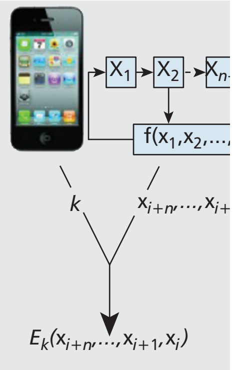
RECENT ADVANCES IN
WIRELESS TECHNOLOGIES FOR SMART GRID

SECURE WIRELESS MONITORING AND CONTROL SYSTEMS FOR SMART GRID AND SMART HOME

TONGTONG LI, JIAN REN, AND XIAOCHEN TANG, MICHIGAN STATE UNIVERSITY



Secure and efficient communication between human being and managed devices is critical for Smart Grid and Smart Home. This article considers the architecture and design of a secure access gateway (SAG) for home area networks.

ABSTRACT

Secure and efficient communication between human being and managed devices is critical for Smart Grid and Smart Home. This article 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 using dynamic resource management. Remote monitoring and control of home/office devices through a Smart Phone is coming closer to us more than ever before.

INTRODUCTION

FROM SMART GRID TO SMART HOME

Smart Grid [1] has been characterized as an integrated system that can increase the efficiency, reliability and flexibility of the electricity network through a two-way flow of electricity and information. The main point is to resolve the peak problem by enabling real-time communications between the customer and the utility, and to increase power network resilience through the integration of renewable energy sources. As the customers choose to tailor their energy consumptions in responding to price or environmental concerns, the peak load burden will be reduced, and hence Smart Grid can meet increased customer demand without adding expensive infrastructure. At the same time, integration of the renewable energy sources will increase the power diversity, and reduce our dependence on fossil fuel as well as the greenhouse gases.

As indicated by the DOE, real-time two-way communications and device control lie in the core part of Smart Grid. Considering the user mobility and freedom, it is therefore highly desired to monitor and control the home devices through the wireless networks. This overlaps with the idea of Smart Home [2], where all the home appliances are connected to smart mobile devices. The underlying framework here is: a real-time, secure wireless communication interface between the human being and the monitored/controlled devices.

COMMUNICATION BETWEEN HUMAN BEING AND DEVICES

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:

- 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
- 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, in this article, 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.

MAJOR CHALLENGES

In this article, we discuss the design of a reconfigurable framework for mobile-based device monitoring and control, which can be applied in both fixed or moving LAN scenarios, such as

1536-1284/12/$25.00 © 2012 IEEE

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.

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 can be 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:

- How to design efficient but effective security solutions tailored for mobile-based device monitoring and control in unprotected wireless environments?
- How to track user accountability while preserving privacy protection?

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?

Demand on Secure and Efficient Resource Management — 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 networks. 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:

- Traffic collisions between the PU and the SU, or among SUs, leading to low efficiency and reliability
- Mobile-controlled spectrum sensing enables the SU to perform legitimate traffic analysis of the PU, leading to a security compromise of the PU
- 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 security drawbacks, traffic collisions 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

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 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.

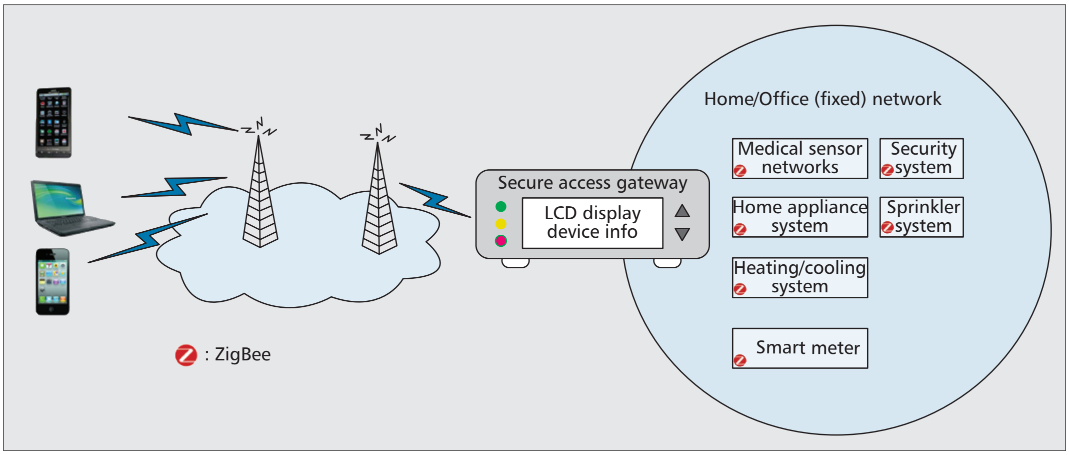


Figure 1. *Proposed system architecture.*

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.

Proposed System Architecture

In this article, the proposed architecture for the mobile-based monitoring and control system is shown in Fig 1. 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, especially home devices for Smart Grid. We will briefly describe each component below.

- 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 Grid/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 Grid/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 Grid/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.

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.

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 $f(x_1, x_2, \ldots, x_n)$, as shown in Fig. 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, the period of the sequence has to be sufficiently long, which can be guaranteed by selecting the feedback polynomial $f(x_1, x_2, \ldots, x_n)$ 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 [3] 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

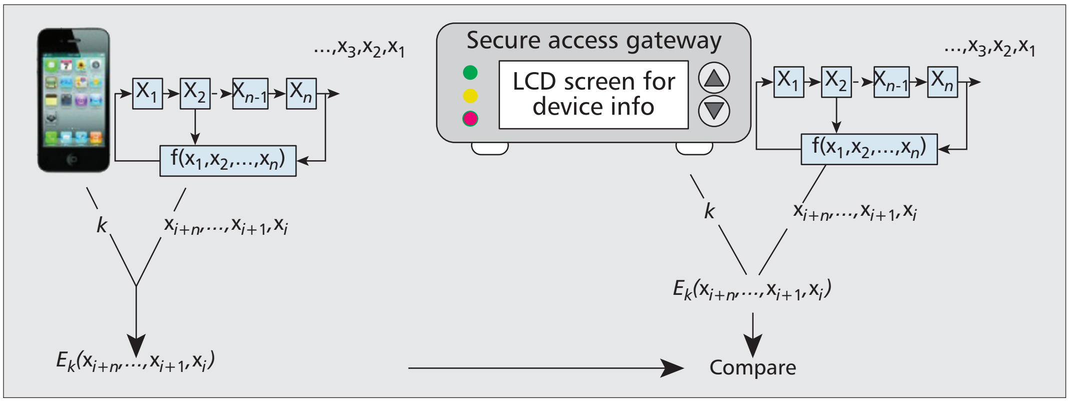


Figure 2. *Proposed OTP secure access authentication.*

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.

length. We then use a symmetric cipher (such as the Advanced Encryption Standard (AES) [4]) 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 *i*th OTP_i is given by $OTP_i = E_k(C_i)$, 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 *i*th 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 devices 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), the resources that can be accessed, the operations allowed, and also the configurations that cannot be altered. It can also specify the remote access hours, including the days of the week and times of the day that the remote access is enabled/disabled.

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.

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 system parameter n with the SAG. Based on this shared secret, SAG and the terminal will generate an *ID-hash-chain*: $\{id_1, id_2, \ldots, id_n\}$, where $id_n = H(ID)$, $id_{n-1} = H(id_n)$, $\ldots$, $id_1 = H(id_2)$, and H is a one-way hash function.

The SAG access authentication will use id_i as its *i*th login name. Because H is a one-way hash function, the login names $id_1, id_2, \ldots, id_n$ form a reverse hash-chain. It is computationally infeasible to compute id_{i+1} from id_i. The dynamic login names can prevent the identities from being predetermined, reused and also 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 and dynamic login names will be exe-

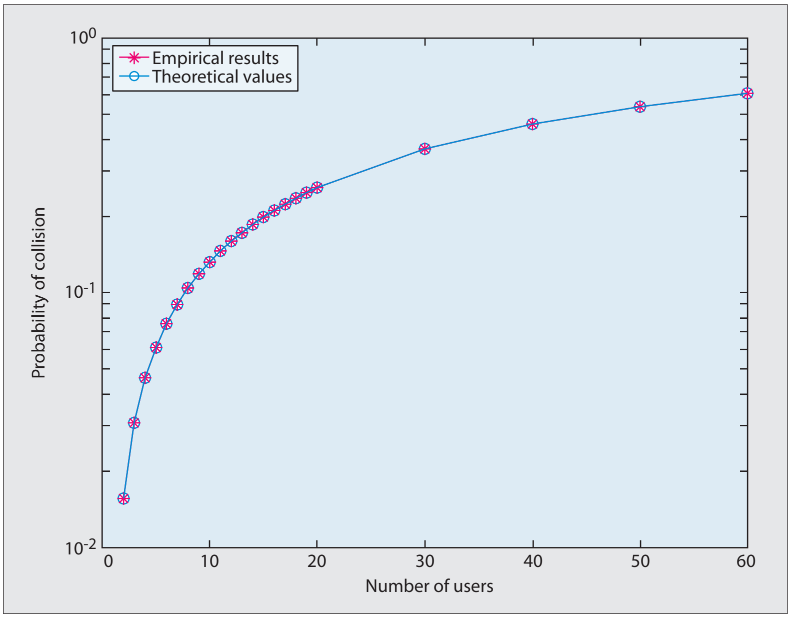


Figure 3. *Collision effect in an FH system with 64 channels.*

cuted through an automated process. The users do not need to remember the OTP and the dynamic login names, which makes the implementation feasible and practical.

Physical Layer Security

Why PHY 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. 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?

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 pseudorandom manner among available frequencies according 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 Fig. 3, the spectral efficiency of the conventional FH is very low due to the collision effects among different users.

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 [5]. The proposed secure subcarrier assignment is achieved through an AES-based secure permutation algorithm, which is designed to ensure that:

- Each user hops to a new set of subcarriers in a pseudo-random manner at the beginning of each hopping period
- Different users always transmit on non-overlapping sets of subcarriers
- 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.

The anti-jamming property of the OFDMA based CFFH can be further enhanced by incorporating space-time coding (STC) [6] (as shown in Fig. 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.

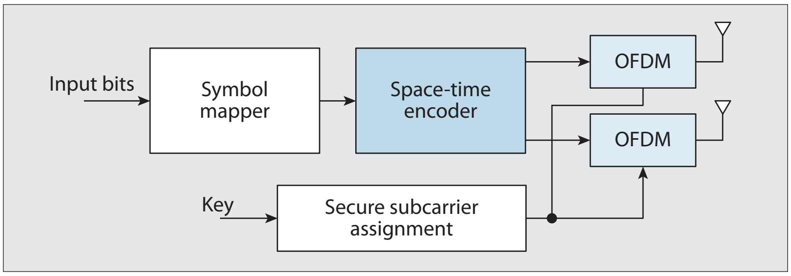


Figure 4. *STC-CFFH transmitter.*

Dynamic Resource Management

Cognitive Networking

Cognitive radio has been proposed as a promising technique to promote efficient wireless spectrum allocation [7]. 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).

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:

- Spectral inefficiency due to traffic collisions between the PU and SU, and among the SUs themselves
- Serious security fragility evoked by spectrum sensing and denial-of-service attacks launched by hostile SUs
- 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-

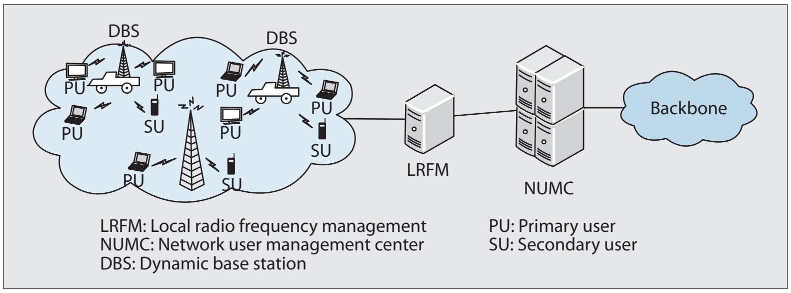

DBS
DBS
PU
PU
PU
PU
PU
PU
PU
SU
SU
SU
LRFM
NUMC
Backbone
LRFM: Local radio frequency management
NUMC: Network user management center
DBS: Dynamic base station
PU: Primary user
SU: Secondary user

Figure 5. *Architecture for cognitive networks.*

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 powerful software-defined radios (SDRs). We propose a novel architecture for cognitive network, as shown in Fig. 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.

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 B Hz, the channel capacity can be calculated as: $C = B \log_2 (1+ SNR)$ b/s, 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.

Conclusions

Reliable and efficient communication between human being and devices play a key role for Smart Grid and Smart Home. In this article, we discussed the 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. We also provide a framework on how to improve the system security, capacity, flexibility and scalability through cognitive networking. 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 lifestyle.

Acknowledgments

This research was supported in part by NSF grants CNS-0845812, CNS-1050326, CNS-1117831, and CNS-0746811.

References

[1] The Smart Grid: An Introduction, http://www.oe.energy.gov/SmartGridIntroduction.htm.

[2] Simmons, Mobile Tips and Tricks, http://www.mobiletipstricks.com/home-control-centre/.

[3] J. Massey, "Shift-Register Synthesis and BCH Decoding," *IEEE Trans. Info. Theory*, vol. 15, Jan. 1969, pp. 122–27.

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

[4] L. Lightfoot *et al.*, "Secure Collision-Free Frequency Hopping for OFDMA Based Wireless Networks," *EURASIP J. Advances in Sig. Proc.*, 2009 (Article ID 361063), 2009.

[5] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-Time Block Code from Orthogonal Designs," *IEEE Trans. Info. Theory*, July 1999.

[6] S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications," IEEE JSAC, vol. 23, no. 2, Feb. 2005, pp. 201–20.

Biographies

Tongtong Li [SM'08] (tongli@egr.msu.edu) received her Ph.D. degree in Electrical Engineering in 2000 from Auburn University. From 2000 to 2002, she was with Bell Labs, and had been working on the design and implementation of 3G and 4G systems. Since 2002, she has been with Michigan State University, where she is now an Associate Professor. Her research interests fall into the areas of statistical signal processing, wireless and wired communications, wireless security and infor-

mation theory. More recently, her research has been focused on time-varying jamming modeling and classification, and spectrally efficient and secure communications under malicious environments. She is a recipient of a National Science Foundation (NSF) CAREER Award (2008) for her research on efficient and reliable wireless communications. He served as an Associate Editor for IEEE Signal Processing Letters from 2007–2009, and as an Editorial Board Member for EURASIP Journal Wireless Communications and Networking from 2004–2011. Currently, she is an Associate Editor for IEEE Transactions on Signal Processing.

JIAN REN [M'98, SM'09] (renjian@egr.msu.edu) received his Ph.D. degree from the Xidian University in 1994. Currently, he is an Associate Professor in the Department of Electrical and Computer Engineering at Michigan State University. Prior to joining MSU, he was the Leading Secure Architect at Avaya Lab, Bell Lab and Racal Datacom in security architecture and solution development. His research interests include network security, wireless security, secure and energy efficient wireless sensor network protocols, cryptographic primitives, information forensics, network management, error-control coding and digital copyright protection. He received the National Science Foundation (NSF) CAREER award in 2009. Currently, he serves an as Editorial Board Member for Ad Hoc & Sensor Wireless Networks.

XIAOCHEN TANG (tangxia2@msu.edu) received his Bachelor degree from School of Information Science & Engineering, Southeast University in 2009. Currently he is pursuing his MS degree at Michigan State University in the department of ECE.