- The SAG enable a secure authentication service that only allowing the authenticated C-mobile devices to communicate with Smart Home Managed Devices.

Next we will first introduce the hardware platform and networks that our system prototype are build upon. Then, we will introduce the details of how we implement functions into our evaluation platform.

3.1 Overall Evaluation Platform

Figure 3.1 present the evaluation platform we implemented for our proposed Smart Home architecture. The computer and the Smartphone represent the C-Mobile devices. The device located in the middle of the platform is the SAG. The two devices to the right are called CC2430 DB and MICAz Sensor Mote. They are used to represent the Smart Home Managed Devices. On one side, for the external network or public area network, the C-Mobile devices communicate to the SAG via the external interface. On the other side, for the internal network or home area network, the Smat Home Managed Devices communicate to the SAG through the internal interface.

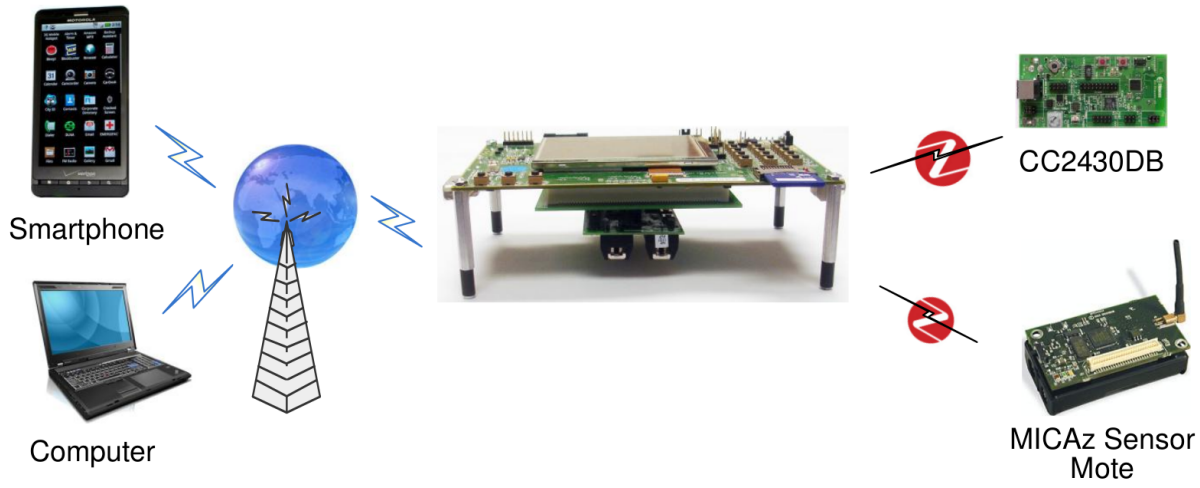

Figure 3.1: Overall System Physical Prototype

3.1.1 System Network Platform

Accrording to the requirement of an end-to-end secure communication, both the two network platforms should have integrated a varieties security service to provide information confidentiality, effective access control and prevent malicious attack. Except the common security requirement, they also have different properties according to the different communication objects. For the external network platform, it should be capability of providing long distance communication between the C-Mobile device and the SAG so that the SAG could be accessed by or trace back to the C-

Mobile device far away from the SAG location, even anywhere around the world. Otherwise, it will be meaningless if the communication is limited by distance. On the other hand, the main concern of the internal network platform is not the communication distance since all the communication happen in home area. But it should be able to provide low energy consumption, low cost and secure network service.

3.1.1.1 External Network Platform – Internet

There are only two existing network platforms that can provide a long distance transmission and can be implemented in our system: the Cellular network (GSM, 3G) and the Internet. Both of them are mature and their services are available worldwide. However, because of the reason that we need the service contract from a service provider such as (At&T, Varizon, Sprint) to allow us to transfer data on the cellular network, we determine to use Internet for our external network connectivity.

Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve billions of users worldwide. Millions of private, public, academic, business, and government networks consist the Internet. The range of Internet is from local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. It has no centralized governance in either technological implementation or policies for access and usage so that we can implement our system uppon Internet platform. People can access Internet almost everywhere around the world by numerous approach, including through mobile Internet devices, mobile phones, datacards, handheld game consoles and even cellular routers wirelessly [10].

The framework of Internet that is defined in the Internet protocol suits is devided into four layers: application layer, transport layer, internet layer and link layer.

- ***The application layer*** which is the highest layer contains all protocols and method that defined for data communication service based on a process-to-process level (e.g., HTTP for web browser or SMTP for email service)

- ***The transport layer*** which is under the application layer provides end-to-end communication services for applications in different hosts. The most well know protocol in transport layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). The former is used for a connection-oriented communication, whereas the latter is used for connectionless byte-oriented communication.

- ***The internet layer*** which is below the transport layer connects local networks. It is the fundation of the internet by providing methods and protocol that are used to transfer packets from the original host across the network boundaries. It enable computers and devices that are in the network to identify and loacte each other via Internet Protocol address (IP address) which is a numerical label assigned to each device participating in the Internet.

- ***The link layer*** which located at the bottom of the internet protocol suits provides connectivity between hosts on the same local network. It contains methods and protocols that operate only on adjacent network devices.

3.1.1.2 Internal Network Platform – ZigBee

The internal secure communication is used to exchange data between the Smart Home appliances and the SAG. Hence, it is better to be a wireless communication than wire communication. And it also should be low consumption and low cost as we descibed before. To compare several different wireless communication platform such as WIFI, Bluetooth and ZigBee, we finally select ZigBee as our internal communication platform beacuse of its low cost, fast response time and security features.

ZigBee is a specification for a suite of high level communication protocols using small, low-power digital radios based on IEEE802 standard for personal area networks. The design of ZigBee is intended to be cheaper and simpler than other wireless personal area network protocol such as Bluetooth. The motivation to develop ZigBee is to provide a solution for radio frequency applications that require a low data rate, long battery life, and secure networking. As a resule, it really

suitable for Smart Grid and Smart Home applications and other consumer energy equipment. ZigBee has a defined data rate of 250 kbps and operates in the unlicensed industrial, scientific and medical radio bands including 868 MHz in Europe, 915 MHz in Nouth America and Australia and 2.4GHz in globe [11].

Figure 3.2 shows the ZigBee protocol stack. It includes for layers: The physical layer, media access control (MAC) layer, network layer and application layer. Zigbee builds upon the physical layer and medium access control layer defined in IEEE 802.15.4, which specifies the physical layer and MAC layer for low-rate wireless personal area network. It adds network layer and application layer to complete the protocol. ZigBee network layer supports both tree and star typical network structure. Besides, it also supports generic mesh network structure. The application layer components including ZigBee device objective (ZDO), application objective, application support sublayer and security service are responsible for providing ZigBee main function such as secure communication, management of join a network, device discovery, etc.

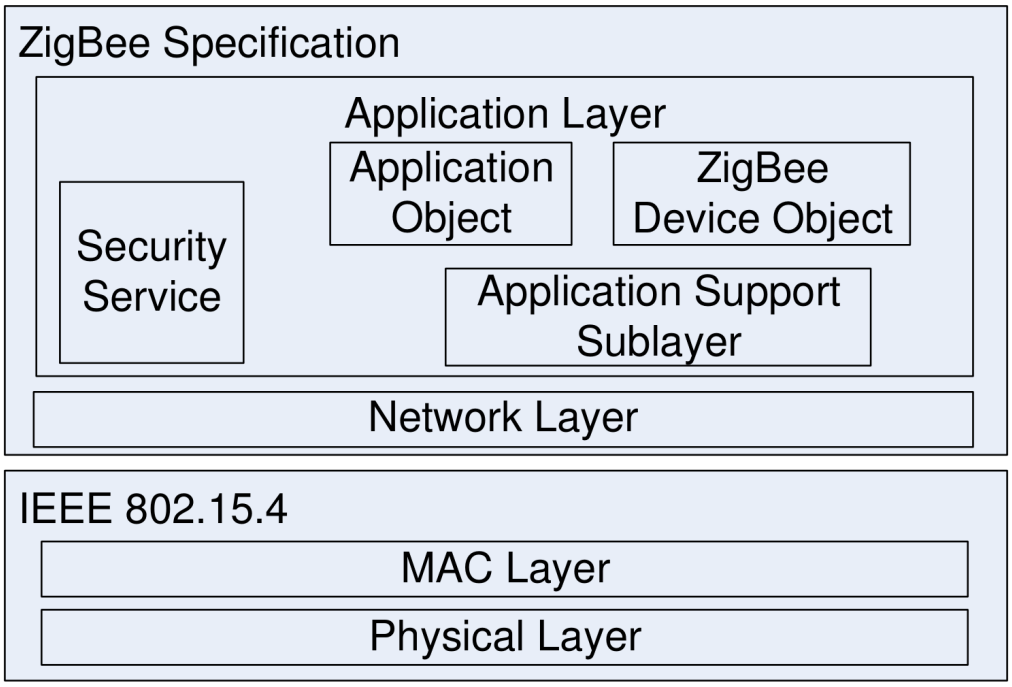

Figure 3.2: ZigBee Protocol Stack

ZigBee devices have three different type: ZigBee coordinator (ZC), ZigBee router (ZR) and

ZigBee end device (ZED). The coordinator is the key component of ZigBee network. Every ZigBee network can only have one coordinator that is used to initial and start ZigBee network. Besides, it can allow other device join its network and store information of the network. The ZR can allow ZED join the network and pass data from one device to other devices as an intermediate router. The ZED can just contact with its parent node. Usually, the ZED works in sleep mode so that it can make a long battery life [12].

The security service is one of the defining features in ZigBee Specification. It builds on the basic security framework of IEEE 802.15.4 and provides facilities including cyphering frames and controlling devices, protecting establishment and transport of cryptographic for secure communication. The security service is based on the correct management of symmetric keys and the correct implementation of methods and security policies.

ZigBee uses 128-bit keys to implement its security mechanisms to ensure confidentiality of the communication. In the ZigBee security service, it could establish keys for different usage based on a master key. Hence, the master key must be obtained through a secure medium such as pre-installation, bacause of that the whole network security depends on it. Besides, there must be one special device called trust center distributing security keys to other devices in ZigBee network.

3.1.2 Hardware System Platfrom

To implement a practical evaluation platform of our proposed Smart Home architecture, we use three kinds of PCB boards purchased from semiconductor companies. They are TI's OMAP35x EVM, CC2430 DB and MICAz Mote. Following are basic informations of these board.

3.1.2.1 TI's OMAP35x Evaluation Board

The OMAP35x is the 3rd generation OMAP, which developed by TI is a category of proprietary system on chips (SOC) for portable and mobile multimedia applications. Figure 3.3 is the picture of OMAP35x EVM. This OMAP35x EVM system is based on TI's OMAP3530 applications processor. This processor includes a high-performance Super scalar ARM® Cortex^{TM}-A8 with

NEON co-processing. NEON is a single instruction multiple data (SIMD) accelerator processor integrated in as part of the ARM® Cortex^{TM}-A8 [13]. It means that during the execution of one instruction the same operation will occur on up to 16 data sets in parallel. Within the help of powerful OMAP3530 processor, this EVM enough to run significant operating system such as Linux so that our implementation can design based on a mature platform. Besides, this high-performance application processor is able to run complexity encryption method that may required in our authentication and control algorithm.

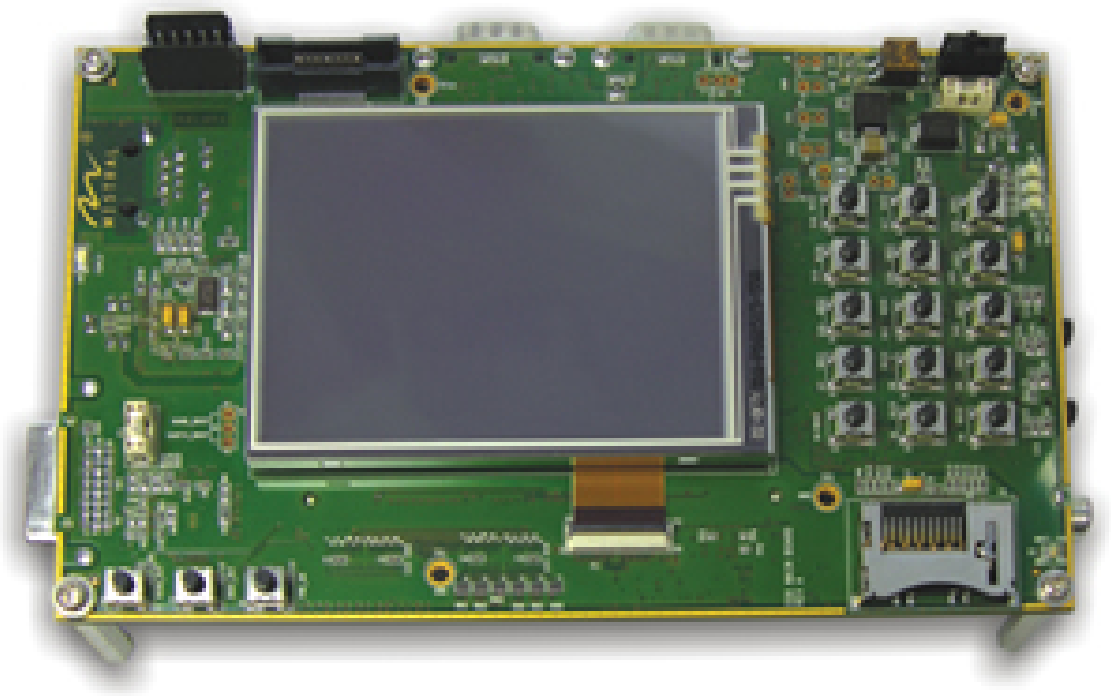

Figure 3.3: OMAP35x EVM

The OMAP35x EVM consists of three major parts:

- ***EVM Main Board*** is the largest board and is where the OMAP Processor Module and Power Module plug into. It contains all of the I/O and connectors for the system such as UART Interface, I^2C Interface, Audio and Video Interface, Ethernet, SD/MMC Interface. Besides, it includes 11 status LEDs, 2 user DIP switches, 14 pin JTAG and ETM debug interface. Moreover, it equipped with a 3.7" TFT LCD panel connected to the DSS interface of the

processor.

- ***OMAP Processor Module*** consists of OAMP3530 Processor with a Micron memory via the Package-On-Package (POP) technology. It supports 2Gbit NAND flash and1 Gbit mobile DDR SDRAM. This POP memory technology offers several benefits. The obious one is motherboard apce saving. Electrically, by minimizing track length between controller and memory, it provide better electrical performance since shortor interconnection between circuits yields faster signal propagation and reduced noise.

- ***Power Module*** takes care of the generation and distribution of various power requirements of the Main Board and Processor Module. The board may be powered by an external 5V power supply or from an external Lithium-Ion battery supply. It can provide several voltage level for different use. For example, +1.2V is for CPU core usage; +1.8V is for peripherals and DDR memory usage.

This board supports three UART (Uart 1, 2 and 3) interfaces via two RS-232 serial port. UART is a type of "asynchronous receiver/transmitter" used for serial communications over a computer or peripheral device serial port. This serial port provide a solution for us to connect OMAP35x EVM with other board to work together. The I^2C Interface provide similar function The 10/100 Mbps Ethernet interface on EVM Main Board using an external MAC/PHY controller LAN 9115 interfaced to the OMAP processor via GPMC interface. It provide Internet access solution for our system. SD/MMC Interface provide the function that the system can boot from SD card or store any information in SD card.

3.1.2.2 CC2430 Development Board

The CC2430 DB is based on CC2430—A true System-on-Chip (SOC) solution specificaly tailored for 2.4 GHz IEEE 802.15.4 and Zigbee® applications. Figure 3.4 is the picture of CC2430 DB. It is highly suited for our proposed system which require a low power consumption. Because, the CC2430 is ensured by various operating modes such as low-power mode or active mode. And

the very fast transition times from low power mode to active mode not only enable the system response rapidly, but also ensure a low power consumption. This demonstration board includes a low power 2.4 GHz IEEE 802.15.4 compliant RF transceiver, a high performance and low power 8051 microcontroller and several peripherals [14].

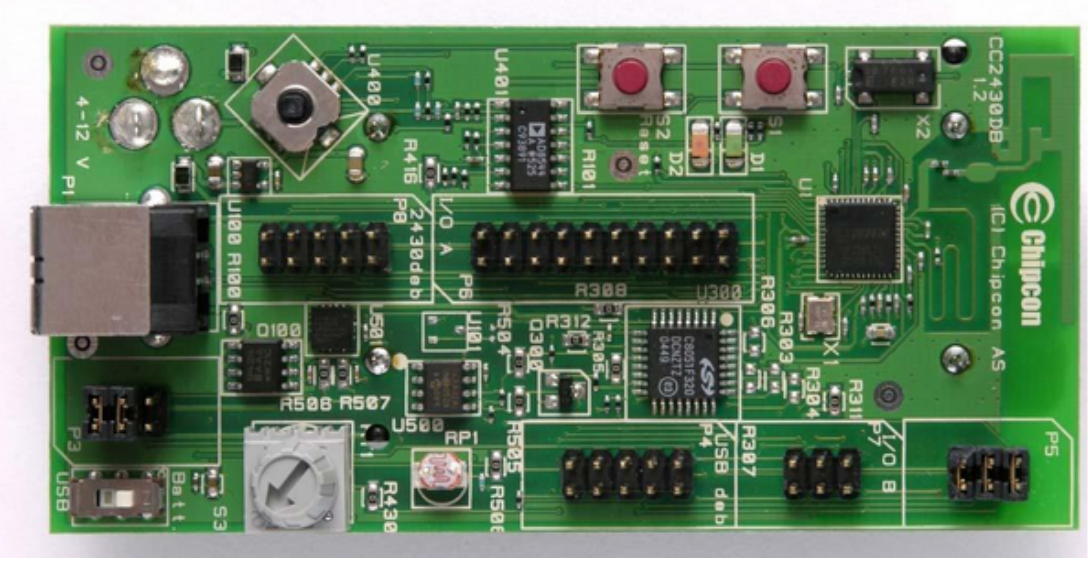

Figure 3.4: CC2430 DB

- ***Low power 2.4 GHz IEEE 802.15.4 compliant RF transceiver*** with excellent receiver sensitivity and robustness to interferers. It seperate transmit and receive FIFOs. Besides, it need very few external components, which is only a reference crystal. It support 250 Kbps data rate and O-QPSK modulation method.

- ***High performance and low power 8051 microcontroller core*** with 128 KB in-system programmable flash. It provide a USB interface on CC2430 DB. This interface is used to power the board, download firmware from computer and debug this board.

- ***Peripherals*** include two powerful UART, twenty-one general purpose I/O (GPIO) interface, AES security coprocessor and CSMA/CA hardware support. The UART serial port and GPIO are used to connect CC2430 DB with other board. The AES coprocessor and

CSMA/CA hardware support can improvment the performance of the board much better than software implementation.

3.1.2.3 MICAz Mote

MICAz is a wireless sensor mote from Crossbow technology. It is composed of the ATmega128L microcontroller and the CC2420 radio chip, which is the same radio chip consisted by CC2430 DB [15]. As it use same radio chip with CC2430 DB, all the RF features supported by CC2430 DB included in MICAz sensor mote. The difference between this two PCB is that the MICAz has less peripheral than CC2430 DB. Because it is design for indoor building monitoring and security, it only have expansion connector for plugin different sensors such as light, temperature, acoustic, etc. Figure 3.5 shows a picture of MICAz mote.

3.2 Secure Access Gateway Design

According to the description of the SAG, it is actually an interface between C-Mobile devices and Smart Home Managed Devices. As a result, it should capable of providing two different network solutions for forwarding data package between the external network and the internal network. Besides, it also should be able to provide secure authentication and access control. Hence, we design our SAG architecture that shows in Figure 3.6.

There are three major functional modules in the architecture: the application module, the external network module and the internal network module.

- **The application module** contains high-level program to manage and require service from low-level functional module (e.g. the external network module and the internal module) through relevent APIs. By calling service provided by basic functional module, it can logically forward data packages between C-Mobile device and the Smart Home Managed Devices, authenticate the authorized C-Mobile devices, etc.

Figure 3.5: MICAz Mote

- **The external network module** contains the protocol and firmware, which are both used to provide the Internet solution. It provides communication service to transfer packet between the SAG and the C-Mobile devices upon the Internet platform. It also includes a really important module called the security service module. Since the security of Internet is not enough to achieve our aim, we implement the security service module for secure authentication and access control upon the Internet platform.

- **The internal network module** contains all the protocol and firmware that needed for ZigBee wireless network communication. As we do not need special authentication and access control scheme in ZigBee, the original ZigBee security service is enough.

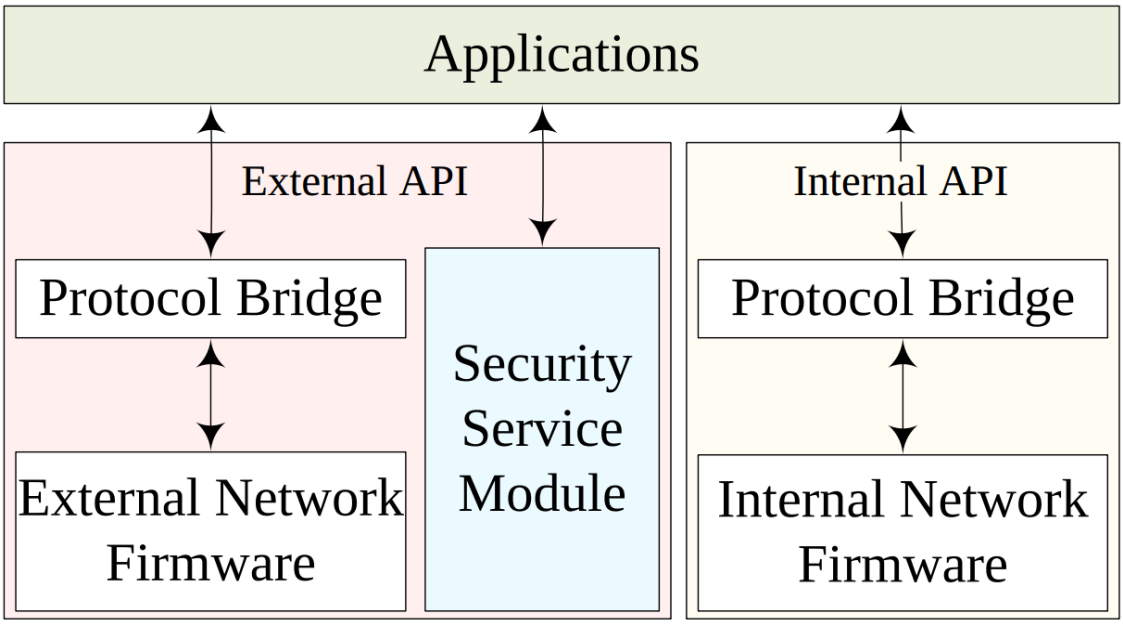

Figure 3.6: Secure Access Gateway Software Architecture

3.2.1 SAG Functions Implementation

The implementation of SAG functions can be considered as two steps: the establishment of communication and the secure algorithm implementation. To establish the Internet communication between SAG and C-Mobile devices, we implement the socket programming based on client-server model. In the following, we will first introduce our implementation of socket programming. Then we will introduce the establishment of internal ZigBee network and the secure algorithm implementation.

3.2.1.1 Client-Server Model Socket Programming

Client-Server model is a computing model that acts as distributed application which partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients [16]. A server is a host that running server program to share resource or function with one or many clients. The client always initials the communication by sending request service for such server.

There are lots of applications based on this model. For example, in the email system, every user can be seen as a client. The mail servers received the email sent from one client, forwarding it to another client. In the web access application, each browser is a client, and the web servers provide web content to each client that are accessing their web.

To implement this model into our system, we consider the SAG as the server and each C-Mobile remote terminal as a client. The resource provided by the SAG is an interface or function that used to manage the Smart Home Devices. The communication always initialed by the C-Mobile device that want to exchange data with Smart Home Device.

Based on the Internet platform and client-server model, our software package of establishing external communication follows the underlying process: Both the SAG and the C-Mobile devices will be assigned an IP address. The SAG always run a program to wait for the connection request. Everytime a mobile device want to communicate with the Smart Home appliance, it will initial a service request sending to the IP address of the SAG. After the SAG accept the request, the external communication established. However, since we are going to establish a secure end-to-end communication, we do not willing every mobile device can establish the connection to communicate with Smart Home appliances, but only the authenticated user such as the home members. As we described before,we design a security service module integrated in the external network module to provide secure authentication and access control for Internet. It can be seen as an door of the SAG. To implement this module, we integrate a software package called Plugable Authentication Module (PAM) into the SAG system.

3.2.1.2 Pluggable Authentication Module Design

The PAM is a mechanism to integrate multiple low-level authentication schemes into a high-level Application Programming Interface (API) [18]. It is a suite of shared libraries that provide dynamic authorization for applications and services in a computer system and enable

the local system administrator to choose how applications authenticate users. By providing a library of functions that an application may use to request that a user be authenticated, PAM help developer seperating the development of privilege granting software from the development of secure and appropriate authentication algorithm. Here is a Figure 3.7 that shows the overall organization of Linux-PAM, which is one of the PAM supported for Linux Operating System.

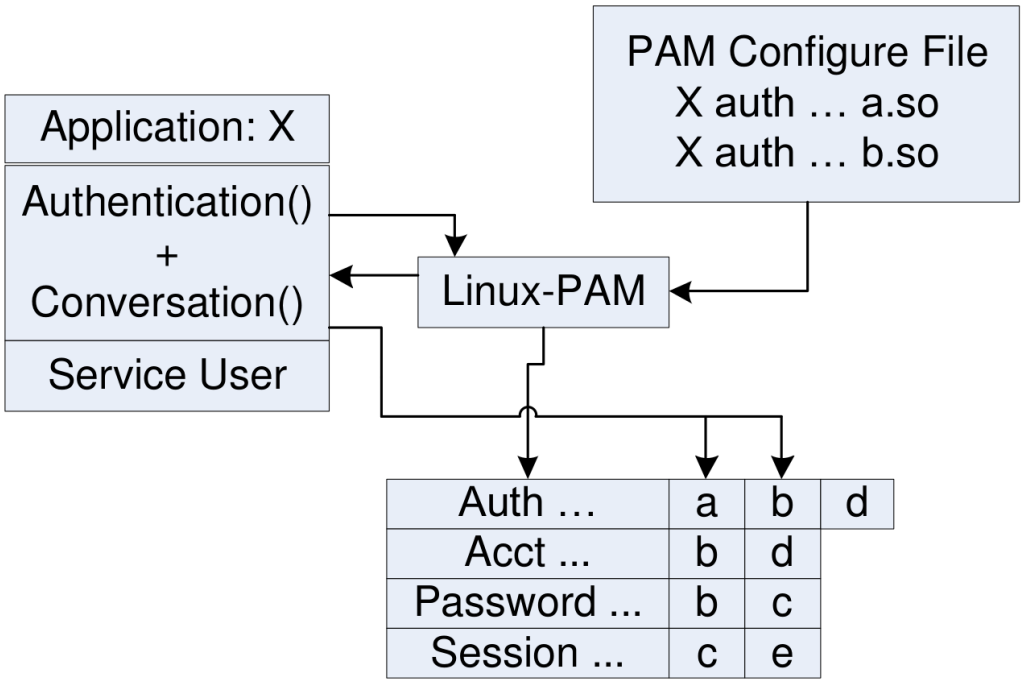

Figure 3.7: Linux-PAM Overall Organization

The PAM normally has four basic management tasks: authentication management, account management, session management and password management, which are showed in the Figure 3.7. The management functions are performed by modules specified in the configuration file called PAM config file in the upper-right of the figure. There must be a conversation function in the privilige granting application such as application X in the left of figure. The conversation function is provide a interface between the application X and the PAM library . When the application authenticate users, the application X is able to call the PAM library in

the center through the conversation function. Then the library will read the configuration file and load the modules specified by the configuration file to perform the authentication task.

From the PAM structure, we can conclude that the core authentication algorithm is specified by different module in the PAM. Hence, we decide to design our own PAM module based on the authentication scheme we described in Section 2.2. Then we use the interface provided by PAM call that module to achieve the aim of secure authentication and access control. The module we create is called PAM-OTP module. Before we describe the PAM-OTP module, we will first introduce three algorithms implemented in the module.

- ***Linear Feedback Shift Register (LFSR)*** is a shift register whose input bits is a linear function of its previous state. All the outputs of the LFSR are determined by the linear function and the initial value of the LFSR which is called the seed. The sequence of output values will enter a repeating cycle because that the register has a finite number of possible states. But, with a well-chosen of feedback function, the LFSR can produce a sequence of bits which seems like random and which have the very long cycle. Normally, the LFSR is used to generate pseudo-random numbers, pseudo-noise sequence or fast digital counters.
- ***Advanced Encryption Standard (AES)*** is a specification that define data encryption method using symmetric-key algorithm. The symmetric-key algorithm means that there is only one key used for both encryption and decryption processes. The principle of design AES is based on substitution-permutation network which is a series of linked mathematical operation used in block cipher algorithms. Normally, AES has a fixed 128-bit block size and a key size of 128, 192, or 256 bits.
- ***MD5 Message-Digest Algorithm (MD5SUM)*** is a widely used cryptographic hash function which is able to produces a 128-bit hash value. With this hash algorithm, theoritically there is no same hash value generated from different files. Hence, the MD5 usually is used to check data integrity which means that the data has not been

modified.

As we described before, the LFSR is used to generate the pseudo-random numbers. The primitive polynomial we implemented in the LFSR is

$$\begin{aligned} &x^{42}+x^{35}+x^{33}+x^{31}+x^{27}+x^{26}+x^{25}+x^{22}+x^{21}+x^{19} \\ &+x^{18}+x^{17}+x^{16}+x^{10}+x^{7}+x^{6}+x^{5}+x^{3}+x^{2}+x+1 \end{aligned} \tag{3.1}$$

Therefore, the period of the LFSR is $2^{42}-1$ which is a really large number to make sure the pseudo-random number would not repeat for a long time. After send each pseudo-random number to the AES, we get the one time password. The predetermined shared secret k which is used to encript the pseudo-random number can be the password defined by the authorized user. The MD5SUM is used to compute the dynamic login name. The intial ID was also defined by the authorized user.

Besides, we create an users' profile in the SAG. Everytime the PAM module was called, it will compare the login name and password sent by the C-Mobile device with the login name and password listed in the profile stored in the SAG. After every successful authentication, the PAM module will update the login name the password to ensure the one time password and dynamic login name scheme. By adding more elements in the profile, we can implement more function we desicribed before. For example, we set a number to represent the failure authentication times for each user so that if this number larger than the maximum failure times, we will directly deny the rest access requirement without check the login name and password. Besides, since our system use one time password and dynamic login name authenctication scheme, each login name and password can only be send once by the C-Mobile for the authentication process no matter the authentication result is what. Suppose there is any reason (e.g. bad network performance or denial-of-service attack to the SAG) result in that the SAG does not receive login name and password send by the authencticated C-Mobile device, it won't response any message to the authenticated C-Mobile device. After waiting for an indentified peorid, the authenticated C-Mobile device will generated its new

login name and password based on previous value and sent it to the SAG again to requist accessing the SAG. If we only check one login name on the file, this requist will be denied since both the password and login name will not match that listed on the file. As are result, to prevent this situation happen, we actually not only check the listed login name and password, but also their follow five login name and password.

3.2.1.3 Establishment of ZigBee Network Communication

The SAG is going to initialize, start and maintain the ZigBee home area network. The ZigBee network communication will follow the ZigBee specification. In our system design, the SAG is the ZC of our internal ZigBee network. All the other Smart Home appliance can be seen as ZRs and ZEDs. We will pre-installation the master key in every nodes in the internal network and setup ZC as our trust center to distribute keys. As a result, all the Smart Home appliances and monitors will only accept the communications originating from the key provided by SAG to avoid information leaks and other security risk, making sure a secure internal communication.

3.2.2 SAG Prototype Integration

It is hard to find one PCB that provide both Internet solution and ZigBee solution when we started our implementation work. As a result, we have to integrate the two PCBs together: the TI's OMAP35x EVM and the TI's CC2430 DB. One of them provide Internet solution and the other one provide ZigBee solution. The communication interface between OMAP35x EVM and CC2430 DB is the UART serial port. The reason why we use UART is based on transfer data rate requirement of our proposed Smart Home architecture. Normally, the types of data package transmitted between these two PCBs are command or small information indicating the usage of Smart Home Managed Device, which means that low transfer data rate is enough for our system.

Because the output voltage levels of UART port on the OMAP35x EVM is 1.8V, which is different from 3.3V on the CC2430 DB. We design a simple PCB for the purpose to shift voltage-level between these two UART ports. Figure 3.8 shows the picture of our SAG prototype. The board located in the middle of OMA35x EVM and CC2430 DB is the voltage-level convert PCB board we design.

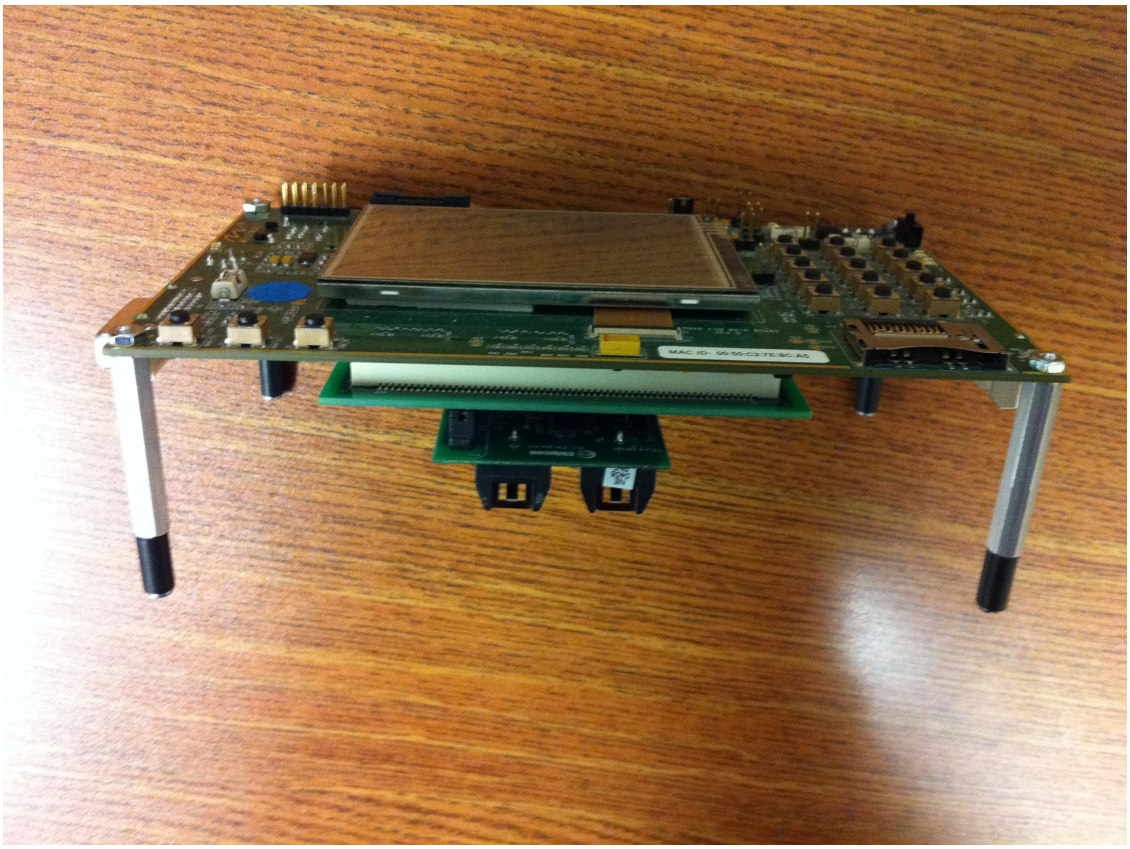

Figure 3.8: SAG Hardware Prototype

3.3 Smart Home Managed Device Implementation

Based on our proposed Smart Home Architecture, the Smart Home Managed Device can be any type of home appliances, monitors or smart meter. In our concept framework, we use sensor node with ZigBee solution to replace the truly home appliance. These sensor nodes can be fully functional development board such as CC2430 DB, but also can be simple sensor

board such as MICAz. In the following, we will introduce the functions of the Smart Home Managed Devices.

Both CC2430 DB and MICAz will be start as ZED components. After that, they will scan the nearby ZigBee network and apply to join it. The basic function that they both have is the LED function, which is used to test the connectivity between the C-Mobile devices and the Smart Home Managed Devices. The LED statue will change based on the command it received from C-Mobile. Moreover, we implement a function of reporting an alert to the C-Mobile devices. This function is used to prove the the concept of two-way communication between the C-Mobile and Smart Home Managed Devices

3.4 C-Mobile Remote Control

In this section, we will introduce the C-Mobile devices and the Android apps we developed for the Android smart phone. The Figure 3.9 shows the screenshot of the apps.

The apps development is also based on client-server model socket programming. However, we implement client side on the smart phone so that everytime the C-Mobile will initialize the communication and require access service. It is able to control the Smart Home Managed Deivces if it is authenticated by the SAG. We also create a user profile for each client side. This user profile will provides the login name and password only for the authorized user who owned this smart phone. It is different from the file stores in SAG, which includes all the login name and password of every authorized user. The apps have another function which is used to proof the two way communication concept. It will notify the user when it received an alarm from Smart Home Managed Devices.

Figure 3.9: Screenshot of Remote Terminal

Chapter 4

CONCLUSIONS

Reliable and efficient communication between human being and devices play a key role for Smart Grid and Smart Home. In this paper, we provide a design of a secure access gateway (SAG) for home area network. The SAG serves as the interface between the remote users and the managed devices, such that real-time secure monitoring and control to the devices can be achieved through a Smart Phone. The major challenges for the design and deployment of the SAG lie in the ever-increasing demand on security and capacity. We enhance the security from both the network layer and the physical layer. At the network layer, we implement a varieties of security services, including secure one-time password (OTP) authentication, fine access control, event logging alarm, and dynamic login names. At the physical layer, we build inherently secure wireless system by integrating advanced cryptographic techniques into transmitter design. We also provide a detailed framework on how to improve the system capacity through cognitive network spectrum sharing. Potentially, secure monitoring and control of home devices through wireless communications will gradually penetrate into the world surrounding us and bring great changes to our daily life style.

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] The Smart Grid: What is the Smart Grid. http://www.smartgrid.gov/the_smart_grid#smart_grid.

[2] The Smart Grid: An introduction. http://www.oe.energy.gov/SmartGridIntroduction.htm.

[3] Simmons. Mobile tips and tricks. http://www.mobiletipstricks.com/home-control-centre/.

[4] J. Massey. Shift-Register Synthesis and BCH Decoding. *IEEE Transactions on Information Theory*, 15:122–127, January 1969.

[5] National Bureau of Standards. FIPS Publication 197: Advanced Encryption Standard (AES). http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf, March 2002.

[6] L. Lightfoot, L. Zhang, J. Ren, and T. Li. Secure collision-free frequency hopping for ofdma based wireless networks. *EURASIP Journal on Advances in Signal Processing*, 2009(Article ID 361063), 2009.

[7] V. Tarokh, H. Jafarkhani, and A.R. Calderbank. Space-time block code from orthogonal designs. *IEEE Trans. Information Theory*, July 1999.

[8] S. Haykin. Cognitive radio: brain-empowered wireless communications. *IEEE Journal on Selected Areas in Communications*, 23(2):201–220, February 2005.

[9] Huahui Wang, Jian Ren, and Tongtong Li. Resource allocation with load balancing for cognitive radio networks. In *GLOBECOM 2010, 2010 IEEE Global Telecommunications Conference*, pages 1–5, Dec 2010.

[10] Internet from Wikipedia. http://en.wikipedia.org/wiki/Internet

[11] ZigBee from Wikipedia. http://en.wikipedia.org/wiki/ZigBee

[12] ZigBee Alliance *ZigBee Specification*, Jan 2008

[13] Mistral Solutions Pvt. Ltd *OMAP35x Evaluation Module Hardware User Guide*, Rev. 1.2 May 2008

[14] Chipcon Products from Texas Instruments *CC2430 Data Sheet*, Rev. 2.1

[15] Crossbow *MICAz wireless measurement system* , Rev. A

[16] Client-Server model from Wikipedia http://en.wikipedia.org/wiki/Client-server_model

[17] Brian Hall *Beej's Guide to Network Programming Using Internet Sockets*, Jorgensen Publishing, October 2011

[18] Andrew G. Morgan, Thorsten Kukuk *The Linux-PAM System Administrators' Guide* Version 0.99.7.0, January 2007

[19] Kraig Mitzner *Complete PCB Design Using OrCAD Capture and PCB Editor* Elsevier Inc, 2009, ISBN 978-0-7506-8971-7

[20] Android Developers from Google http://developer.android.com/index.html