International Journal of Digital Multimedia Broadcasting

Communications and Networking for Smart Grid: Technology and Practice

Guest Editors: Chi Zhou, Hossam S. Hassanein, Robert Qiu, and Pierangela Samarati

Communications and Networking for Smart Grid: Technology and Practice

International Journal of
Digital Multimedia Broadcasting

Communications and Networking for Smart Grid: Technology and Practice

Guest Editors: Chi Zhou, Hossam S. Hassanein, Robert Qiu, and Pierangela Samarati

Editorial Board

Contents

Hindawi Publishing Corporation
International Journal of Digital Multimedia Broadcasting
Volume 2011, Article ID 617624, 2 pages
doi:10.1155/2011/617624

Editorial

Communications and Networking for Smart Grid: Technology and Practice

Chi Zhou,[1] Hossam S. Hassanein,[2] Robert Qiu,[3] and Pierangela Samarati[4]

[1] *Department of Electrical and Computer Engineering, Llinois Institute of Technology, 3301 S. Dearborn Street, Chicago, IL 60616, USA*
[2] *School of Computing, Queens's University, Kingston, ON, Canada K7L 3N6*
[3] *Department of Electrical and Computer Engineering, Tennessee Tech University, Campus Box 5077, Cookeville, TN 38505, USA*
[4] *Department of Information Technology, University of Milan, Via Bramante 65, 26013 Crema, Italy*

Correspondence should be addressed to Chi Zhou, zhou@iit.edu

Received 18 December 2011; Accepted 18 December 2011

The drive for improved power system efficiency, stability, and flexibility has served as a catalyst for smart grid research and development, so the communications networks in smart grid must facilitate the wide-scale utilization of various communications systems, enable the interoperability among various communications protocols, and provide secure and reliable communications for the smart grid. Many open issues in communications and networking need to be addressed by researchers.

The major interesting topics investigated in this special issue include home area networking (ZigBee, OpenHAN, etc.), wireless mesh networking, and neighborhood area networks, protocol interoperability, green routing and switching protocols, and cyber and physical security and privacy. Many thanks to the authors for submitting high-quality papers as well as to guest editors and reviewers for providing the timely reviews. A summary of papers is as follows.

"*M2M communications in the smart grid: applications, standards, enabling technologies, and research challenges,*" by S. K. Tan et al., presents some of the ongoing standardization work in machine-to-machine (M2M) communications followed by the application of M2M communications to smart grid. The paper analyzes and discusses the enabling technologies in M2M and provides an overview of the communications challenges and research opportunities with a focus on wireless sensor networks and their applications in a smart grid environment.

"*Location discovery based on fuzzy geometry in passive sensor networks,*" by R. W. et al., provides a solution to location discovery with uncertainty for passive sensor networks in the nation power grid. The approach of fuzzy geometry is introduced to investigate the fuzzy measurability. The interplay between fuzzy geometry of target localization and the fuzzy estimation bias for the case of fuzzy linear observer trajectory is analyzed in detail in sensor networks.

"*Building automation networks for smart grids,*" by P. Yi et al., presents a framework for end-to-end interoperability in home and building area networks within smart grids. 6LoWPAN and the compact application protocol are utilized for network and application layer interoperability, respectively. A differential service medium access control scheme enables end-to-end connectivity. Several issues are also addressed, including interference mitigation, load scheduling, and security and possible solutions.

"*Expected transmission energy route metric for wireless mesh senor networks,*" by Y. L. Jin et al., considers wireless mesh sensor networks for smart grid application, as mesh topology achieves high throughput and stable intercommunication. A new routing metric is designed to improve the energy balance of the whole network and extends the lifetime of wireless mesh sensor networks.

"*Cyber security for smart grid, cryptography, and privacy,*" by S. Iyer, reviews different types of attacks to smart grid. The specific focus is on cyber security, as the smart grid uses high level of computation. It is shown that cryptography and key management techniques can be used to overcome these attacks. The paper also discusses the privacy of consumers as another important security concern.

"*BVS: a lightweight forward and backward secure scheme for PMU communications in smart grid,*" by W. Ren et al., proposes a family of security schemes that are lightweight in terms of computation and storage for phasor measurement units (PMUs), including billed value-based scheme (BVS). Security analysis justifies that the proposed schemes, especially BVS, can attain the security goals with low computation and storage cost.

"*Cognitive radio for smart grid: theory, algorithms, and security,*" by R. Ranganathan et al., introduces a novel concept of incorporating a cognitive radio network as the communications infrastructure for the smart grid. From the power system point of view, a supervised learning method is used for the automated classification of power system disturbances. The impending problem of securing the smart grid is also addressed, in addition to the possibility of applying FPGA-based fuzzy logic intrusion detection for the smart grid.

Chi Zhou
Hossam S. Hassanein
Robert Qiu
Pierangela Samarati

Hindawi Publishing Corporation
International Journal of Digital Multimedia Broadcasting
Volume 2011, Article ID 372020, 8 pages
doi:10.1155/2011/372020

Review Article

Cyber Security for Smart Grid, Cryptography, and Privacy

Swapna Iyer

Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL 60616-3793, USA

Correspondence should be addressed to Swapna Iyer, siyer9@iit.edu

Received 1 December 2010; Revised 21 June 2011; Accepted 26 July 2011

Academic Editor: Pierangela Samarati

The invention of "smart grid" promises to improve the efficiency and reliability of the power system. As smart grid is turning out to be one of the most promising technologies, its security concerns are becoming more crucial. The grid is susceptible to different types of attacks. This paper will focus on these threats and risks especially relating to cyber security. Cyber security is a vital topic, since the smart grid uses high level of computation like the IT. We will also see cryptography and key management techniques that are required to overcome these attacks. Privacy of consumers is another important security concern that this paper will deal with.

1. Introduction

One of the most important, complex, and intelligent network we have is the "power system". This system consists of circuits, wires, towers, transformers, sensors, and cables interlinked to provide us with uninterrupted power supply. This system is mainly a mechanical system and has very little electronics associated with it like sensors and communication. However, as technology has progressed rapidly and almost all the latest devices need electricity for their operation, it is necessary that we make our present power system more reliable and efficient [1].

We can say the demand for electricity is greater than its supply. The demand is not only high but also fluctuating. We could rely on renewable resources like solar energy and wind energy to meet the present need, but unfortunately, they turn out to be fluctuating too.

The smart grid enhances the functionality of the power delivery system. This is possible because smart grid uses sensors, communications, computation, and control in order to make the system smart and by applying intelligence to it in the form of control through feedback or in other words by using two way communication. In order to utilize the available resources, consumers need to change, and they need to act more "smart". They have to change from being passive consumers to being active consumers [1]. Smart grids aim to reduce the energy consumption, ensure reliability of power supply, reduce carbon foot print, and minimize the costs associated with power consumption.

The smart grid system has many advantages, one of them being cost effectiveness. This is because the grid uses internet for communication purpose. However, using the internet means vulnerability to cyber attacks. As opposed to the original power system, the smart grid uses ethernet, TCP/IP and other operating systems, thus making the grid more susceptible to attacks. The smart grid should enhance the security of the power system, but protecting the grid is a more challenging task now. Once the system is attacked, the attacker may control several meters or disrupt the load balance of the system. Thus, we need to gain complete knowledge about cyber security, so we can eliminate it completely. We also need to focus on the cryptographic methods proposed by the National Institute of Standards and Technology (NIST) in order to avoid these cyber attacks.

In this paper, we will study smart grid security in more depth. The goal of this paper is to cover the security challenges related to cyber security, and we will also study how cryptography is used in order to eliminate cyber attacks. Finally, we will also discuss in brief privacy which is another smart grid security concern. The rest of the paper is organized as follows. We start by reviewing the challenges and goals of smart grid in Section 2. This is followed by the smart grid architecture in Section 3. We focus on cyber security in Section 4. Section 5 explains cryptography used for smart grid security in depth. Privacy in context with smart grid security is explained in Section 6. And finally, we conclude in Section 7.

2. The Smart Grid: Goals and Challenges

2.1. Goals. The present power grid has more than 9200 electric generating units, 1,000,000 plus megawatts of generating capacity connected by using 300,000 miles of transmission lines [2].

Electricity has one basic requirement; it needs to be utilized as soon as it is generated. The present grid does so successfully. However, now, the grid is overburdened. The reliability of the present grid is at stake, and this can be seen, since we have been witnessing more brownouts and blackouts recently.

Another thing that needs to be addressed when we consider the present grid is the efficiency. By making the grid more efficient, we can save millions of dollars. There is also a reverse case here; if there is an hour of power outage, the nation loses a tremendous amount of money. Electricity needs to be more affordable too. The rate of electricity is increasing gradually which makes it less affordable.

Majority of the electricity produced in the United States of America comes by burning coal. The carbon footprints that occur due to this contributes to global warming. If we introduce the use of renewable energy in our grid, we can reduce the carbon footprint.

We also need to compete globally with other countries that have better technology for energy distribution.

And finally, the grids security is of major concern. The current grid has a centralized architecture, and thus making it more vulnerable to attacks. A failure can hamper the country's banking, traffic, communication, and security system [2].

Thus, we introduce the smart grid system (Figure 1). We now have a smart power grid that creates a link between electricity, communications, and computer control. Many countries are actively participating in the development of smart grid; for example, the ETP created a joint vision for the European network of 2020 [3] and beyond, and the US established a federal smart grid task force under the Department of Energy (DoE).

The aim is first to control the electricity supply with utmost efficiency and also reduce the carbon emissions. A smart grid system basically needs to have the following properties (Figure 2) [4]:

(1) digitalization,

(2) intelligence,

(3) resilience,

(4) customization,

(5) flexibility.

Digitalization means to have a digital platform which makes the system fast and reliable. Flexibility would mean that the smart grid needs to be compatible, expandable, and adaptable. Intelligence would mean to inherit an intelligent technology. Resilience would mean that the system should not be affected by any attacks. And lastly, customization means the system needs to be client tailored.

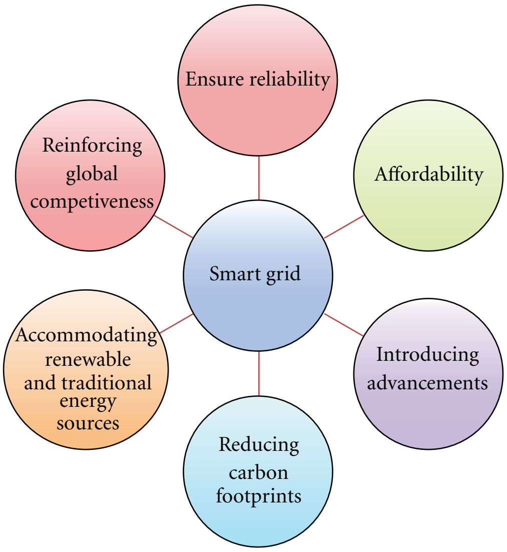

Ensure reliability
Reinforcing global competiveness
Affordability
Smart grid
Accommodating renewable and traditional energy sources
Introducing advancements
Reducing carbon footprints

Figure 1: Smart grid goals.

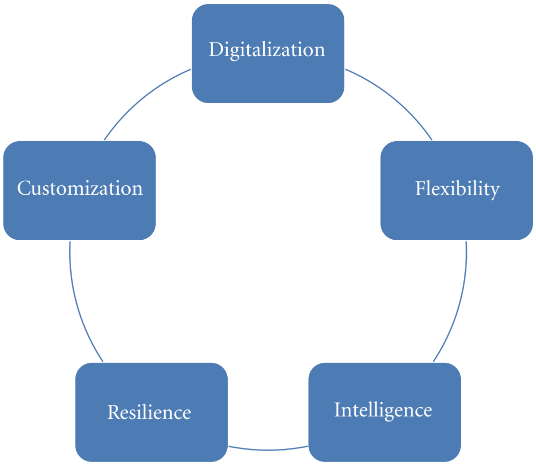


Figure 2: Smart grid properties.

The power grid today is already a very complex and intelligent system. It comprises thousands of miles of high voltage lines, an intelligent control system that controls it, and a communication system that distributes it. A smart grid would help us improve the efficiency and availability of the same power system by using better control strategies.

2.2. Challenges. Let us see what are the problems related to the current power grid system.

The current grid is "purpose built". This means that it is made in such a way that we cannot add any new control points and any security functions. The grid is bandwidth limited, and this restricts us from adding any extra information that would be required to ensure authentication. If there is no room for security, it implies the protocols runs relying on trust, and thus ignoring the possibility of any unknown entity.

In case of the new smart grid, the practice has changed; initially the devices used were purpose built, and these days, they are multipurpose. Instead of using dedicated lines for communication, we use the TCP/IP. Though the technology has drastically improved, the chances of being attacked have also increased rapidly.

Another issue is that smart meters would read the energy usage of a particular residence multiple times in an hour, which would lead to a loss of privacy for the consumer. That is because if one has a smart grid, then one can know whether a residence is occupied or not and also at what time what appliances are being used. This could lead to two different types of attack, either a simple theft or pricing the signals for monetary gains [5].

3. The Smart Grid Architecture

3.1. A General Model. The electricity delivery network basically consists of two subsystems, a transmission system and a distribution subsystem (Figure 3).

In the transmission network, electricity is moved in bulk from 345 kV to 800 kV over AC and DC lines. Power flows in one direction and is distributed to consumers at 132 kV. However, the smart grid will provide bidirectional metering unlike the present grid.

The grid includes a monitoring system and a smart meter which keeps track of the electricity consumed. It includes superconductivity transmission lines which help to reduce the resistive losses and also is compatible to other sources of energy like wind, solar, and so forth.

3.2. Functional Components. The three functional components of a smart grid are smart control centers, smart transmission networks, and smart substations. Let us take a look at them one by one as follows [4].

3.2.1. Smart Control Centers. The smart control centers will depend on the existing control centers. The main functions of a control center are as follows [4].

Monitoring/Visualization. The present control center performs monitoring based on the data collected via SCADA and RTUs (remote terminal units). In the future, information will be obtained from state measurement modules. It is better than the present module in terms of “running time” and “robustness”. In the future, the outcomes will be combined with a wide area geographical information system (GIS), and a visual display will be provided. In this manner, more information will be covered. Also, in the future, the control centers will provide the root cause of a problem rather than just giving an alarming signal.

Analytical Capability. The future is expected to have online time domain-based analysis. These would include voltage stability and transient angular stability. The present grid does not provide the real-time dynamic characteristics of the system whereas in the future, we will have a dynamic model updates. Also, the future grid is expected to have a look ahead simulation capability.

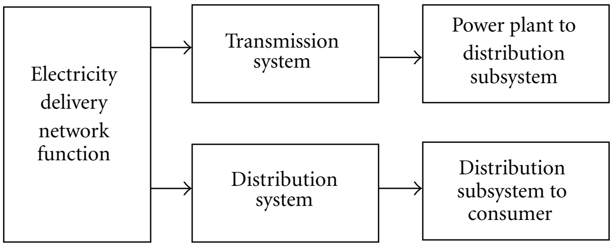

Electricity delivery network function
Transmission system
Power plant to distribution subsystem
Distribution system
Distribution subsystem to consumer

Figure 3: A general model.

Controllability. In the present grid, operations like separating, restoration, and so forth, depend on offline studies. In the future, these will be real time and dynamic. Fixed values are used for the protection and the control settings now, but in the future, proactive and adaptive approaches will be used. Also, there is no coordination when any decision is taken in the current technology. In future, there will be coordination in order to gain a better control.

Interaction with Electricity Market. The main aim of a smart grid system is to achieve high efficiency. For this, we need a control system that dynamically adjusts in accordance with the market. Sophisticated tools are used for this purpose. Also, the smart grid needs to accommodate renewable energy sources.

3.2.2. Smart Transmission Networks. There are new features that are included in the smart grid which involves signal processing, sensing, advanced materials, power electronics, communications and computing. These would improve the efficiency, utilization, quality, and security of the present system.

For long distance transmission, we use high-capacity AC and DC facilities. When the overhead lines are not possible, underground cables are used. High-temperature composite conductors and high-temperature superconducting cables are used for electrical transmission, since they have a higher current carrying capacity, low voltage drop, reduced line losses, light in weight, and better controllability. Six and twelve phase transmission lines are used which provide greater power transmission with reduced electromagnetic field and great phase cancellation.

Flexible and reliable transmission is made possible by using advanced flexible AC transmission system (FACTS) and high-voltage DC (HVDC) devices. FACTS are placed in the transmission network, and they improve the dynamic performance and stability. They will help grid to be free from transmission congestions. HVDC is used as a cost-effective alternative to AC lines.

Intelligent sensors are used with advanced signal processing to measure the line parameters and monitor the status around the sensor location. These sensors can detect the conductor temperature, detect galloping lines, predict initial failures of insulators and towers, identify fault locations, and so forth.

Based on these parameters, the operating conditions can be autonomously detected, analyzed, and responded in case of emergencies, thus maintaining the reliability and security of the transmission system. Also, smart grid systems have reduced catastrophic failures and less maintenance cost. Extreme event facility hardening systems are used to manage failure and restore the system rapidly [4].

3.2.3. Smart Substation. The equipments in the substation should be more reliable and efficient for functions like monitoring, controlling, operating, protecting, and maintaining. The main functions are the following [4]:

(1) smart sensing and measurement,

(2) communication,

(3) autonomous control and adaptive protection,

(4) data management and visualization,

(5) monitoring and alarming,

(6) diagnosis and prognosis,

(7) advanced interfaces with distributed resources,

(8) real-time modeling.

4. Cyber Security

4.1. Cyber Security Model. Like for any other network's security, the three main objectives that cyber security focuses on is availability, integrity, and confidentiality, that is, availability of power with integrity of information and confidentiality of customer's information.

Availability. The reason why we have smart grid is "availability". The basic goal of our network is to provide uninterrupted power supply to the users and to match user requirements.

Confidentiality. The grid network is responsible for the protection of a user's information. If the data is not protected, ample information about the user can be revealed to the attacker.

Integrity. The messages received from the user end should be authenticated. The network must ensure the information is not tampered. Also, the source of message should be authentic.

The smart grid's cyber infrastructure consists of electronic information and communication systems and services along with the information contained in these systems and services. This includes both the hardware and software too. Their basic functions are to process, store, and communicate information. This is done using a control system (SCADA) [6, 7]. The SCADA is a neutral system.

4.2. SCADA System. Supervisory control and data acquisition (SCADA) systems are basically centralized control systems that are used by our power distribution system. It is used for monitoring and controlling process [8].

The main blocks that a SCADA system includes are the following:

(i) HMI (human machine interface) presents processed data,

(ii) a supervisory computer that collects all the data and uses it for processing purpose,

(iii) remote terminal units (RTUs),

(iv) programmable logic controller (PLC),

(v) communication infrastructure.

By using the power system communication in the smart grid, the SCADA systems are connected to other systems like the internet or by certain dedicated lines. The vendors are using off the shelf products as part of the SCADA systems. These products are similar to the personal computers we use at home, and thus are susceptible to attacks and different threats [9].

A SCADA system is a necessary element in the grid infrastructure. It is used for two purposes, first the public transport system and second the public control system.

The cyber security basically can be attacked in three steps [10] as follows:

(1) the attacker has control over the SCADA system,

(2) the attacker identifies the system to launch an intelligent attack,

(3) attacker initiates the attack.

These SCADA systems are most vulnerable to attacks. In order to prevent the attackers from gaining control of SCADA system, automation will be required. The NIST has established smart grid cyber security coordination task group (CSCTG) which addresses and evaluates processes leading to comprehensive cyber security policies for smart grid [6].

The risks assessed by the CSCTG include [6, 11] the following:

(i) complexity of grid leading to weak point and openings to attackers,

(ii) cascading errors as a result of interconnected networks,

(iii) DoS (denial of service) attack,

(iv) attack on consumer privacy to excessive data gathering,

(v) attacks from annoyed employees and terrorists,

(vi) as number of nodes increases the number of entry points for an attacker also increases.

In order to obtain cyber security, we also need to have a robust hardware. We can discuss this further by dividing the hardware section in two parts: (a) new substations and (b) existing systems. In case of new substations, we can completely design the system to be immune against cyber security threats. For this, we can use managed switches. These are smart switches which perform multifunctions like access control, traffic prioritization, managing data flow, and so forth. However, since we already have an ethernet-based system laid, we must make changes to these systems such that they can withstand cyber attacks. For this, we can either update the present infrastructure or Install Security appliances. Security appliances are present between the ethernet connections and are used for examining and monitoring purposes. Another addition to existing systems would be the use of firewalls. They block unauthorized access to any network and work according to the user defined rules. We could also use a technology called VPN (virtual private network), where the connection between two stations is secured [12].

The Cyberspace Policy Review initiated by President Obama advised that "the Federal government should work with the private sector to define public-private partnership roles and responsibilities for the defense of privately owned critical infrastructure and key resources." Specifically, the review recommended that as "the United States deploys new Smart Grid technology, the Federal government must ensure that security standards are developed and adopted to avoid creating unexpected opportunities for adversaries to penetrate these systems or conduct large-scale attacks [11, 13]."

The Department of Energy should work with the federal energy regulatory commission to determine whether additional security mandates and procedures should be developed for energy-related industrial control systems. In addition, the United States deploys new smart grid technology, the federal government must ensure that security standards are developed and adopted to avoid creating unexpected opportunities for adversaries to penetrate these systems or conduct large-scale attacks [11].

Chairman Thompson issued the following statement regarding the legislation: "Any failure of our electric grid, whether intentional or unintentional would have a significant and potentially devastating impact on our nation. We must ensure that the proper protections, resources and regulatory authorities are in place to address any threat aimed at our power system. This legislation addresses these critical issues by providing a common sense approach to ensure continued security of the nation's electric infrastructure [14],".

The security concerns are increasing as the numbers of connections are increasing. There have been cases where cyber spies from China, Russia, and other countries are reported to have entered the United States electrical grid and tried to attack the system. The ability to resist attacks is one of the inevitable functions of the smart grid [15].

5. Cryptography and Key Management

In order to obtain cyber security, we must secure data using cryptography and different keys. In this section, we will study the various aspects related to cryptography and key management. We will first go through the different constraints related to cryptography followed by the cryptographic issues and solutions [16].

5.1. Constraints

5.1.1. Computational Constraints. Residential meters will have limitations when it comes to computational power and the ability to store cryptographic materials. The future devices are bound to have the basic cryptographic capabilities including the ability to support symmetric ciphers for authentication. The use of low-cost hardware with embedded cryptography is necessary but not enough to achieve high availability, integrity and confidentiality in the smart grid.

5.1.2. Channel Bandwidth. The communications that will take place in a smart grid system will take place over different channels that have different bandwidths. AES is a cipher that produces the same number of output bits as input bits. These bits cannot be compressed too, since they are encrypted and random in nature. In case we need to compress this data, we need to do so before encryption. Another factor to be taken into consideration is the cipher-based message authentication code (CMAC), which is added as a fixed overhead to a message and is typically 64 bits or 96 bits. These overheads turn out to be significant when we are dealing with short messages, since they would need large channel Bandwidth.

5.1.3. Connectivity. Standard public key infrastructure-based on peer-to-peer key establishment model where any peer may need to communicate with another is not desirable from a security standpoint for components. Many devices may not have connectivity to key servers, certificate authorities, online certificate status, and protocol Servers. Many connections between smart grid devices will have longer duration than typical internet connection.

5.2. General Cryptographic Issues

Entropy. Cryptographic key generation requires a good source of entropy that creates randomness which is unavailable for many devices.

Cipher Suite. A cipher suite that is open is needed in order to achieve interoperability. A decision about which block cipher, their modes, key sizes, and asymmetric ciphers forms the base of authentication operation.

Key Management Issues. Security protocols depend on security associations. There can be two types in which the security is authenticated: (1) use of Secret key and (2) use of certificate authority. In case we use secret keys, the keys have to be transported from a device to another. To transport these keys, we need a set of keys for each pair of communicating devices and all this needs to be well coordinated. There is also a hardware alternative for this, but that is a costlier option and involves a large amount of overhead. Digital certificates turn out to be cost effective solution as coordination is not required as it was in the case of public key system. Each device needs just one certificate for key management and one private key that is fixed from the time of installation. However, generating PKI and also having certificate authorities will also have a certain amount of overhead unnecessary for smaller systems.

Elliptic Curve Cryptography. A cryptographic Interoperability strategy (CIS) initiated by National Security Agency (NSA) for government systems selects approved cryptographic techniques. It consists of AES for encryption with 128 or 256 bits. Ephemeral unified model and Diffie-Hellman key agreement schemes, elliptic curve digital signature algorithm and secure hash algorithm (SHA) for hashing.

5.3. Cryptographic and Key Management Solutions

5.3.1. General Design Considerations

(i) Selection of cryptographic technique should be such that the design is robust and the algorithm is free of flaws.

(ii) Entropy issue can be solved by seeding a deterministic random bit generator (RBG) before distribution or use a key derivation function which comes with the device.

(iii) Use of cryptographic modules that is used to protect the cryptographic algorithm. We need to upgrade these modules timely, since smart grid equipments would be used for around twenty years and also replacing them would be a costlier affair.

(iv) Failure in encryption systems may occur due to implementation errors, compositional failures, insecure algorithms, or insecure protocols. These categories should be taken into consideration while designing.

(v) Since a random number generator is an integral part of the security system, its failures would result in a compromise of cryptographic algorithm or protocol.

(vi) There must be alternatives for authentication and authorization procedures in case we cannot connect to another system.

(vii) Availability must always be there since dropping or refusal to re-establish a connection may affect the critical communication.

(viii) The algorithms and key lengths should be such that the desired security strength is attained.

(ix) In order to maintain security of the keying materials and authentication data, we must protect it from unauthorized access or any device tampering. Physical security is required for this purpose.

5.3.2. Key Management System for Smart Grid. We use certificates that have validity, that is, certificates that have not expired. If this certificate is issued to a device, that is, no longer reliable, either lost or stolen, then the certificate can be revoked. A certificate revocation list is used for this purpose. A device that uses the information in a certificate is called relying party (RP). RP has a checklist that must be considered when accepting a certificate.

The points that need to be checked are as follows

(i) if the certificate was issued by a trusted CA,

(ii) if certificate is still valid and not expired,

(iii) certificate should be in an authoritative CRL,

(iv) verification of the certificate subject and policy for which certificate is being used.

5.4. Approved Algorithms

Symmetric Key. Advanced encryption standards (AESs), triple data encryption algorithm (TDEA), or triple data encryption standard (TDES).

Asymmetric Key. Digital signature standard (DSS), digital signature algorithm (DSA), RSA digital signature algorithm (RSA), elliptic curve digital signature algorithm (ECDSA).

Secure Hash Standard. Secure hash standards (SHSs) and secure hash algorithm (SHA).

Message Authentication. CMAC, CCM, GCM/GMAC (Galois counter mode), and HMAC (hash message authentication code).

Key Management. SP800-108 KDF's.

Deterministic Random Number Generators. FIPS 186–2 APPENDIX 3.1 RNG, FIPS 186–2 APPENDIX 3.2 RNG, ANSI X9.31-1998 APPENDIX A2.4 RNG, ANSI X9.62-1998 ANNEX A.4 RNG, and ANSI X9.31 APPENDIX A.24 RNG using TDES and AES RNG, SP 800-90 RNG.

Nondeterministic Random Number Generators. Currently None.

Symmetric Key Establishment Techniques. FIPS 140–2 1G D.2.

Asymmetric Key Establishment Techniques. SP 800–56 A, SP 800–56 B, and FIPS 140–2 1G D.2.

These algorithms can be studied in detail from [17–34].

6. Privacy

Privacy cannot be defined. The basic definition of privacy would be “the right to be left alone”. Privacy should not be confused with confidentiality. Confidentiality of information is information that can be accessed only by a few. In reference to the smart grid privacy means considering the rights, values and interests of customers (like their personal information, electric signatures, etc.). The data used by smart grid could be used to violate individuals [35].

A privacy impact assessment (PIA) is used for determining the privacy, confidentiality, and secure risks that arise due to the collection, use, and disclosure of personal information. PIA findings and recommendations are as follows [35].

(1) *Management and Accountability.* People should be appointed to ensure that the documented policies for information security and privacy are followed. Audit functions should be present in order to check the data access activity.

(2) *Notice and Purpose.* Before collecting data, using it, or sharing it, a notice must be prepared and exchanged.

(3) *Choice and Consent.* The consumer should be provided with the choices present in context to the energy usage data that could be revealed and their consent should be obtained.

(4) *Collection and Scope.* Only the information that is really necessary should be collected from the user by appropriate lawful means and with their consent.

(5) *Use of Retention.* The information that is collected should be used only for those purposes for what they were taken. Also, the information should be saved in such a way that no activity or information about the consumer can be found out from it. The data should be discarded once its purpose is over.

(6) *Individual Access.* Consumers should be able to see their individual data and can also request for correction if any of the data is inaccurate. They also have the right to know where their information is being shared.

(7) *Disclosure and Limiting Use.* The personal information cannot be shared by anyone not present in the initial notice and should only be used for the reason stated in the notice.

(8) *Security and Safeguards.* The personal information should be secure and must be protected from thefts, modification or unauthorized access.

(9) *Accuracy and Quality.* The personal information should be as accurate as possible and related to the purpose mentioned in the notice.

(10) *Openness, Monitoring, and Challenging Compliance.* A service recipient should be able to access the personal data and should be able to challenge the organizations compliance.

7. Conclusion

The various security concerns related to smart grid was proposed in this paper. Smart grid is an emerging project. Its implementation will result in numerous benefits for the society. However, it has to face a few challenges and concerns when it comes to security. We have studied these challenges in this paper. Cyber security is an integral part of the grids security concern. As the grid develops and expands in the future, the number of nodes that will be not susceptible to cyber attacks will increase. Domain architecture which is used to evaluate these challenges is explained in one of the sections. We then explain cryptography and key management techniques which are used to secure the system against cyber attacks. In this section, we covered the constraints for cryptography and also the proposed solutions. The last part of the paper deals with consumer privacy which is another important security parameter that cannot be neglected. In order to make the smart grid more popular, it should be free from any security drawbacks and hazards in order to have a better future.

Acknowledgment

I would like to thank Dr. Zuyi Li for his guidance and the help and inspiration he extended for this paper.

References

[1] C. W. Gellings, *The Smart Grid: Enabling Energy Efficiency and Demand Response*, The Fairmont Press, 2009.

[2] "The smart grid: an introduction," http://energy.gov/oe/downloads/smart-grid-introduction-0.

[3] "European smart grids technology platform," http://www.smartgrids.eu/documents/vision.pdf.

[4] F. Li, W. Qiao, H. Sun et al., "Smart transmission grid: vision and framework," *IEEE Transactions on Smart Grid*, vol. 1, no. 2, Article ID 5535240, pp. 168–177, 2010.

[5] S. Clements and H. Kirkham, "Cyber-security considerations for the smart grid," in *Proceedings of the Power and Energy Society General Meeting (2010 IEEE)*, pp. 1–5, July 2010.

[6] G. Iyer and P. Agrawal, "Smart power grids," in *Proceedings of the 2010 42nd Southeastern Symposium on System Theory (SSST 2010)*, pp. 152–155, March 2010.

[7] Z. Vale, H. Morais, P. Faria, H. Khodr, J. Ferreira, and P. Kadar, "Distributed energy resources management with cyber-physical SCADA in the context of future smart grids," in *Proceedings of the 15th IEEE Mediterranean Electrotechnical Conference (MELECON 2010)*, pp. 431–436, April 2010.

[8] "SCADA," http://en.wikipedia.org/wiki/SCADA.

[9] G. N. Ericsson, "Cyber security and power system communication—essential parts of a smart grid infrastructure," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, Article ID 5452993, pp. 1501–1507, 2010.

[10] F. Boroomand, A. Fereidunian, M. A. Zamani et al., "Cyber security for smart grid: a human-automation interaction framework," in *Proceedings of the IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe 2010)*, pp. 1–6, October 2010.

[11] "Cyberspace policy review," http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[12] A. Dreher and E. Byres, "Get smart about electrical grid cyber security," http://www.belden.com/pdfs/techpprs/PTD_Cyber_SecurityWP.pdf.

[13] "Introduction to NISTR 7628 guidelines for smart grid cyber security," 2010, http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf.

[14] "Critical electric infrastructure protection act," http://ciip.wordpress.com/2009/04/30/critical-electric-infrastructure-protection-act/.

[15] "The security vulnerabilities of smart grid," 2009, http://www.ensec.org/index.php?option=com_content&view=article&id=198:the-security-vulnerabilities-of-smart-grid&catid=96:content&Itemid=345.

[16] "Guidelines for smart grid cyber security vol. 1, smart grid cyber security, architecture and high-level requirements," 2010, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf.

[17] "Advanced encryption standard (AES)," 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[18] M. Dworkin, "Recommendation for block cipher modes of operation-methods and techniques," 2001, http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf.

[19] M. Dworkin, "Recommendation for block cipher modes of operation-the XYS-AES mode for confidentiality on storage device," 2010, http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf.

[20] W. C. Barker, "Recommendation for the triple data encryption algorithm (TDEA) Block Cipher," 2008, http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf.

[21] "Digital signature standards," 2009, http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf.

[22] "FIPS PUB 186-2," 2000, http://csrc.nist.gov/publications/fips/archive/fips186-2/fips186-2-change1.pdf.

[23] "Secure hash standard," 2008, http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf.

[24] M. Dworkin, "Recommendation for block cipher modes of operation-the CMAC Mode for authentication," 2005, http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf.

[25] M. Dworkin, "Recommendation for block cipher modes of operation-the CCM mode for authentication and confidentiality," 2004, http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C.pdf.

[26] M. Dworkin, "Recommendation for block cipher modes of operation-galois/counter mode (GCM) and GMAC," 2007, http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf.

[27] "The keyed hash message authentication code(HMAC)," 2002, http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf.

[28] L. Chen, "Recommendation for key derivation using pseudorandom functions," 2009, http://csrc.nist.gov/publications/nistpubs/800-108/sp800-108.pdf.

[29] "Recommendation guidance for FIPS PUB 140-1 and cryptographic module validation program," 2002, http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-1/FIPS1401IG.pdf.

[30] S. S. Keller, "NIST-recommended random number generator based on ANSI X9.31 appendix A2.4 using the 3 key triple DES and AES algorithms," 2005, http://csrc.nist.gov/groups/STM/cavp/documents/rng/931rngext.pdf.

[31] E. Barker and J. Kelsey, "Recommendation for random number generation using deterministic random bit generator (revised)," 2007, http://csrc.nist.gov/publications/nistpubs/800-90/SP800-90revised_March2007.pdf.

[32] E. Barker, L. Chen, A. Regenscheid, and M. Smid, "Recommendation for Pair wise key establishment schemes using integer factorization cryptography," 2009, http://csrc.nist.gov/publications/nistpubs/800-56B/sp800-56B.pdf.

[33] E. Barker, D. Johnson, and M. Smid, "Recommendation for pair wise key establishment schemes using discrete logarithmic cryptography (revised)," 2007, http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf.

[34] "Implementation guidance for FIPS PUB 140-2 and the cryptographic module validation," 2010, http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf.

[35] "Guidelines for smart grid cyber security vol. 2, privacy and smart grid," 2010, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.

Hindawi Publishing Corporation
International Journal of Digital Multimedia Broadcasting
Volume 2011, Article ID 289015, 8 pages
doi:10.1155/2011/289015

Review Article

M2M Communications in the Smart Grid: Applications, Standards, Enabling Technologies, and Research Challenges

Siok Kheng Tan, Mahesh Sooriyabandara, and Zhong Fan

Telecommunications Research Laboratory, Toshiba Research Europe Ltd., 32 Queen Square, Bristol BS1 4ND, UK

Correspondence should be addressed to Zhong Fan, zhong.fan@toshiba-trel.com

Received 9 February 2011; Revised 28 April 2011; Accepted 26 May 2011

Academic Editor: Chi Zhou

We present some of the ongoing standardisation work in M2M communications followed by the application of machine-to-machine (M2M) communications to smart grid. We analyse and discuss the enabling technologies in M2M and present an overview of the communications challenges and research opportunities with a focus on wireless sensor networks and their applications in a smart grid environment.

1. Introduction

Smart grid (SG) networks will be characterised by the tight integration of a flexible and secure communications network with novel energy management techniques requiring a very large number of sensor and actuator nodes. The communications network will not only facilitate advanced control and monitoring, but also support extension of participation of generation, transmission, marketing, and service provision to new interested parties.

In order to realise the intelligent electricity network, machine-to-machine (M2M) communication is considered as a building block for SG as a means to deploy a wide-scale monitoring and control infrastructure, thus bringing big opportunities for the information and communication technology (ICT) industry. For example, smart metering in M2M can facilitate flexible demand management where a smart meter (SM) is a two-way communicating device that measures energy (electricity, gas, water, or heat) consumption and communicates that information via some communications means back to the local utility. With near realtime information available for example based on the flow of energy in the grid, different levels of tariff can be calculated and made available for the consumer, the consumer can make a smarter and more responsible choice. The information generated by SM therefore acts like "glue" allowing various components of SG to work together efficiently. There are also various large-scale wireless sensor and actuator networks (WSAN) deployed in SG (such as the electric power system generation, or home applications) in order to carry out the monitoring task, for example [1]. These WSANs with the collaborative and self-healing nature have an important role to play in realising some of the functionalities needed in SG. On the other hand, there is also cellular M2M where cellular technology plays an important role in M2M communications due to its good coverage, promising data rates for many applications, and so forth. However, in this paper, we mainly focus on WSAN where various short-range wireless technologies are used to support various M2M applications.

There are currently various standardisation activities in M2M communications with a conscious effort to deliver a harmonised set of European standards. The challenges and opportunities that smart metering and smart grids present to communications networks are significant and include interoperability, scalable internetworking, scalable overlay networks, and home networking with potentially much larger numbers of devices and appliances. The security and privacy aspects are also extremely important given the large amount of private data that can be exposed by smart metering alone.

In this paper, we discuss the applications of M2M communications to SG. We present a brief introduction

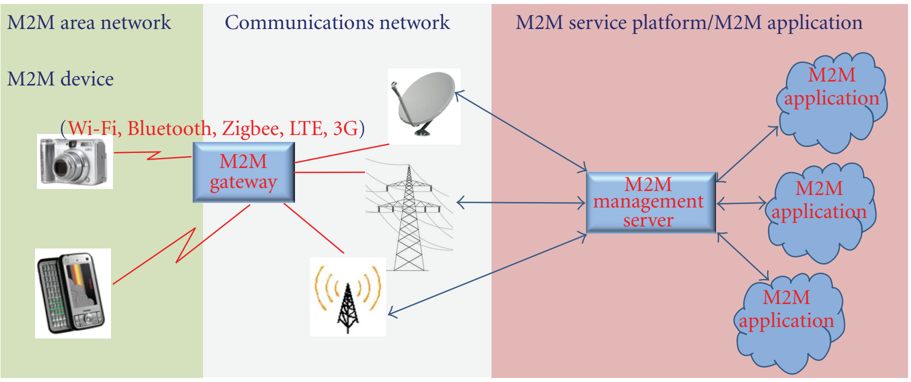


Figure 1: Architecture of M2M networks.

on M2M standardisation work in Section 2, and M2M scenarios and requirements in SG in Section 3. Further we discuss the enabling technologies in Section 4 and provide an overview of the communications challenges and research opportunities in Section 5, with a focus on WSAN and its applications in an SG environment. Section 6 is devoted to the conclusion of this paper.

2. M2M Standardisation Activities

2.1. M2M Architecture and Topology. M2M is unarguably a combination of various heterogeneous electronic, communication, and software technologies. The general architecture of M2M networks such as those being specified in ETSI TC (technical committee) M2M is shown in Figure 1. Other more detailed information of the M2M architecture can be derived from the on-going work in ETSI TC M2M. In reference to this architecture, M2M devices (intelligent and communication enabled) form an M2M area network; this could be from a small-scale home environment to a bigger environment such as a factory. The M2M area network is connected to the communication network such as satellite, power line, or mobile base stations through the M2M gateway. Through the communication networks, they are connected to the M2M management server on the M2M service platform and subsequently reaching the M2M applications (video for monitoring, online social networking, etc.) on the other side of the M2M management server.

2.2. ETSI M2M. The European Telecommunications Standards Institute (ETSI) Technical Committee is developing standards for M2M communications. The group aims to provide an end-to-end view of M2M standardisation, and will cooperate closely with ETSI's activities on next generation networks, and also with the work of the 3GPP standards initiative for mobile communication technologies. ETSI TC M2M is among one of the three European Standardisation Organisations which have been issued a mandate by the European Commission on Smart Metering (M/441). The TC M2M domain of coordination to answer M/441 includes providing access to the meter databases through the best network infrastructure (cellular or fixed) and providing end-to-end service capabilities, with three targets: the end device (smart meter), the concentrator/gateway, and the service platform. Further, smart metering application profiles will be specified including service functionalities. Figure 2 shows the responsibility area among CEN (European Committee for Standardisation), CENELEC (European Committee for Electrotechnical Standardisation), and ETSI on the M/441 mandate work.

A number of liaisons have also been established with other standardisation bodies, for example, CEN, CENELEC, DLMS UA, ZigBee Alliance, and other ETSI TCs.

2.3. 3GPP. Apart from ETSI, 3GPP is also active in M2M technology-related activities. In 3GPP M2M is also called machine-type communications (MTC) where work has been carried out on the optimisation of access and core network infrastructure, allowing efficient delivery of M2M services. 3GPP SA1 has already completed a technical report TR 22.868 in 2008 on "Facilitating M2M Communications in GSM and UMTS." They have now started a new work item on network improvement for MTC, in order to gather requirements to reduce the operational costs of supporting M2M services. 3GPP SA1 Services is working on the services and features for 3G systems. In release 10, they have produced "Service Requirements for Machine Type Communications (MTC) Stage 1." 3GPP SA 3 has started looking into the security aspects of MTCs.

2.4. IETF ROLL—Wireless Sensor Networks (WSN) and Internet of Things. IETF has created a set of activities related to sensor technologies and smart objects such as 6Lowpan and ROLL (routing over low-power and lossy networks). These efforts are aiming at bringing the Internet Protocol to sensors and M2M devices needed for building a monitoring infrastructure for SG. Working Group ROLL is focusing on RPL (routing protocol for LLNs) for low-power and lossy networks (LLNs) where the nodes in the networks are many embedded devices with limited power, memory, and processing resources. These nodes are interconnected by various wireless technologies such as IEEE 802.15.4, Bluetooth, low-power WiFi, and power line communication links. The emphasis of the work is on providing an end-to-end IP-based solution in order to avoid the non-interoperable networks problem.

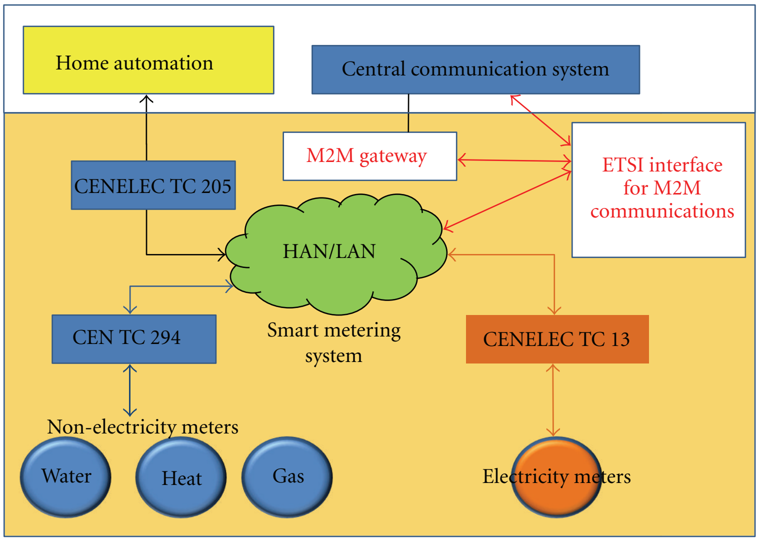


Figure 2: M441 responsibility split among CEN/CENELEC/ETSI.

3. M2M in Smart Grid:M2M Scenarios and Requirements in SG

With the various functionalities that an M2M system could offer, it has been considered as one of the foundation ICT solutions on realising SG. In this section, first of all, we look into the basic architecture for SG and how the M2M architecture relates to this. This is followed by discussing two important M2M scenarios and exploring the related applications with WSAN in mind. Such understanding is essential when more detailed functional and technical requirements need to be developed. In particular, we look into how WSAN play a key part in delivering M2M applications in an SG context.

Figure 3 [2] shows the ETSI board of director architecture for SG which is formed by three main planes: Layer 1, the energy plane handles the energy related to production, distribution, transmission, and consumption, therefore includes a large amount of sensors, electricity storage systems, transmission, and distribution systems. This layer corresponds to the M2M area (device) network in M2M networks. Layer 2 is the control and connectivity layer which connects the energy plane to the service plane. This relates to the M2M communications network layer. Layer 3 is the service layer which provides all the SG-related services. This is related to the M2M service layer in the M2M network architecture. How to apply M2M architecture to SG networks will need to be further studied or standardised.

More recently, WSAN has been gaining popularity on becoming a promising technology that can enhance various aspects of today's electric power systems, including generation, delivery, and utilisation. This is due to the collaborative and low-cost nature of the networks (also without the need to construct a complex and expensive infrastructure). At the same time WSAN also has some intrinsic advantages over other conventional communication technologies, such as wide area coverage and adaptability to changing network conditions. However, different environments pose different challenges to a WSAN; for example in a harsh and complex electric power system environment, WSAN communication in SG applications faces significant challenges on its communications reliability, robustness, and fault tolerance. In this section, we study the role of WSAN in different M2M applications/scenarios in SG and discuss the different characteristics and challenges.

3.1. Home Applications and Smart Buildings. Wireless home networks (or home area networks (HANs)) are now becoming increasingly popular and have evolved from just computers to including all different types of electronic devices including home appliances and home entertainment systems such as TVs and audio. General applications include that of lighting control, heating, ventilation, and air conditioning control (HVAC) which requires WSAN in place to support the monitoring and also act as the wireless communication infrastructure. Further, they also provide a way to detect fluctuations and power outages. It also allows customers to control remotely the meter (such as switching on and off) enabling cost savings, and to prevent electricity theft. Other applications include demand response and electric vehicle charging.

Smart buildings such as offices rely on a set of technologies to enhance energy-efficiency and user comfort as well as for monitoring and safety of the building. The M2M technology and WSAN are used in building management system for lighting, HVAC, detecting empty offices and then switching off devices such as monitors, and for security and access systems.

The main requirement of the M2M devices in a home and office environment is their very low power consumption so that many devices can last years without requiring battery replacement. With the wide range of home/office devices that need to be networked, there is a need to support several different physical links. Among all the different networking

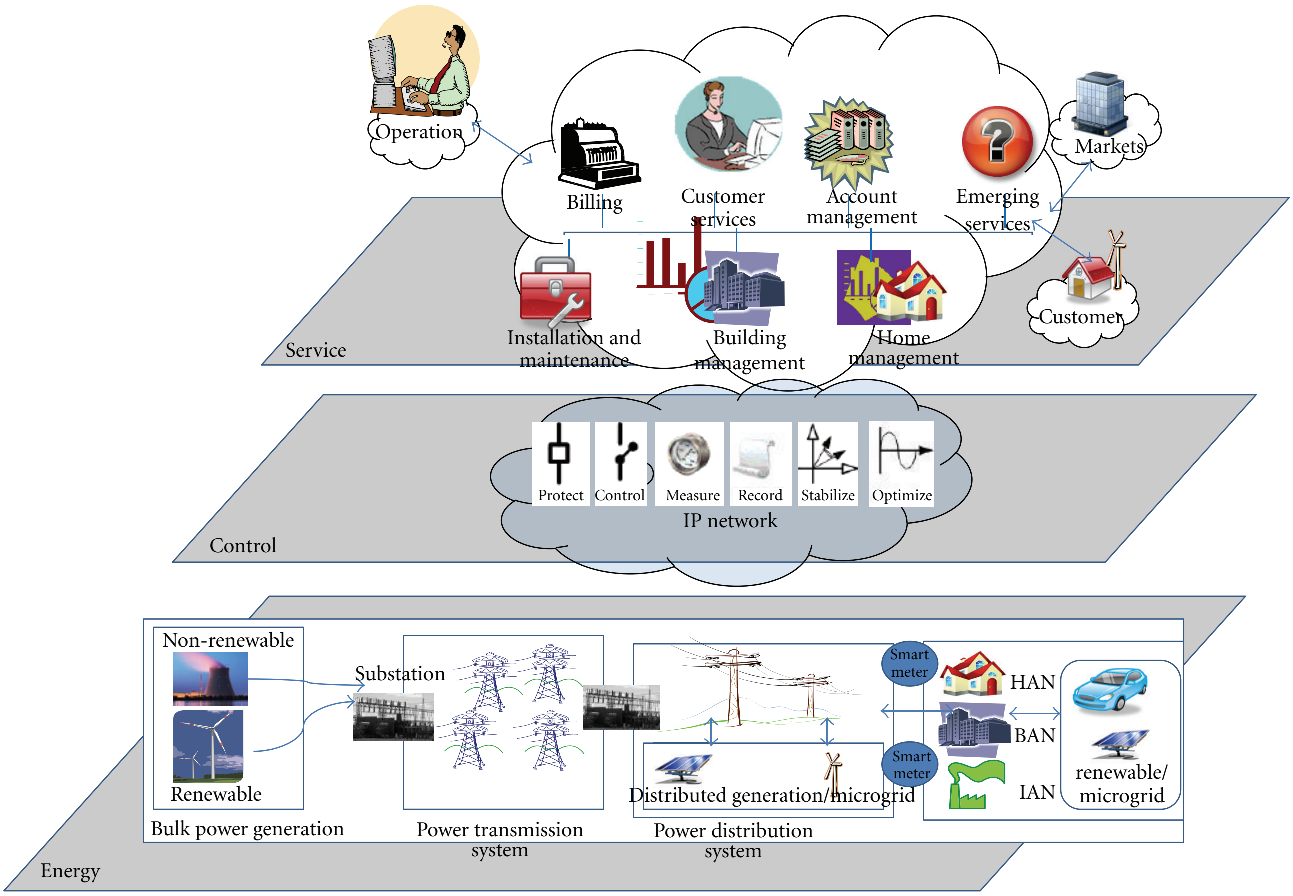


FIGURE 3: ETSI board of directors view on smart grid architecture including M2M network (adapted from [2]).

technologies, Ethernet, 802.15.4, Wi-Fi, Bluetooth, power line communications, and cellular all have a place in the home networking environment. The home M2M network will have to support all the different physical links and protocol stacks through the M2M gateway. The gateway also needs to be able to gather information on what processing and energy resources are available in the M2M devices (which are usually equipped with limited resources) and decide on how to disseminate data in a way that can optimise the resources. In general, the gateway capabilities include that of routing, network address translation (NAT), authentication, resource allocation, and so forth. Other more elaborate services or capabilities of the M2M gateway are on-going work in TC M2M dealing with gateway reachability, addressing and repository, communication, remote entity management, security, history and data retention, transaction management, interworking proxy, and compensation brokerage. Smart building systems with WSAN are also expected to learn from the building environment and adapt the monitoring and control functions accordingly.

3.2. Power Distribution Systems. An SG being the emerging next-generation electric power system, offers improved efficiency, reliability, and safety by allowing smooth integration of alternative energy source as well as automated control and modern communication technologies [3]. Traditional electric power systems rely on wired communication for monitoring and diagnostic purposes. However, these systems require expensive cables to be installed and maintained on a regular basis. Therefore, there is a need for a cost-effective solution that would enhance the management process of the electric power systems.

WSAN has an important role to play in this area due to its low cost, flexible, and collaborative nature for aggregated intelligence. They are capable of monitoring the critical parameters of the equipments in SG and provide a timely feedback to enable the SG system to respond to the changing conditions. This enables SG to function in a reliable way with self-healing capability. The role of sensors in various parts of the SG power distribution system cover a wide range of transmission systems, substations and distribution systems. A WSAN-based wide area network (WAN) electric energy substation monitoring system plays an important role in ensuring the health of the power subsystems (transformers, circuit breakers, etc.) and transmission lines, and improving the observability and reliability of power systems [1].

WSN provides the capability for wireless automatic meter reading (WAMR) for electric power distribution systems with the benefit of reduced operational cost, online pricing, and remote monitoring for asset protection. The challenge in WAMR is reliable two-way communications between the electric utilities and customer's smart metering devices.

One of the major roles of the WSAN in a power distribution system is voltage quality management (VQM). With the growth of nonlinear time variant loads due to various existing and new applications, the distortion and disturbances on the voltage signal have become increasingly a significant problem. In a VQM WSAN, ideally each node can assess the information of performance of the monitored site, by using local information for computation, also the global performance of the monitored grid section by using local information exchanges between its neighbour nodes. With these features, the node could detect local voltage quality anomalies [4].

Some of the requirements of WSAN solutions in SG in a power distribution system are as follows. Highly scalable: the network should be able to scale to hundreds and thousands of devices and many could be communicating at the same time. High reliability: many of these power automation systems are expected to maintain good reliability that will last at least 20–30 years once installed. Other requirements include being able to handle range and obstruction issues as the harsh environment in a power distribution system could affect the link quality and range. Further, there could be various hardware and infrastructure obstructing the communication of the WSAN.

3.3. Other Applications. Other M2M applications cover a wide variety of domains from sales and payment, fleet management, telemetry, e-health applications, to security and surveillance.

4. Enabling Technologies

4.1. Short-Range Wireless Technology. Short-range wireless technology (SRWT) is becoming increasingly popular for ubiquitous WSAN connectivity in various instrumentation, monitoring, and measurement systems. In the context of M2M communications, SRWT plays a crucial role in terms of communication of the M2M devices with little or no human intervention. Such devices will proliferate in various environments with different applications up and running such as home security sensing, lighting control, and health monitoring. There are many challenges in designing such M2M networks which will be described in the later section. In this section, we survey the various potential SRWT for M2M networks and their respective features. In summary as shown in Table 1 (adapted from [5]), IEEE 802.15.4-based protocols such as 6LowPAN and ZigBee are suitable for low power and low data rate applications, also with less stringent range requirements such as sensor networks applications, whereas the IEEE 802.11 (Wi-Fi) protocol is well suited for higher data rate applications (also supporting longer range) including audio and video streaming-related applications. Bluetooth, on the other hand, is suitable for short-range and low-data-rate peer-to-peer communications.

4.2. Networks and Protocols. An efficient routing mechanism in the M2M networks decides how efficient the data can be transported from one end to the other. There are various challenges on applying existing routing protocols to these M2M networks due to some inherent characteristics of the networks such as

(i) Long sleep cycles

(ii) Low power nodes

(iii) Changes to the radio propagation environment

(iv) Changes of topology (mobility of nodes, nodes in sleep mode).

Many low-power protocols such as Zigbee uses the AODV protocol from RFC 3561 [7] as its routing protocol. Under the AODV protocol method, nodes in the network that are not part of an active communication do not maintain any routing information or participate in the periodic routing table exchanges as required in the algorithm. The routing paths are established on an on-demand basis, so only nodes that are awake will be involved in the process. The node that initiates the process will be responsible for most of the computational work in the routing protocol, which includes collecting and evaluating the responses to the route request sent and making decisions on the route with the lowest network cost which could be the path with the smallest number of hop counts or the path with the largest remaining battery power of the nodes.

Another solution proposed in the literature is [6] which is suitable for a long-term environment monitoring network with low duty cycles. The routing is done by allowing the network nodes to sleep most of the time and reviving them whenever the gateway is performing a bulk data download. The low-power node upon waking up would send a probe message to its neighbour to check for any potential communication and the gateway would calculate the network paths using the reachability information collected.

The IETF RPL protocol will enhance the advanced metering infrastructure (a network of smart meters) with IP routing characteristics such as dynamic discovery of network paths and destination, ability to adapt to logical network topology changes, equipment failures or network outages, independence from data link layer technologies, and support for high availability and load balancing. In [8], an RPL-based routing protocol for advanced metering infrastructure (AMI) in SG has been proposed, aiming to enable realtime automated meter reading and realtime remote utility management in the AMI.

5. Challenges and Research Opportunities

Having discussed the various scenarios and its challenges of WSAN in SG, in this section, we elaborate on the various topics of research interests that demonstrate great potential for further studies.

(1) *Gateway Design.* The gateway plays an important role in interconnecting various network devices and sensors in an application scenario. There is a need to cater for the different characteristics of the devices in the gateway. For example

Table 1: M2M short range wireless technology (adapted from [6]).

	802.15.4 (ZigBee/6LoWPAN)	Bluetooth/Bluetooth low energy (LE)	802.11 (Wi-Fi)
Max data rate	250 kb/s	3 Mb/s (enhanced) 1 Mb/s (basic or LE)	22 Mb/s (802.11 g) 144 Mb/2 (802.11 n)
Indoor range	10 m–20 m	1 m, 10 m and 100 m classes, 5–15 m (LE)	45 m
Power	Low	Medium low (LE)	High
Battery life	Years	Days years (LE)	Hours
Frequency band	2.4 GHz 868 MHz and 915 MHz	2.4 GHz	2.4 GHz, 3.6 GHz, and 5 GHz
Channel access	CSMA/CA (non-beacon based) or superframe structure (beacon based, non-contention)	Frequency hopping or CSMA/CA	CSMA/CA
Applications	Smart appliances Smart meters Lighting control Home security Office automation	Voice Smart meters Data transfer Game control Health monitoring (LE) Computer peripheral (LE)	Networking between WAN and customer premises (M2M area networks) Digital audio/voice

in a home environment, there will be devices that have different requirements on power, distance, data rate, and are running different communication protocols. Other issues are security capability, communication selection capability, and so forth. Software-defined radio technologies have been proposed in [5] as a solution to the home M2M gateway architecture enabling the gateway to function at multicarriers and multibands which can communicate simultaneously with different protocols, on different frequencies and in different frequency bands.

(2) *Harsh Environment.* This is a common problem for certain WSANs in SG such as those operating in the power system environment. The WSAN may be subject to strong RF interference, and also harsh physical environment such as corrosion and high humidity. These may cause the network topology and wireless connectivity to change when certain nodes fail or the measurements are not suitable for drawing good conclusions. Wireless channel modelling and link quality characterisation are some of the important work [9] when designing a reliable WSAN in the smart grid in such harsh environment as the power system designers can make use of such model to predict the performance of the network.

(3) *Service Differentiation.* In order to enable efficient prioritisation of certain applications that have some critical requirements to meet such as those belonging to protection and control functions, the WSAN must be able to support quality of service (QoS). For example, an alarm notification for the electric power systems will require immediate attention hence requires a realtime communication; other periodic reporting activities would require reliable communications.

(4) *Packet Loss or Errors and Variable Link Capacity.* In WSAN, the perceived level of interference and bit error rates affects the attainable capacity of each wireless link [9]. Also, the wireless links exhibit a varying characteristic over time and space due to various reasons such as obstructions and noisy environment in an electric power system. Therefore the capacity and delay at each link vary from location to location and could be bursty in nature. This poses a serious challenge to providing QoS in the system. There have been a wide range of methods proposed in the literature based on MIMO (multiple-input and multiple-output) communication and smart antennas that can be exploited to improve the network capacity in a noisy environment.

(5) *Resource Constraint.* The resources required in a sensor node can vary from application to application in terms of energy, memory, as well as processing power. In general, limited battery power is the main resource constraint that requires various communication protocols for WSAN to provide high energy efficiency. Energy efficient protocols such as routing solutions are needed where WSAN are usually expected to function over years without having to change the battery. The routing technique also has to take into account the long sleep cycles, changing radio environment, change of topology, and the limited processing power.

(6) *Security.* Security for WSAN in SG is an essential requirement in order to ensure that the whole system functions smoothly and safe from any sorts of attack and intrusion. This covers a wide range of solutions targeting threats such as denial-of-service, eavesdropping on transmission, routing attacks, flooding for generation plant security, data centre security, WAN security, identity management, access control,

and so forth. Conventional centralised IT network security models are not directly applicable to the highly distributed and low-cost devices in M2M communications networks due to the need for dispersed and decentralized methods.

(7) *Self-Configuration and Self-Organisation.* As the topology of the sensor nodes in a WSAN changes due to sleep mode schedule, mobility or node failure, there is a need for self-configuration and self-organisation to make sure that the network functions as normal. Therefore, fault diagnosis is essential for the hardware as well as software in the infrastructure. Failure analysis or predictive maintenance makes sure that the system has the ability to identify failure (assisting quick failure remedy), predict failure and recover from fault/failure. Intelligent diagnosis methods such as those that filter and reason the mass information related to an alarm, helps quick understanding of the nature of the fault and localised the fault. Various machine learning techniques such as artificial neural network have been proposed in [10, 11] for power system fault diagnosis and alarm information processing.

(8) *Data Processing.* With the large scale development of WSAN in SG, there are a large amount of information collected over time. There is a need to intelligently combine or aggregate, fuse or infer these data in order to draw conclusion on what action is needed or how to configure the parameters in the system for optimum functionality. The other benefit is for increased energy efficiency by better match of supply and demand. For example, the authors [12, 13] proposed using artificial neural network for load forecasting which is important for demand response. Data processing can also help achieve improved security and reliability by fast response to unusual events and in the case of energy shortage. For example, methods for traceback and traceability for malicious activities in critical information such as methods proposed in [14] to examine relevant attributes features at intermediary stages of data transaction in the infrastructure. This is followed by finding the maximum occurrence features pertaining to characteristics of normal and abnormal transactions. These attributes are mined using hybrid data mining algorithms in order to identify unique classes in the traceability matrix for security and privacy.

(9) *Reliability.* Reliability can be tackled from multiple levels such as the communication link level and the system level. The system needs to be able to cope with the harsh environment and adaptively work out the best way to cope with node failure and link variability.

(10) *Middleware and APIs.* Advanced application programming interfaces (APIs) help to enable implementation of optimisation algorithms and efficient management and configuration of networks, open interfaces to enable independent software vendor, device manufactures, and telecoms operators to implement their services. Open APIs provide the means for third parties not directly associated with the original equipment manufacturers to develop a software component which could add functionality or enhancements to the system. On the other hand, smart energy management solutions require access to more information ideally from different service providers and devices implemented by different vendors. Such information should be available and presented in a usable format to interested parties. Further, timing and specific configuration of measurements and controls are also critical for dynamic scenarios. Since support for different technologies and some level of cooperation over administrative boundaries are required, proprietary or widely simplified interfaces will not be sufficient in these scenarios. This situation can be improved by standard generic API definitions covering methods and attributes related to capability, measurement, and configurations. The design of such APIs should be technology agnostic, lightweight and future-proof.

(11) *M2M Computing Platform.* With the deployment of large-scale M2M networks and its various applications to be provided, there needs to be a way to control and manage these devices as well as to work on the data or make the data available efficiently for a different purpose. Cloud computing has been regarded as one of the potential technology to be leveraged for M2M computing. The cloud, a combination of IT virtualisation by combining Internet, information and communication technology, and various resources (hardware, development platforms), makes it easier to deliver the M2M applications as services (through the Cloud) virtually. This allows flexible IT management and data sharing across the platform and resources can be dynamically reconfigured according to the variable load allowing optimum resource utilisation. For example, a commercially available cloud platform for M2M applications is Sierra Wireless AirVantage Cloud Platform [15] which enables M2M solution providers, system integrators and network operators to rapidly develop, is deploy and operate M2M applications and services.

(12) *Multi-Radio Support and Spectrum Efficiency.* Multiple communication technologies and standards are being deployed to support communications in different parts of SG. For example, Bluetooth could be used for the communications between meter and end customer devices. On the other hands, ZigBee and IEEE 802.11 could be used for smart meter interfaces in the home and local area network. In order to manage and support all these different communications, there needs to be multi-radio support functionality in the SG. Also, radio spectrum scarcity is an increasingly important problem due to the rapid growth in the telecommunication service industry. One of the proposed ways of managing the spectrum efficiently is a solution such as using the unoccupied television spectrum, also known as the white space, has been proposed by the Federal Communications Commission (FCC). As this is no longer the static spectrum allocation case in the conventional way, there needs to be an efficient secondary spectrum management strategy. Company such as NEUL [16] has developed M2M communications network solutions which operate in TV white spaces.

(13) *M2M Protocols.* There are various scopes for M2M protocols research such as reliable (i.e. delivery-guaranteed),

delay-guaranteed, rate-efficient, and energy-efficient protocols design. Energy-efficient protocols such as routing and transmission protocols are needed where WSAN are usually expected to function over years without having to change the battery. The routing technique also has to take into account the long sleep cycles, the changing radio environment, changes of topology, and also the limited processing power. The existing leading transmission protocol, that is, TCP/IP is known to be inefficient for M2M traffic with low data volume as there are redundant and overhead which therefore is not energy efficient for M2M communications. Therefore, protocols redesign for M2M communications needs to be explored.

(14) *Optimal Network Design.* As an M2M network consists of an interconnection of a number of devices and systems together, there is a need to design the network to minimise the cost of M2M communications while still meeting the QoS requirements. Placement of gateway, number of M2M devices supported in a clusters, and so forth are some of the related topics [17].

6. Conclusion

There has been no doubt that M2M communication plays an important role in realising the next-generation smart electrical system, SG. In this paper, we have looked into various on-going M2M standardisations-related activities which have shown the growing momentum of M2M in becoming the one of the important ICT solution for SG. We highlighted the work carried out in organisations such as ETSI M2M, 3GPP, and IETF ROLL to draw attention on the set of topics of interest among various stakeholders on M2M in SG picture. Next, we studied a selection of challenges and requirements of M2M application/scenario and WSAN in SG. We then focused on the technical details of M2M communications, which covered a wide range of topics, M2M architecture and topology, various short-range wireless technology, and networks and protocols. Having extensively discussed the above topics, we provided our view on various research opportunities in this topic. We believe that data processing, security, reliability, middleware and APIs, M2M computing platform, multiradio support and spectrum efficiency, M2M protocols and optimal network design are some important and interesting topics that can be looked into in the future work.

Although the roadmap of worldwide smart grid deployment is still not clear, it is almost certain that the future intelligent energy network empowered by advanced ICT technology will not only be as big as the current Internet, but also change people's lives in a fundamental way similar to the Internet. On an even larger scale, the notion of Internet of things will connect trillions of objects and the whole world will become an extremely large-scale wireless sensor network. As M2M communications is an underpinning technology for this vision, we therefore envisage that M2M will be an exciting research area for communication engineers for many years to come.

References

[1] R. A. León, V. Vittal, and G. Manimaran, "Application of sensor network for secure electric energy infrastructure," *IEEE Transactions on Power Delivery*, vol. 22, no. 2, pp. 1021–1028, 2007.

[2] O. Elloumi, J. M. Ballot, and D. Boswarthick, "Smart Grid- an introduction," presentation slides, TCM2M #9, 2010.

[3] U.S. Department of Energy, "The SG: An Introduction," September 2008.

[4] M. di Bisceglie, C. Galdi, A. Vaccaro, and D. Villacci, "Cooperative sensor networks for voltage quality monitoring in SGs," in *Proceedings of the IEEE Bucharest PowerTech Conference*, 2009.

[5] M. Starsinic, "System architecture challenges in the home M2M network," in *Proceedings of the Applications and Technology Conference, (LISAT '10)*, pp. 1–7, 2010.

[6] R. Musaloiu-E, C. J. M. Liang, and A. Terzis, "Koala: ultra-low power data retrieval in wireless sensor networks," *Information Processing in Sensor Networks*, pp. 421–432, 2008.

[7] RFC 3561, http://www.ietf.org/rfc/rfc3561.txt.

[8] D. Wang, Z. Tao, J. Zhang, and A. Abouzeid, "RPL based routing for advanced metering infrastructure in smart grid," in *Proceedings of the ICC*, pp. 1–6, 2010.

[9] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid—a case study of link quality assessments in power distribution systems," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 99, pp. 3557–3564, 2010.

[10] M. A. H. El-Sayed and A. S. Alfuhaid, "ANN-based approach for fast fault diagnosis and alarm handling of power systems," in *Proceedings of the 5th International Conference on Advances in Power System Control, Operation and Management (APSCOM '00)*, pp. 54–58, October, 2000.

[11] M. Ma, D. Zhao, X. Zhang, and D. Liu, "China's research status quo and development trend of power grid fault diagnosis," in *Proceedings of the Asia-Pacific Power and Energy Engineering Conference (APPEEC '10)*, pp. 1–4, 2010.

[12] H. T. Zhang, F. Y. Xu, and L. Zhou, "Artificial Neural Network for load forecasting in smart grid," in *Proceedings of the International Conference on Machine Learning and Cybernetics (ICMLC '10)*, vol. 6, pp. 3200–3205, 2010.

[13] F. Y. Xu, M. C. Leung, and L. Zhou, "A RBF network for short-term load forecast on microgrid," in *Proceedings of the International Conference on Machine Learning and Cybernetics (ICMLC '10)*, vol. 6, pp. 3195–3199, 2010.

[14] E. Hooper, "Strategic and intelligent smart grid systems engineering," in *Proceedings of the International Conference for Internet Technology and Secured Transactions (ICITST '10)*, 2010.

[15] http://www.sierrawireless.com/productsandservices/AirVantage.

[16] NEUL, http://www.neul.com/.

[17] D. Niyato, L. Xiao, and P. Wang, "Machine-to-machine communications for home energy management system in smart grid," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 53–59, 2011.

Hindawi Publishing Corporation
International Journal of Digital Multimedia Broadcasting
Volume 2011, Article ID 382147, 9 pages
doi:10.1155/2011/382147

Research Article

BVS: A Lightweight Forward and Backward Secure Scheme for PMU Communications in Smart Grid

Wei Ren,[1] Jun Song,[1] Min Lei,[2] and Yi Ren[3]

[1] *School of Computer Science, China University of Geosciences, Wuhan 430074, China*
[2] *School of Software Engineering, Key Laboratory of Network and Information Attack and Defense Technology of MoE, Beijing 100876, China*
[3] *Department of Information and Communication Technology, University of Agder (UiA), Grimstad, Norway*

Correspondence should be addressed to Wei Ren, weirencs@gmail.com

Received 30 November 2010; Accepted 20 April 2011

Academic Editor: Pierangela Samarati

In smart grid, phaser measurement units (PMUs) can upload readings to utility centers via supervisory control and data acquisition (SCADA) or energy management system (EMS) to enable intelligent controlling and scheduling. It is critical to maintain the secrecy of readings so as to protect customers' privacy, together with integrity and source authentication for the reliability and stability of power scheduling. In particular, appealing security scheme needs to perform well in PMUs that usually have computational resource constraints, thus designed security protocols have to remain lightweight in terms of computation and storage. In this paper, we propose a family of schemes to solve this problem. They are public key based scheme (PKS), password based scheme (PWS) and billed value-based scheme (BVS). BVS can achieve forward and backward security and only relies on hash functions. Security analysis justifies that the proposed schemes, especially BVS, can attain the security goals with low computation and storage cost.

1. Introduction

Smart grid is envisioned as a long-term strategy for national energy independence, controlling emission, and combating global warming [1]. Smart grid technologies utilize intelligent transmission to deliver electricity, together with distribution networks to enable two-way communications. These approaches aim to improve reliability and efficiency of the electric system via gathering consumption data, delivering dynamic optimization of operations, and arranging energy saving schedules.

The smart grid promises to transform traditional centralized, producer-controlled network to a decentralized, consumer-interactive network. For example, consumers react to pricing signals delivered by control unit from smart meters to achieve active load adjustment. Supervisory control And data acquisition (SCADA) or energy management system (EMS) may collect one data points every 1 to 2 seconds, whereas phaser measurement units (PMUs) may collect 30 to 60 data points per second [2].

The security of smart grid is a critical issue for its applicability, development and deployment [3–7]. On one hand, the security, and especially the availability of power supplying system, affects homeland security, as it is an indispensable infrastructure for pubic living system [8–10]. That is, any transient interruption will result in economic and social disaster. On the other hand, introduction of end devices such as PMUs requests for data and communication security to support secure and reliable uploading of measurements [11, 12].

As the PMUs are exposed far from the central control unit, they present as a security boundary line between defenses and attacks. Such frontier may be tampered by curious users who intend to make certain profits or, even worse, hacked by malicious attackers who target for damaging power scheduling performance [13, 14]. For example, in the former case, advanced customers may try to reduce the value of meter's readings by revising circuits or interfering signals outside; curious eavesdroppers may be interested in customers' power-consuming patterns to pry about the consumers' privacy such as daily behaviors or schedules. In the latter case, the attackers may invoke long-lasting peak values in meters to disturb the SCADA's scheduling strategies [15] or inject a worm to infect all meters to threaten the entire system resulting in a so-called billion-dollar bug [1]. To thwart the former security threaten, a straightforward way is to protect data confidentiality in PMU communications. Furthermore, to guarantee data integrity and data source authentication in PMU communications can mitigate the latter threat. Thus a prerequisite requirement arises—how to deliver and protect the encryption key and integrity key for such communications.

As the security issue for smart grid is an emerging new topic, currently available and customized solutions are a very few or undergoing development. Most existing work focuses on formulating the security problems [1–4, 7, 16] or build the security frameworks [5, 6, 8, 11, 17–19]. Especially, no existing work addresses key management issue for PMU communications in depth to the best of our knowledge. In this paper, we address data security and communication security between PMUs and control units in smart grid from the viewpoint of key management, including key generation, key deployment, and key evolution. After analyzing the data and communication security requirements, firstly, we propose several customized approaches and solutions.

Smart grid has some characteristics of itself own, for example, large number of deployment of end devices, real-time communications, resource constraints in tangible devices, to name a few. Thus, proper security solutions should beware of those specialities, for example, avoid disadvantages in applicable context to improve the applicability of proposed scheme. On the other hand, security design should be crafted for taking advantages of some properties of smart grid such as network architecture, domain context, and operational flow, as it may help to improve the overall performance. More specifically, we will dissect smart grid architecture to extract networking and system model and explore the inner mechanisms such as operational flow between SCADA and PMUs. We propose to solve the security problems by incorporating security scheme into the operational flow seamlessly to shrink the overall cost, and thus improve integrated performance. Such a design rationale makes use of inherent information in operational procedures as a security gradient and will be explained in the paper.

The major contributions of this paper are listed as follows.

(1) The security analysis, including network and system model, attack model and security requirements between PMU and SCADA communications in smart grid are extensively explored.

(2) We propose several lightweight schemes, including public key based scheme (PKS), password based Scheme (PWS), and billed value-based scheme (BVS) to tackle different application scenarios.

The rest of the paper is organized as follows. In Section 2, we discuss basic assumption and models used throughout the paper. Section 3 provides detailed description of our proposed schemes. We analyze security and performance aspects of the proposed scheme in Section 4. Finally, Section 5 concludes the paper.

2. Problem Formation

2.1. Network Model and System Model. The following related entities usually exist in smart grid applications.

(1) *PMU*s. Phaser measurement unit is an indispensable device for smart grid. As it may be exposed outside to potential adversaries, its security should be addressed firstly in the exploration of solutions. Each PMU has an automatic meter reading (AMR) to provide power values (or additionally a unit to delivery pricing information). The PMUs rely on the communication network to send measurements (or receive control instructions).

The characteristics of PMUs are as follows.

(i) Scalability. The number of PMUs is very large, could be in a scale of more than fifty thousands, depending on family quantity in a management domain, for example, in a county or a city scale.

(ii) Resource constraints. The computation and storage resources of PMUs are usually assumed to have constraints.

(iii) Compatibility. PMUs may have multiple variants for different categories of customers, and certain legacy systems or devices may try to be migrated or upgraded to a new version at first as more as possible.

(iv) Asymmetry. PMUs has a large volume of uploading traffics, but down-link traffics are comparatively much less than uploading traffics.

Therefore, incorporated security enhancement modules in PMUs should be affordable and have minimized revision for end customers. The design also needs to be suitable to multiple variants of PMUs, being compatible to general situations or legacy systems. We, thus, make the least assumption on the processing ability of PMUs. That is, their computation ability may be as low as a chip in sensor node, and storage space may be in megabyte magnitude. Thus, our solution can be applied in most architectures and perform better once higher processing platforms are available.

(2) *SGCC*. The control instructions are sent from smart grid control center, denoted as SGCC in this paper. It is a part of control unit of SCADA (or EMS). SGCC usually has enough computation and storage resources.

(3) *Customer*. The customers are always presented or related in smart grid applications; the PMU is not an isolated computing unit (this point is different with sensor node). Thus in security design, the human element could be considered and exploited if needed.

The communication network could be currently available home networks; we do not specify networking settings such as topology and parameters such as bandwidth to make our discussion be suitable in most general situations.

To summarize, we observe that in smart grid, two asymmetry or unbalance present: computation resources in PMUs and in SGCC; uploading and downloading communication volumes. They may affect some subtle tradeoff in design of security schemes. Moreover, human interaction may also be incorporated into the design.

2.2. Attack Model. Similar to the statement in related work [2], traditional communications involve devices that are in areas with physical access controls (such as fences and locked houses), but smart PMUs are deployed in the areas that could be accessible by both consumers and adversaries. Consequently, we have to assume that PMUs are located in a hostile environment and much stronger adversaries exist.

As attackers are assumed to be malicious and intended to tamper the system to gain some profits. For example, attackers may reduce the transmission data such as power consuming value for lower payment; they may also pulse the data in the transmission to corrupt the scheduling strategies; they may pry the communication patterns to speculate the privacy of consumers, such as daily behaviors; they may inject any forgeable data such as consuming value into the communication by manipulating PMUs, or even aim to crash partial or entire SCADA or EMS.

2.3. Security Requirement. The data are generated from PMUs and transmitted into communication networks. To protect such kind of data, security scheme should the fulfill security requirements as follows:

Data Confidentiality. Data confidentiality in transmission should be protected. Otherwise, utility consumption values will be known by attackers, which will leak much information on consumers' behaviors.

Data Integrity. Integrity of the data transferred in communication should be guaranteed so that any modification of the data can be detected.

Data Source Authentication. The source of the data should be verifiable by receivers to confirm the data authenticity and so as to exclude forged data.

Above requirements should be addressed in context of smart grid, or the solution should concern its applicability in smart grid environments. Such security requirements inevitably ask for a prerequisite demand—key management issue. The related keys such as the encryption key, integrity key, or authenticity key can be available and properly protected.

2.4. Design Goal. Based on above observations, we state the design goal as follows:

We search for a highly robust but lightweight scheme to protect data confidentiality, data integrity, and data source authentication in case of the presence of strong attackers and in the context of smart grid. To fulfill such objectives, the prerequisite is how to generate, manage, and refresh underlying keys such as encryption key, integrity key, and authentication key. The encryption key is called session encryption key, denoted as SEK, which is only used for one uploading session of power values. The authentication key and integrity key are combined (or interchangeable) together and is called session integrity key, denoted as SIK, which is also used only for one session. The session period depends on the gathering interval of power values, scheduling policy, and security strength.

Table 1: Notation.

PKS	Public Key based Scheme
MK	Master Key
UID	Unique ID
PMU	Phaser Measurement Units
SGCC	Smart Grid Control Center
SEK	Session Encryption Key
PubK	Public Key
PriK	Private Key
PWS	Password based Scheme
PWD	Password
BVS	Billed Value based Scheme
V	Value of automatic meter readings
ETK	Evolutionary Transportation Key
$\{M\}_K$	Encryption of M using key K
$\|\|$	Concatenation

3. Proposed Schemes

In this section, we investigate a family of schemes for better understanding and explaining motivations. Each latter scheme may improve previous one by addressing some of its limitations in terms of performance or usability, or deal with several subtle tradeoff to achieve better overall performance and security.

We list all major notations used in the remainder of the paper in Table 1.

3.1. Public Key based Scheme—PKS. We firstly propose a basic public key based scheme, called PKS, to illustrate our motivations. To facilitate the encryption and message authentication code, the encryption key and integrity key are required. The naive scheme is using predistributed master key (*MK*) in the PMUs, but this solution has one weakness—if a PMU is compromised, the *MK* in this PMU will be leaked. Therefore, all derived keys from *MK* will be exposed if such derivation is only related to *MK*.

Each PMU has a *MK* that is preloaded into the PMU upon the deployment. PMU always has a unique id, called *UID*, which could be a designated sequence number of the PMU upon deployment and stored in on-chip read-only memory. Similar to *MK*, the UID is also stored by SGCC after the deployment of PMU. Customers are assumed to have a certificated public key generated by certificate authority (CA), usually a trusted third party for smart grid.

The Public Key based scheme (PKS) is described as following stages:

(1) Stage I—Preparation. Before session key establishment, SGCC checks whether the customer's PubK is revoked from Revocation List (RL). If not, go to next stage. Otherwise, stop or choose another scheme.

(2) Stage II—Session key seed establishment.

(2.1) Establishment request (SKER). SGCC selects a random number $R = \{R_1 \| R_2\}$ and sends R that is encrypted by a customer's PubK to PMU. That is,

$$\text{SGCC} \longrightarrow \text{PMU} : \{Tm \| R_1 \| R_2\}_{\text{PubK}}, \quad (1)$$

where Tm is a time stamp denoting current time.

(2.2) Establishment acknowledgement (SKEA). The customer relies her private key (PriK) to decrypt out R, checks whether Tm is in the proper range and sends back as follows:

$$\text{PMU} \longrightarrow \text{SGCC} : \{R_1 + 1 \| R_2 - 1\}_{\text{PriK}}. \quad (2)$$

(3) Stage III—session key generation.

(3.1) SEK generation. The customer uses following method to generate session encryption key: SEK = Hash(R_1‖UID‖MK).

(3.2) SIK generation. The customer uses following method to generate session integrity key: SIK = Hash(R_2‖UID‖MK).

(4) Stage IV—data transmission. The PMU sends power value to SGCC:

$$\text{PMU} \longrightarrow \text{SGCC} : \{V\}_{\text{SEK}}, \{\text{Hash}(V)\}_{\text{SIK}}, \quad (3)$$

where V is a value of meter reading in the last sample period.

Remarks.

(1) Two random values (R_1 and R_2) are used instead of one random value, can protect SEK and SIK independently. The exposure of one random number (i.e., R_1 in SEK or R_2 in SIK) will not result in the leakage of the other.

(2) Tm is used for defending replay attack. If Tm is not in the range, the SKER (session key establishment request) message will be ignored. The replay attack may result in DoS (denial of service) attack to PMUs. It can be mitigated by security policy that is out of the scope of the paper.

(3) SKEA (session key establishment acknowledgement) message confirms the authenticity of PMU and synchronizes the generation of session keys.

(4) SEK generation relies on $\{R_1 \| \text{UID} \| \text{MK}\}$. If MK is compromised by software flaws in program, UID may remain secure due to its hardware compromising hardness (namely, tamper-proofed read-only memory accessed only by PMU). R_1 guarantees the freshness and authenticity of SEK.

(5) The confidentiality and integrity of power data V are guaranteed by SEK and SIK.

Security Analysis. The security of SEK and SIK is guaranteed by the security of PriK. If the PriK is safely possessed, attackers cannot recognize SEK and SIK. UID is used for generating SEK and SIK, which increases the difficulties of hardware tampering by attackers. That is, even if MK is leaked by software compromising, the UID may still sustain secrecy, because it is a hardware extracted value and not easy to be revealed by only software compromising. Moreover, even though the attacker can further reveal UID by hardware scrutiny physically, they cannot be able to possess the PriK simultaneously, as it is securely and personally held by customers. The customers are assumed to safely possess their PriK and only use such keys in session establishment stage. Therefore, the security of SEK and SIK can be guaranteed.

Performance Analysis. We mainly consider performance at PMU side. The session key seed establishment stage induces the operations are 1 public key decryption and 1 public key encryption.

The session key generation stage incurs 2 hash function computation. Data transmission stage has 2 symmetric key encryption and 1 hash function computation. The communication includes two messages for key establishment and one message for data transmission. It shows that the operations in this stage almost remain to being minimized.

Usability and Cost Analysis. PKS involves customers' PriK, so customers usually have to possess some local device such as a USB disk to store such key (that is distributed by third trusted party). It may induce a USB port in PMU attached devices, which increases the cost of PMU devices. It also demands customers to safely possess a portable USB key, which may add customers' burden. The RL (revocation list) must be maintained or synchronized with CA (certificate authority) by SGCC. Or, SGCC will retrieve the RL if RL is only maintained by CA, it will introduce some response delay due to RL retrieval.

The customers are asked for participating the key establishment stage only when session keys are generated or updated. In proposed scheme, the session key establishment (or updating) stage are launched by SGCC, if customers and SGCC previously agree on one or multiple time-slots, for example, each Sunday 10:00 PM, which is only a management issue. If needed, the session key updating request can also be launched by customers, in this case customers may communicate with SGCC offline to negotiate a proper time-slot.

3.2. Password based Scheme: PWS. The public Key based Scheme (PKS) scheme is resilient to software compromise, but it assumes the existence of PKI (Public Key Infrastructure) system. To avoid such a restricted assumption, we propose a password based scheme, called PWS, to improve the flexibility and usability of the proposed solution.

In this scheme, password (denoted as PWD) is induced, which is a easily memorized (at least 8) digits in range $[0,\ 9]$ so that PKI becomes unnecessary. The password are usually selected by customers for their favors so as to be easily memorized. The password usually is uploaded to SGCC off-line, for example, when create or start up the utility account or upon the deployment of PMUs.

The PWS scheme is described as follows:

(1) Stage I—session key seed establishment.

(1.1) Establishment request (SKER). SGCC selects a random number $R = \{Tm \| R_1 \| R_2\}$ and sends R encrypted by the customer's password PWD to PMU. That is

$$\text{SGCC} \longrightarrow \text{PMU} : \{Tm \| R_1 \| R_2\}_{\text{PWD}}, \tag{4}$$

where Tm is current time stamp.

(1.2) Establishment acknowledgement (SKEA). The customer decrypts out R via her PWD, checks whether Tm is in the range, and sends back as follows:

$$\text{PMU} \longrightarrow \text{SGCC} : \{R_1 + 1 \| R_2 - 1\}_{\text{PWD}}. \tag{5}$$

(2) Stage II—session key generation.

(2.1) SEK generation. The customer uses following method to generate session encryption key:

$$\text{SEK} = \text{Hash}(R_1 \| \text{UID} \| \text{MK} \| \text{PWD}). \tag{6}$$

(2.2) SIK generation. The customer uses following method to generate session integrity key:

$$\text{SIK} = \text{Hash}(R_2 \| \text{UID} \| \text{MK} \| \text{PWD}). \tag{7}$$

(3) Stage III—data transmission. The customer sends power value to SGCC as follows:

$$\text{PMU} \longrightarrow \text{SGCC} : \{V\}_{\text{SEK}}, \{\text{Hash}(V)\}_{\text{SIK}}. \tag{8}$$

Enhancement. In PKS scheme, once PriK is exposed, all random number R are revealed. It is appealing that certain previous keys and together ciphertext encrypted by such keys are still safe even if current keys are exposed. This situation is so-called forward secrecy. To further enhance the security of scheme PWS, we propose to use key evolution method. Here, we call the key used for transporting random number R is a transportation key. We propose to use one-time hash value of PWD as the transportation key, and use hash chain as a key evolution strategy.

More specifically, at ith time in Stage I the encrypted key is not PWD but $\text{Hash}^{(i)}(\text{PWD})$, $(i \geqslant 1)$. That is, assuming at the ith time (or session) of transmission of random number R. The two steps in stage I are revised as follows.

(1.1) SGCC selects a random number $R = \{R_1 \| R_2\}$ and sends R to PMU that is encrypted by hashed customer's password. That is,

$$\text{SGCC} \longrightarrow \text{PMU} : \{Tm \| R_1 \| R_2\}_{\text{Hash}^{(i)}(\text{PWD})}. \tag{9}$$

(1.2) The customer uses $\text{Hash}^{(i)}(\text{PWD})$ to decrypt out R, checks whether Tm is in the range, and sends back:

$$\text{PMU} \longrightarrow \text{SGCC} : \{R_1 + 1 \| R_2 - 1\}_{\text{Hash}^{(i)}(\text{PWD})}. \tag{10}$$

In this way, the encryption key for random number transportation will be evolved very time and be used for only once. Even attackers can reveal one encryption key, for example, $\text{Hash}^{(i)}(\text{PWD})$, they cannot conjecture previous encryption keys such as $\text{Hash}^{(j)}$ (PWD) $(1 \leqslant j < i)$. The reason comes from the one-wayness of hash function. That is, given the image of the function, it is computationally infeasible to compute preimage. Therefore, this enhancement guarantees the forward secrecy of the transportation key.

In addition to the introduction of key evolution, a value SALT is further suggested to strengthen the limited length of PWD and defend off-line dictionary attack. As PWD needs to be easily memorized, the length of PWD usually is no longer than 8 digits. To extend the off-line brute force search space, SALT value can be used. The SALT will be safely stored in SGCC and PMU, respectively. The indeed PWD used for key evolution will be $\{\text{PWD} \| \text{SALT}\}$ instead of PWD.

Security Analysis. The security of SEK and SIK is guaranteed by the security of PWD. SGCC is always assumed to securely possess the PWD, as it is in a trusted domain. If PWD is only memorized by consumers and its secrecy is maintained when it is typed on keyboard, attackers cannot recognize SEK and SIK due to the unknownness of PWD. Without PWD, attackers cannot reveal R that is the generating ingredient of session keys (namely, SEK and SIK).

Moreover, UID and MK are incorporated in the generation of SEK and SIK for the similar reason with public key based scheme. Especially, PWD is also proposed to embed into the generation of SEK and SIK, to further enhance the session key's secrecy.

The scheme can further provide forward secrecy of transportation key used for transferring random number R. That is, even a key $\text{Hash}^{(i)}$ (PWD) for encryption of R are exposed, the keys such as $\text{Hash}^{(j)}$ (PWD) $(1 \leqslant j < i)$ still remain secret.

Based on above analysis, the security of SEK and SIK can be guaranteed.

Performance Analysis. The operations induced at PMU side are 1 symmetric key decryption, 1 symmetric key encryption for key establishment, and 2 hash function computation for key generation.

Usability and Cost Analysis. PWS scheme may ask users to plug a small numeric keyboard into PMU attached device or PMU itself incorporates such a numeric keyboard panel, which slightly increases the cost of PMU. Nonetheless, the usability of scheme PWS is better than scheme PKS, as the USB key is not required and numeric keyboard is much cheaper than USB key. The PWD can be reinstated or updated by customers via off-line channel with SGCC.

3.3. Billed Value-Based Scheme: BVS. PWS scheme can further be improved to avoid typing password by customers. We further propose a more lightweight scheme by using billed value. The billed value here means the last billed value for consumed utility. We assume that value is only known by SGCC and PMU, as we assume the utility consumption result is a private information of customers and should be kept secret (that is the underlying goal of proposed schemes). Suppose the billed value is BV, we use Hash(BV) to replace the functionality of PWD in PWS scheme. Note that the BV is always not equal to real-time consuming value V, as the billing period is always longer than data gathering period and billed value is a constant value in last billing period. For example, BV is altered once in one billing period, but the gathering value V is collected by SGCC much more frequently (depending on the control and scheduling strategies). The enhancement rationale for forward secrecy in PWS scheme can also be migrated to BVS scheme. Thus, the proposed BVS scheme is as follows.

(1) Stage I—session key seed establishment.

(1.1) SGCC selects a random number $r = \{R_1 \| R_2\}$ and sends R encrypted by Hash(BV) to PMU. That is,

$$\text{SGCC} \longrightarrow \text{PMU} : \{R_1 \| R_2\}_{\text{Hash}^{(i)}(\text{Hash(BV)})}. \qquad (11)$$

(1.2) Customers use their $\text{Hash}^{(i)}(\text{Hash(BV)})$ to decrypt out R.

(2) Stage II—session key generation.

(2.1) SEK generation. The customer uses following method to generate session encryption key:

$$\text{SEK} = \text{Hash}(R_1 \| \text{UID} \| \text{MK} \| \text{BV}). \qquad (12)$$

(2.1) SIK generation. The customer uses following method to generate session integrity key:

$$\text{SIK} = \text{Hash}(R_2 \| \text{UID} \| \text{MK} \| \text{BV}). \qquad (13)$$

(3) Stage III—data transmission. The customer sends power value to SGCC as follows:

$$\text{PMU} \longrightarrow \text{SGCC} : \{V\}_{\text{SEK}}, \{\text{Hash}(V)\}_{\text{SIK}}. \qquad (14)$$

Enhancement.

(1) The hash functions used in our scheme could be the same function or different functions, depending on the available storage space for implementation of hash function code. We suggest to use different hash functions as it will be more secure. That is, the transportation key is $\text{Hash}_1^{(i)}(\text{Hash}_2(\text{BV}))$.

(2) The synchronization of SGCC and PMU on BV is straightforward if the clock of PMU and SGCC can be strictly synchronized. Normally, the transaction is cutoff at the end of billing period, for example, at the 1:00 AM of the first day of each month. At that moment, the PMU will save this value (also the last uploading value) before 1:00 AM as a billing value. That value is the utility consumption of last payment period. Hence, it performs as a common shared secret between PMU (customer) and SGCC in a natural way, and it is automatically and periodically updated to maintain freshness.

(3) If the clock of PMU is not strictly synchronized, we propose the following policy—multiple transmission of BV. That is, in the first day of each month before 1:00 AM, PMU stores any current V as BV and attaches it to multiple messages. That is,

$$\begin{aligned}\text{PMU} \longrightarrow \text{SGCC} :&\{V \| \text{BV} \| \text{BV}_{\text{TAG}}\}_{\text{SEK}}, \\ &\{\text{Hash}(V \| \text{BV} \| \text{BV}_{\text{TAG}})\}_{\text{SIK}},\end{aligned} \qquad (15)$$

where BV_{TAG} presents a tag for notifying SGCC that the BV is attached.

(4) As the success of update of BV is critical for key synchronization, we propose another policy by using confirmed reply if two-way communication is available (in fact, two-way communication is usually available in smart grid). That is, the two-way messages include confirmation from SGCC on the receipt of BV, as follows:

$$\begin{aligned}\text{PMU} \longrightarrow \text{SGCC} :& \{V \| \text{BV} \| \text{BV}_{\text{TAG}}\}_{\text{SEK}}, \\ &\{\text{Hash}(V \| \text{BV} \| \text{BV}_{\text{TAG}})\}_{\text{SIK}}, \\ \text{SGCC} \longrightarrow \text{PMU} :& \{\text{BV} \| \text{BV}_{\text{TAGACK}}\}_{\text{SEK}}, \\ &\{\text{Hash}(\text{BV} \| \text{BV}_{\text{TAGACK}})\}_{\text{SIK}} .\end{aligned} \qquad (16)$$

(5) In PWS scheme, only forward secrecy of the transportation key are ensured. That is, from $\text{Hash}_2^{(i)}(\text{BV})$ attackers can compute $\text{Hash}_2^{(i+1)}(\text{BV})$, but not $\text{Hash}_2^{(i-1)}(\text{BV})$. To further enhance the secrecy of transportation key, we propose an enhancement method for both forward secrecy and backward secrecy. Here, backward secrecy means that even if the current key is exposed, the future keys cannot be correctly conjectured. Concretely, we propose the

following key evolution strategy, assuming the *i*th transportation of random number R:

$$\begin{aligned} \text{SEED} &\longleftarrow \text{Hash}_2(BV), \\ \{L\|R\} &\longleftarrow \text{SEED}, \\ \text{ETK}_L &\longleftarrow \text{Hash}^{(n+1-i)}(L), \\ \text{ETK}_R &\longleftarrow \text{Hash}^{(i)}(R), \\ \text{ETK} &\longleftarrow \{\text{ETK}_L\|\text{ETK}_R\}, \\ \text{SGCC} &\longrightarrow \text{PMU}: \{R_1\|R_2\}_{\text{ET}K}, \end{aligned} \tag{17}$$

where ETK means evolutionary transportation key, used for the transportation of random number R.

In this way, the encryption key for random number will be changed very time and be used for only once. Even attackers can reveal one encryption key, for example, $\text{Hash}^{(n+1-i)}(L)$, they cannot conjecture future encryption keys such as $\text{Hash}^{(n+1-j)}(L)(i < j < n)$. The reason is the one-wayness of hash function. Therefore, the backward secrecy of transportation key ETK is guaranteed. Besides, the value of n is stored in the table of database in SGCC and preloaded into PMU.

(6) As the key is updated in bidirections to provide forward and backward secrecy, the backward secrecy needs the predetermination of maximal evolution times $n + 1$. If the maximal number is reached, or if sampling times i is increased to $n + 1$ within one billing period, we propose to update BV by using $\text{BV} \leftarrow \text{Hash}_2(\text{BV})$ and reset i to 1. The updating period of transporting key result in the alternation of random number R, and further SEK and SIK. The updating period depends on the security policy and data gathering frequency.

(7) In one billing period, all SEKs and SIKs are generated by different random number R that are transported using the derived keys from same BV. As key evolution is involved, the loss of synchronization of i at PMU and SGCC in one billing period will result in the decryption failure of random number R at the PMU side. The minor adjustment can solve this problem. At SGCC side, the random number could have some relation between R_1 and R_2, for example, $R = \{R_1\|R_2 = \text{Hash}_1(R_1)\}$. At PMU side upon receipt of $\{R_1\|R_2\}_{\text{ETK}}$, PMU will decrypt it with supposed ETK. If decrypted value presents the designated relation, the synchronization is maintained.

(8) As the security of BV is critical for BVS scheme, we also propose some strategies to protect BV's secrecy. The secret BV can be a function of public BV. We leave some flexibility of BV value's customized tuning. For example, customers can select a policy on how to generate secrete BV from public BV value, when paying for the utility, and upload the selection into SCADA. Such policy could be an option in policy list. The synchronization of BV between PMU and SCADA can be confirmed by customers upon paying for the utility bill and checking PMU. We assume PMU has a screen to display assumed BV when customers type designated on-board button, and customer can also upload PMU her selected policy by pressing the same button. The public BV will not lead to the exposure of secrete BV, unless corresponding policy is exposed.

Security Analysis. The basic analysis is similar to PWS scheme. The security of SEK and SIK is guaranteed by the security of BV, which is assumed to be the private information of customers. The one-time usage of BV derived encryption key improve the confidentiality of random number, which is an ingredient of SEK and SIK. Together with UID, MK and BV, the security of SEK and SIK can be guaranteed.

Especially, the bidirection hash-chain based derivation guarantees both forward and backward secrecy of the transportation key ETK, so both forward and backward secrecy of R are maintained. As R is the seed of session key SEK and SIK, the both forward and backward secrecy of session keys are guaranteed.

Performance Analysis. The scheme induces the operations are 1 symmetric key encryption, symmetric key decryption, 2 hash function computation. The SEK and SIK generation requires a one-way message from SGCC to PMU. Besides, the enhancement induces more computation, but all are hash function calculation that have low overhead.

Usability and Cost Analysis. Last available BV value can be stored in SGCC and PMU, so customers do not need to remember a password. The security of BV is critical, so it may save in some separated devices such as on-chip rewritable memory to protect its secrecy.

4. Analysis

4.1. Security Analysis. We state the analysis formally by presenting following propositions.

Proposition 1. *If PriK is secretly possessed, PKS will be secure.*

Proof. If PriK is secretly possessed, R will remain secure. If R is secret, computation of SEK and SIK is equivalent to random guess due to the one-wayness of hash function. Thus, if SEK is a secret, the data secrecy of V will be ensured. If SIK is a secret, the message integrity and message source authentication will be ensured. The reason is the one wayness of hash function and the secrecy of SIK. □

Proposition 2. *If PWD is maintained secret, the scheme PWS will achieve security goals.*

Proof. Straightforward. □

Definition 3. Forward secrecy. Given a key K, it is computationally infeasible to conjecture K_f, where K_f is the key before last key evolution. That is, $|\Pr\{K_f \mid K, K \leftarrow f(K_f)\} - \Pr\{K_f\}| < \epsilon(n)$, where $\epsilon(n)$ is a negligible polynomial related to a security parameter n. n usually is the security strength in length. $f(\cdot)$ is the key evolution function. $\Pr\{K_f\}$ denotes the probability of revealing K_f.

Definition 4. Backward secrecy. Given a key K, it is computationally infeasible to conjecture K_b, where K_b is the key after key evolution. That is, $|\Pr\{K_b \mid K, K_b \leftarrow f(K)\} - \Pr\{K_b\}| < \epsilon(n)$, where $\epsilon(n)$ is a negligible polynomial related to security parameter n. n usually is the security strength in length. $f(\cdot)$ is the key evolution function. $\Pr\{K_b\}$ denotes the probability of revealing K_b.

Lemma 5. *One-way function is sufficient for forward secrecy, and necessary for forward secrecy if only one evolutionary key is stored and shared by communication peers.*

Proof. The proof for sufficient condition is straightforward. Next, we proof it is a necessary condition. As only one evolutionary key is stored and shared at communication peers, denoted as K, the next generated key is the function of K. That is, $K_f = f(K)$, where $f(\cdot)$ is a function taking as input K. If $|\Pr\{K_f \mid K\} - \Pr\{K_f\}| = 0$, we have $\Pr\{f(K) \mid K\} = \Pr\{f(K)\}$. $f(\cdot)$ is thus a real random number generation, for example, randomly sample function from a key space. In other words, $f(K) = K_f, (K_f \leftarrow_r \{0,1\}^{|K|})$, where $\leftarrow_r$ means random selection. As communication peers use key evolution for secure communication, they have to maintain holding a shared secret after key evolution. Thus, if $f(\cdot)$ is a real random number generation (RNG), the key evolution is unserviceable because the shared pairwise secret is lost. To maintain holding shared secret after key evolution, it needs to satisfy $|\Pr\{K_f|K\} - \Pr\{K_f\}| < \epsilon(n)$, where $\epsilon(n)$ is a negligible polynomial related to security parameter $n = |K|$. Therefore, $f(\cdot)$ has to take as input K and must has one-wayness, as desired. □

Proposition 6. *BVS has optimal forward and backward secrecy.*

Proof. For forward and backward security, one-way function is required. BVS guarantees forward and backward security by using only single one-way function. The first half key is generated by forward secure key evolution method; the other half key is generated by backward secure key evolution method. Due to the one-wayness of one-way function, the reveal of key after key evolution can only be done by random guess. Suppose $\mathrm{ETK}_L = L_1, \mathrm{ETK}_R = L_2$. That is, $\Pr\{K_b \mid K, K_b \leftarrow f(K)\} = 1/2^{L_1}$, and $\Pr\{K_f \mid K, K \leftarrow f(K_f)\} = 1/2^{L_2}$. Besides, $L_1 + L_2 = |K| = n$. Thus, $\Pr\{K_f, K_b \mid K, K \leftarrow f(K_f), K_b \leftarrow f(K)\} = 1/2^{L_1} \times 1/2^{L_2} = 1/2^{L_1+L_2} = 1/2^n$. Thus BVS has forward and backward secrecy.

Next, we proof it is optimal. If we define overall security strength is the minimum of backward secrecy strength and forward secrecy strength, the key revealing probability will be $\mathrm{MAX}\{1/2^{L_1}, 1/2^{L_2}\}$. Thus, when $L_1 = L_2 = |K|/2$, the overall secrecy strength achieves an optimal strength $1/2^{n/2}$. □

Table 2: Scheme comparison.

Scheme	Security	Performance (PMU side)	Usability
PKS	PriK	PKD + Hash	PKI + USB Key
PWS	PWD + forward security	SKD + Hash	Keyboard
BVS	BV + forward + backward security	SKD + Hash	/

Above proof is valid even for any attack model for communication link (of course, we only consider any attack models that have finite computational ability, namely, polynomial attackers).

Proposition 7. *Scheme PKS is not forward secure, but scheme PWS is forward secure.*

Proof. Straightforward. □

Proposition 8. *Scheme PWS is not backward secure, but scheme BVS is forward and backward secure.*

Proof. In BVS scheme, $\mathrm{ETK}_L \leftarrow \mathrm{Hash}^{(n+1-i)}(L)$. On one hand, if ETK_L is exposed, attacker cannot conjecture future encryption keys $\mathrm{Hash}^{(n+1-j)}(L)(i < j < n)$. Thus, the backward secrecy are guaranteed. On the other hand, if $\mathrm{ETK}_R \leftarrow \mathrm{Hash}^{i}(R)$ is exposed, attacker cannot conjecture future encryption keys $\mathrm{Hash}^{(j)}(R)(j < i)$. Thus, the forward secrecy is ensured. Hence, either ETK_L or ETK_R cannot be conjectured. ETK, thus, has forward secrecy and backward secrecy, as desired. □

4.2. Performance Analysis. The additional computation of BVS only involves hash functions, so the computational cost is manageable. The hash function codes can be reused. For example, one hash function is SHA256; the other is SHA512. The incurred storage for codes is also lightweight. As hash function is typical lightweight cryptographic primitives, it is also extensively applied in computing platforms with much lower computational ability than PMU such as RFID tag [20]. Moreover, the hardware implementation of hash functions has competitive performances [21–23], which further guarantee the applicability of hash functions in PMUs.

Regarding the usability, BVS has the best performances. It has no requirement for PKI comparing with PKS scheme and has no requirement for password inputting device comparing with PWS scheme. We list the comparisons between three schemes in Table 2. (Acronym: PKD—public key decryption and SKD—symmetric key decryption.)

5. Conclusion

In this paper, we proposed a family of lightweight security schemes for session key seed establishment and session key generation to guarantee data secrecy, data integrity, and data source authentication in communications from PMUs to SGCC (SCADA or EMS control center). We proposed public key based scheme (PKS) and password based scheme (PWS) for different application scenarios. Billed value-based scheme (BVS) was proposed and emphasized, as it can achieve forward and backward security by only relying on hash functions and has appealing usability or flexibility. Security and performance analysis justified that the proposed scheme BVS can achieve forward and backward secrecy with lightweight hash function computation.

Acknowledgments

This work was supported by Special Fund for Basic Scientific Research of Central Colleges, China University of Geosciences (Wuhan) under Grant no. 090109, Major State Basic Research Development Program of China (973 Program) (no. 2007CB311203), National Natural Science Foundation of China (no. 60821001), and Ph.D. Programs Foundation of Ministry of Education of China (no. 20070013007).

References

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

[2] H. Khurana, M. Hadley, N. Lu et al., "Smart-grid security issues," *IEEE Security and Privacy*, vol. 8, no. 1, pp. 81–85, 2010.

[3] F. Boroomand, A. Fereidunian, M. A. Zamani et al., "Cyber security for smart grid: a human-automation interaction framework," in *Proceedings of the IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe '10)*, pp. 1–6, November 2010.

[4] S. Clements and H. Kirkham, "Cyber-security considerations for the smart grid," in *Proceedings of the 2010 IEEE Power and Energy Society General Meeting (PES '10)*, pp. 1–5, September 2010.

[5] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99–107, 2010.

[6] D. Wei, Y. Lu, M. Jafari et al., "An integrated security system of protecting smart grid against cyber attacks," in *Proceedings of the Innovative Smart Grid Technologies (ISGT '10)*, pp. 1–7, 2010.

[7] M. Amin, "Challenges in reliability, security, efficiency, and resilience of energy infrastructure: toward smart self-healing electric power grid," in *Proceedings of the IEEE Power and Energy Society General Meeting (PES '08)*, pp. 1–5, Pittsburgh, Pa, USA, July 2008.

[8] G. N. Ericsson, "Cyber security and power system communication—essential parts of a smart grid infrastructure," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1501–1507, 2010.

[9] J. T. Seo and C. Lee, "The green defenders," *IEEE Power and Energy Magazine*, vol. 9, no. 1, pp. 82–90, 2011.

[10] J. Kim and J. Lee, "A model of stability," *IEEE Power and Energy Magazine*, vol. 9, no. 1, pp. 75–81, 2011.

[11] K. M. Rogers, R. Klump, H. Khurana, A. A. Aquino-Lugo, and T. J. Overbye, "An authenticated control framework for distributed voltage support on the smart grid," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 40–47, 2010.

[12] Y. Wang, I. R. Pordanjani, and W. Xu., "An event-driven demand response scheme for power system security enhancement," *IEEE Transactions on Smart Grid*, vol. 2, no. 1, pp. 23–29, 2011.

[13] K. Moslehi and R. Kumar, "A reliability perspective of the smart grid," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 57–64, 2010.

[14] Y. Wang, W. Li, and J. Lu, "Reliability analysis of wide-area measurement system," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1483–1491, 2010.

[15] J. Ma, P. Zhang, H. j. Fu et al., "Application of phasor measurement unit on locating disturbance source for low-frequency oscillation," *IEEE Transactions on Smart Grid*, vol. 1, no. 3, pp. 340–346, 2010.

[16] K. Budka, J. Deshpande, J. Hobby et al., "Geri—bell labs smart grid research focus: economic modeling, networking, and security amp; privacy," in *Proceedings of the 1st IEEE International Conference on Smart Grid Communications (SmartGridComm '10)*, pp. 208–213, November 2010.

[17] A. Vaccaro, M. Popov, D. Villacci, and V. Terzija, "An integrated framework for smart microgrids modeling, monitoring, control, communication, and verification," *Proceedings of the IEEE*, vol. 99, no. 1, pp. 119–132, 2011.

[18] T. Zhang, W. Lin, Y. Wang et al., "The design of information security protection framework to support smart grid," in *Proceedings of the 2010 International Conference on Power System Technology (POWERCON '10)*, pp. 1–5, 2010.

[19] T. M. Overman and R.W. Sackman, "High assurance smart grid: smart grid control systems communications architecture," in *Proceedings of the 1st IEEE International Conference on Smart Grid Communications (SmartGridComm '10)*, pp. 19–24, November 2010.

[20] T. L. Lim and Y. Li, "A security and performance evaluation of hash-based rfid protocols," in *Proceedings of the 5th China International Conferences on Information Security and Cryptology (Inscrypt '09)*, vol. 5487 of *Lecture Notes in Computer Science*, pp. 406–424, 2009.

[21] A. L. Selvakumar and C. S. Ganadhas, "The evaluation report of sha-256 crypt analysis hash function," in *Proceedings of the International Conference on Communication Software and Networks (ICCSN '09)*, pp. 588–592, June 2009.

[22] B. Baldwin, A. Byrne, M. Hamilton et al., "FPGA implementations of SHA-3 candidates: cubehash, grostl, lane, shabal and spectral hash," in *Proceedings of the 12th Euromicro Conference on Digital System Design: Architectures, Methods and Tools, (DSD '09)*, pp. 783–790, Patras, Greece, August 2009.

[23] N. Sklavos and P. Kitsos, "Blake hash function family on fpga: from the fastest to the smallest," in *Proceedings of the 2010 IEEE Computer Society Annual Symposium on VLSI (ISVLSI '10)*, pp. 139–142, September 2010.

Hindawi Publishing Corporation
International Journal of Digital Multimedia Broadcasting
Volume 2011, Article ID 926363, 12 pages
doi:10.1155/2011/926363

Research Article

Building Automation Networks for Smart Grids

Peizhong Yi, Abiodun Iwayemi, and Chi Zhou

Electrical and Computer Engineering Department, Illinois Institute of Technology, Chicago, IL 60616-3793, USA

Correspondence should be addressed to Chi Zhou, zhou@iit.edu

Received 2 November 2010; Accepted 2 April 2011

Academic Editor: Robert C. Qiu

Smart grid, as an intelligent power generation, distribution, and control system, needs various communication systems to meet its requirements. The ability to communicate seamlessly across multiple networks and domains is an open issue which is yet to be adequately addressed in smart grid architectures. In this paper, we present a framework for end-to-end interoperability in home and building area networks within smart grids. 6LoWPAN and the compact application protocol are utilized to facilitate the use of IPv6 and Zigbee application profiles such as Zigbee smart energy for network and application layer interoperability, respectively. A differential service medium access control scheme enables end-to-end connectivity between 802.15.4 and IP networks while providing quality of service guarantees for Zigbee traffic over Wi-Fi. We also address several issues including interference mitigation, load scheduling, and security and propose solutions to them.

1. Introduction

The smart grid is an intelligent power generation, distribution, and control system. It enhances today's power grid with intelligence, bidirectional communication capabilities and energy flows [1]. These enhancements address the efficiency, stability, and flexibility issues that plague the grid at present. In order to achieve its promised potential, the smart grid must facilitate services including the wide-scale integration of renewable energy sources, provision of real-time pricing information to consumers, demand response programs involving residential and commercial customers, and rapid outage detection. All these tasks demand the collection and analysis of real-time data. This data is then used to control electrical loads and perform demand response.

In order to obtain the full benefit of smart grids, their communication infrastructure must support device control and data exchanges between various domains which comprise the smart grid. The smart grid must be allied with smart consumption in order to achieve optimum power system efficiency. This necessitates the integration of smart buildings, appliances, and consumers in order to reduce energy consumption while satisfying occupant comfort. Building automation systems (BASs) already provide this intelligence, enabling computerized measurement, control and management of heating, ventilation, air-conditioning (HVAC), lighting, and security systems to enhance energy efficiency, reduce costs, and improve user comfort. Buildings consume 29% of all electricity generated in the United States [2]; therefore, the ability of BASs to communicate and coordinate with the power grid will have a tremendous effect on grid performance. Home area networks (HANs) provide similar capabilities for residential buildings. They facilitate the interconnection of smart appliances with smart meters to automatically regulate residential electricity usage and respond to pricing signals from the utility [3].

Zigbee is a low cost, low power, low data rate and short-range communication technology based on the IEEE 802.15.4 standard. United States National Institute for Standards and Technology (NIST) has defined Zigbee and the Zigbee smart energy profile (SEP) as the one of the communication standards for use in the customer premise network domain of the smart grid [4]. However, due to Zigbee's limited transmission range, it must be a combined with longer-range communication technologies such as IEEE802.11 in order to provide end-to-end connectivity across the smart grid.

In this paper, we discuss the different issues relevant to communication infrastructures for building automation system in smart grid. We begin with an introduction of whole system architecture of a smart grid system based on a perfect power system [5] including premises networks, field area networks, and a power system controller. We designed and implemented a Zigbee-based building energy management testbed system. Our system integrates a Zigbee-enhanced building automation system with the smart grid to harness energy management schemes such as demand response, real-time power pricing, peak load management, and distributed generation. We also propose a quality of service (QoS) aware 802.15.4/802.11 interoperability framework for home area network and building area network (BAN) which prioritizes wireless sensor network (WSN) traffic over Wi-Fi networks. In our scheme, WSN packets are classified according to their QoS requirements. They are then aggregated and tunneled over the Wi-Fi to the BASs server. We also proposed a frequency agility-based interference mitigation scheme to avoid interference from neighboring Wi-Fi networks. Distributed load scheduling based on optimal stopping rules [6] was proposed in the paper which can reduce the peak load and adjust utility operation time based on electricity pricing and waiting time. We also discuss open issues including security and data compression.

The rest of paper is organized as follows. Section 2 describes a smart grid system architecture. In Section 3, the Zigbee-based building energy management system was introduced. Our proposed QoS-aware 802.15.4/802.11 interoperability framework is presented in Section 4. Frequency-agility-based interference mitigation algorithm is proposed in Section 5. Section 6 presents our proposed optimal stopping rule-based distributed load scheduling scheme. Several open issues including smart grid security and data compression discussed in Section 7. Finally, the paper is concluded in Section 8.

2. System Architecture

The smart grid is the convergence of information technology, communications, and power system engineering to provide a more robust and efficient electrical power system [7]. Smart grids consist of sensing, communication, control, and actuation systems which enable pervasive monitoring and control of the power grid [8]. These features enable utilities to accurately predict, monitor and control the electricity flows throughout the grid. They also transform the power grid into a bidirectional power system in which customers can supply as well as receive power from the grid, converting the grid into a distributed power generation system [9].

The smart grid utilizes the hierarchical structure detailed in [8] and displayed in Figure 1. The foundation of this structure is the power system infrastructure consisting of power conversion, transportation, consumption, and actuation devices. They include power plants, transmission lines, transformers, smart meters, capacitor banks, reclosers, and various devices. Smart meters enable bidirectional power flows between utilities and consumers, enabling consumers to produce and supply energy to the grid, thereby becoming “prosumers”. This development promises significant improvements in power system reliability, as alternative power sources can supply the grid during utility power outages. It also increases system efficiency, as line losses due to long-distance transmission are eliminated. These smart grid capabilities will foster greater incorporation of renewable energy sources such as wind and solar power into the grid, thereby reducing the dependence on fossil-fuel power generation and reducing greenhouse gas emissions.

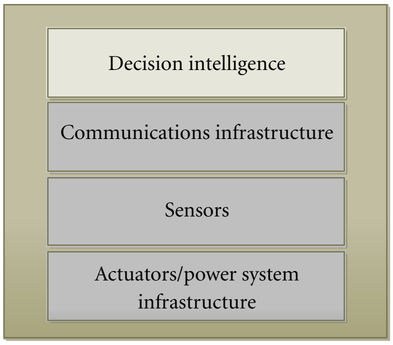

Decision intelligence
Communications infrastructure
Sensors
Actuators/power system infrastructure

Figure 1: Smart grid structure.

The second layer of the smart grid architecture is the sensors. Power system reliability is significantly improved via embedded sensors distributed throughout nodes within the power system. These sensors enable real-time fault detection and isolation via bidirectional digital communication links. They also provide granular system health data that can be used for rapid system analysis, fault preemption, and trending. Smart meters also provide users and utilities with real-time power consumption data and enable the remote monitoring and control of building loads and home appliances. Consumers can also receive real-time pricing information to facilitate informed decision making.

The communications infrastructure is the glue that binds all these various layers together and consists of wide, local building and home area networks. They consist of broadband technologies such as 802.16 WiMAX, 802.11 Wi-Fi, optical fiber, 802.15.4/Zigbee, and power line carrier schemes. Zigbee has found great application in smart metering, home, and building automation control due to its low-cost, flexibility, wide-spread support, and intervendor interoperability.

At the top of the system is the decision intelligence block which encompasses substation automation, fault-management, load distribution, and other control strategies deployed to guarantee power system stability and balance power demand and supply.

The smart grid concept has been extended to smaller smart grid networks known as smart microgrids. A smart microgrid is a localized smart grid covering specific geographical regions, such as suburban neighborhoods or university campuses, and incorporating local or onsite power generation.

Building automation systems provide centralized and automated management of major or critical loads within building. Building automation aims to reduce energy costs, improve energy efficiency and facilitate off-site building management [10–12]. The primary requirements for building automation applications are low cost, ease of installation, and flexibility/reconfigurability.

Table 1: Zigbee radio frequency characteristics.

Frequency	Region	Modulation scheme	Bit rate (kbps)	Channels	Channel spacing
868 MHz	Europe	BPSK	20	1	N/A
915 MHz	America and Asia	BPSK	40	10	2 MHz
2.4 GHz	Global	O-QPSK	250	16	5 MHz

3. Zigbee-Based Home Automation

3.1. Zigbee/IEEE 802.15.4. Zigbee is a low-rate, low-power, wireless personal area networking scheme [10] based on the IEEE 802.15.4 standard. It is designed for short-distance communication and supports a maximum data rate of 250 kbps without encryption.

Zigbee devices are ideal for smart grid and building automation applications, because they are wireless, low cost, and robust. Wireless nodes also provide flexibility, easy re-deployment, and reconfiguration. The integration of Zigbee radios with light switches, occupancy sensors, temperature sensors, and smoke detectors enables measurement and control of all the building loads. The low power consumption of Zigbee is achieved by very low system duty cycles, with typical Zigbee nodes having duty cycles of less than 5%. The result is significant energy savings and greater comfort for building occupants [13, 14]. Details of Zigbee's radio frequency characteristics, frequency bands, and modulation schemes are provided in Table 1.

3.2. Home Automation System. We developed a Zigbee-based home automation system [15] in order to demonstrate the utility of Zigbee-based home automation networks. Two-way communication was used to transmit readings from Zigbee end nodes to a data collection and control center (DCCC) and to pass control messages from the DCCC to the end nodes. Each end node is able to relay the collected data to the DCCC via distributed Zigbee routing nodes. The test bed architecture is shown in Figure 2. The Zigbee coordinator aggregates received data for display and processing and transmits control signals to the end nodes according to the selected power management strategy.

3.2.1. The Data Collection and Control Center (DCCC). The DCCC serves as the system controller, receiving input from the various sensors along with real-time power pricing. It also manages the loads for energy efficiency, demand response, and cost savings. A screenshot of the DCCC's user interface is shown in Figure 3. The DCCC is developed in MATLAB and utilizes a GUI front end to communicate directly with the Zigbee network coordinator and remote actuator modules. The DCCC provides the following functions:

(i) the display of received sensor data (temperature, light levels, room occupancy, etc.),

(ii) remote control of Zigbee modules,

(iii) user configuration of timing, pricing, and sensor data threshold values,

(iv) control of externally connected loads on the basis of user-determined price thresholds, time of day, and sensor readings,

(v) lighting control based on room occupancy and other variables.

3.2.2. Hardware System. Our hardware system consists of several meshbean Zigbee motes which we programmed to support the following functions:

(i) demand response,

(ii) lighting control,

(iii) ambient temperature sensing and control.

As shown in Figure 4, these modules combine an ATMEL 1281 V low-power microcontroller with 8 K of RAM and 128 kB of flash memory, an ATMEL RF230 Zigbee radio, onboard light and temperature sensors in a single battery-powered module with a USB interface. More details of our scheme can be found in [15].

4. Interoperability of Zigbee and Wi-Fi

Building and home area networks are only one of a variety of networks that make up the smart grid. Due to the multiplicity of networks and protocols within the smart grid, interoperability is a key issue. The availability of an interoperability framework is essential to end-to-end communication across and within smart grid domains, so a significant amount of work is being invested in interoperability frameworks for the smart grid.

The usage of IP within wireless sensor networks facilitates easy interconnectivity with existing networks, enables the re-use of existing TCP/IP protocols, tools, and programming paradigms, and permits the usage of IP friendly protocols such as BACnet and Modbus over WSN nodes. These goals sparked research into the use of IPv6 over WSNs, as the ability to connect even tiny wireless sensor nodes to the internet would facilitate ubiquitous computing in the home and throughout the smart grid.

Interconnection between WSNs and TCP/IP networks has primarily been by means of gateways [16], as it had been assumed that TCP/IP was too memory and bandwidth intensive for usage in resource constrained wireless sensor networks [17]. However, the development of uIP, the first lightweight IP stack for WSNs [18] demonstrated the viability of IP for wireless sensor networks and led to a flurry of work into on the use of IP for WSNs. The 6LoWPAN IETF standard defines a framework for deployment of IPv6 over IEEE 802.15.4 networks [19] by means of header compression and routing and forwarding at layers 3 and 2, respectively. This work is extended in [20] to address issues such as link duty cycling, network bootstrapping and node discovery to create a complete IPv6 architecture for WSNs.

The primary interconnection schemes proposed for connecting Zigbee WSNs to the Internet are proxy-based

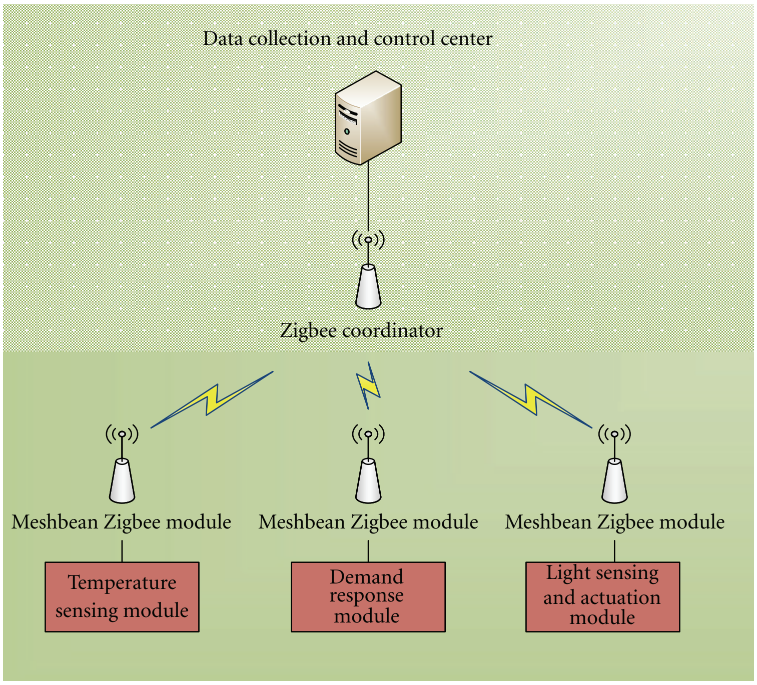
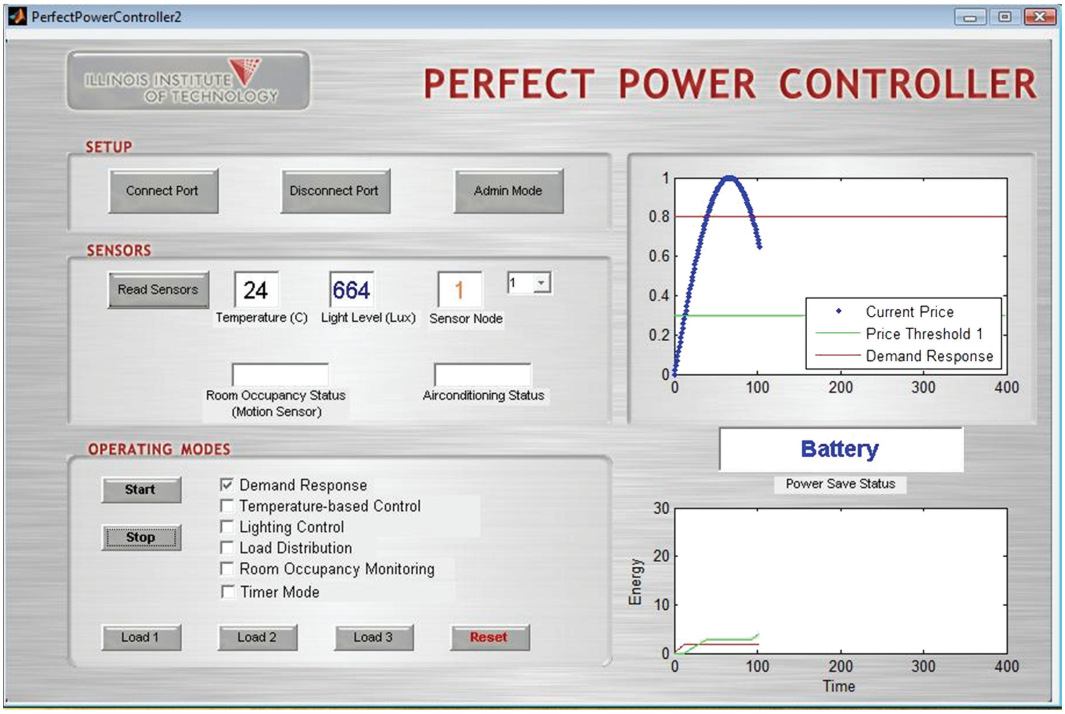


Figure 2: Zigbee HAN demonstration system architecture.



Temperature (C): 24

Light Level (Lux): 664

Sensor Node: 1

Room Occupancy Status (Motion Sensor):

Airconditioning Status:

☑ Demand Response
□ Temperature-based Control
□ Lighting Control
□ Load Distribution
□ Room Occupancy Monitoring
□ Timer Mode

Power Save Status: Battery

Figure 3: Perfect power controller GUI.

gateways [16, 21, 22] and sensor stack schemes [20, 23]. The issue of the inability of Zigbee to natively support IP is addressed by the compact architecture protocol (CAP) [24] in which the authors create a framework to enable the usage of Zigbee application layer protocols over any IP-capable network. We extend their work by creating a framework for interworking between Zigbee and Wi-Fi networks in HANs and BANs while providing QoS guarantees. The proposed interoperability network architecture is shown in Figure 5. Taking into consideration BASs application requirements, reliability and short delay are two most important factor related to the performance. In [25], the authors present

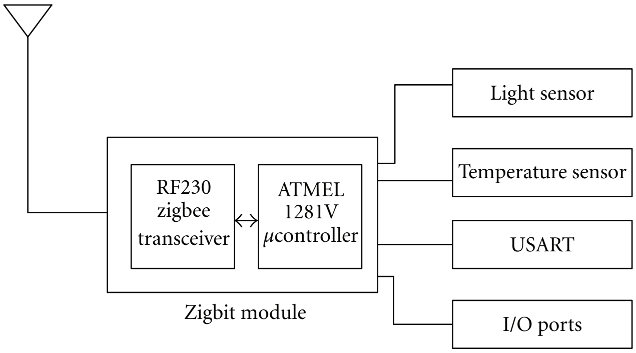


Figure 4: Meshnetics meshbean module block diagram.

an architecture for a medical information system which integrates WLAN and WSNs. In [26, 27], several QoS-enabling mechanisms present in the IEEE 802.11e provide us some ideas to design the frame work of the integration system. A two-tiered WSN and WLAN scheme with QoS guarantees is provided in [28], but the authors do not address IP-based interoperability.

4.1. Interworking. Interoperability is "The capability of two or more networks, systems, devices, applications, or components to exchange and readily use information—securely, effectively, and with little or no inconvenience to the user" [29]. The grid-wise architecture council (GWAC) [30] has defined an 8-layer interoperability framework encompassing all the facets of interoperability. Our primary focus is the 4 lowest layers of this framework (Figure 6), and we utilize it to develop an interoperability framework for HANs and BANs.

The internet engineering task force (IETF) 6LoWPAN working group defined the IPv6 over low-power wireless personal area networks (6LoWPAN) protocol to facilitate the use of IPv6 over low power and low data rate WSNs [31]. It was initially designed for usage over the 802.15.4 physical (PHY) and medium access layer (MAC) layers but can be extended for use over other PHY and MAC architectures (Figure 6).

In order to use IPv6 over 802.15.4 networks, an adaptation layer between the 802.15.4 data link and network layers [17] was developed to provide the following functions:

(i) stateless compression of IPv6 headers by means of HC1 compression [19] to reduce their size from 40 bytes to approximately 4 bytes, thereby reducing transmission overhead,

(ii) fragmentation and reassembly scheme to support the transmission of IPv6 packets over 802.15.4 frames. This is required as the minimum MTU of IPv6 packets is 1280 bytes, while the maximum size of a 802.15.4 frame is 127 bytes.

The benefits of 6LoWPAN over competing WSN implementations are its ease of connectivity with IP networks and its large addressing space (2^{128} compared with 2^{16} for Zigbee). In addition, the concept of device roles found in Zigbee is not applicable, with each device serving as a router for its neighbor's traffic. Unlike Zigbee, 6LoWPAN permits duty cycling of routers, thereby extending device lifetime. The primary drawback of 6LoWPAN is its incompatibility with Zigbee, Zigbee's significant industry support, and very strong device interoperability guarantees across multiple vendors. A combination of the flexibility of IP networking and 6LoWPAN's power saving schemes with Zigbee's application profiles would marry the best features of both implementations to provide an industry standard, interoperable framework for HANs and BANs [32].

The compact application protocol (CAP) details a mapping of the Zigbee application layer to UDP/IP primitives [32, 33], permitting the usage of Zigbee application profiles over any IP capable network [24]. This removes the Zigbee application layer (ZAL) dependency on the Zigbee network layer and the 802.15.4 PHY and MAC layers. As shown in Figure 7, it preserves the excellent application layer interoperability features of public Zigbee application profiles while enabling end to end interoperability across the HAN/BAN using Wi-Fi, 802.15.4, and Ethernet. Rather than transmitting APS frames to the Zigbee network (NWK) layer for transmission to other nodes across the network using Zigbee addresses, the APS frames are now carried over UDP frames, necessitating modification to the addressing scheme to support communication with IP hosts using IP addresses and port numbers.

CAP is composed of four modules which correspond to the Zigbee application support sublayer (APS), Zigbee device objects (ZDO), Zigbee cluster library (ZCL), and APS security modules. The lowest layer of CAP is the Core module, which corresponds to the Zigbee APS layer. It frames data packets for transmission across the network, but now APS layer frames will be sent in UDP datagrams rather than in Zigbee NWK layer frames. In order to achieve this, Zigbee application profiles are rewritten to replace each Zigbee short (16-bit) and long (64-bit) address entry with a CAP address record. This consists of an IP address and UDP port pair, or a fully qualified domain name and UDP port number.

The data protocol is used to exchange data items and commands between communicating peer nodes. It encapsulates the ZCL and allows it to be used without modification, providing full ZCL support. The management protocol encapsulates Zigbee device profile (ZDP) command messages which are handled by the ZDO module, and provides service and device discovery and binding functionality. The final module is the security module which provides the same services as the APS security layer and is used to encrypt APS frames for secure transmission.

4.2. Gateway Router. Zigbee networks are primarily used for periodic data collection of low-bandwidth sensor and alarm data, while Wi-Fi networks support a variety of services with varying quality of service requirements. Based on this, a differential service medium access control scheme [25] is required to guarantee timely and reliable delivery of Zigbee traffic over building Wi-Fi networks. Thus, we design an enhanced distributed channel access-(EDCA-) based QoS model to achieve this.

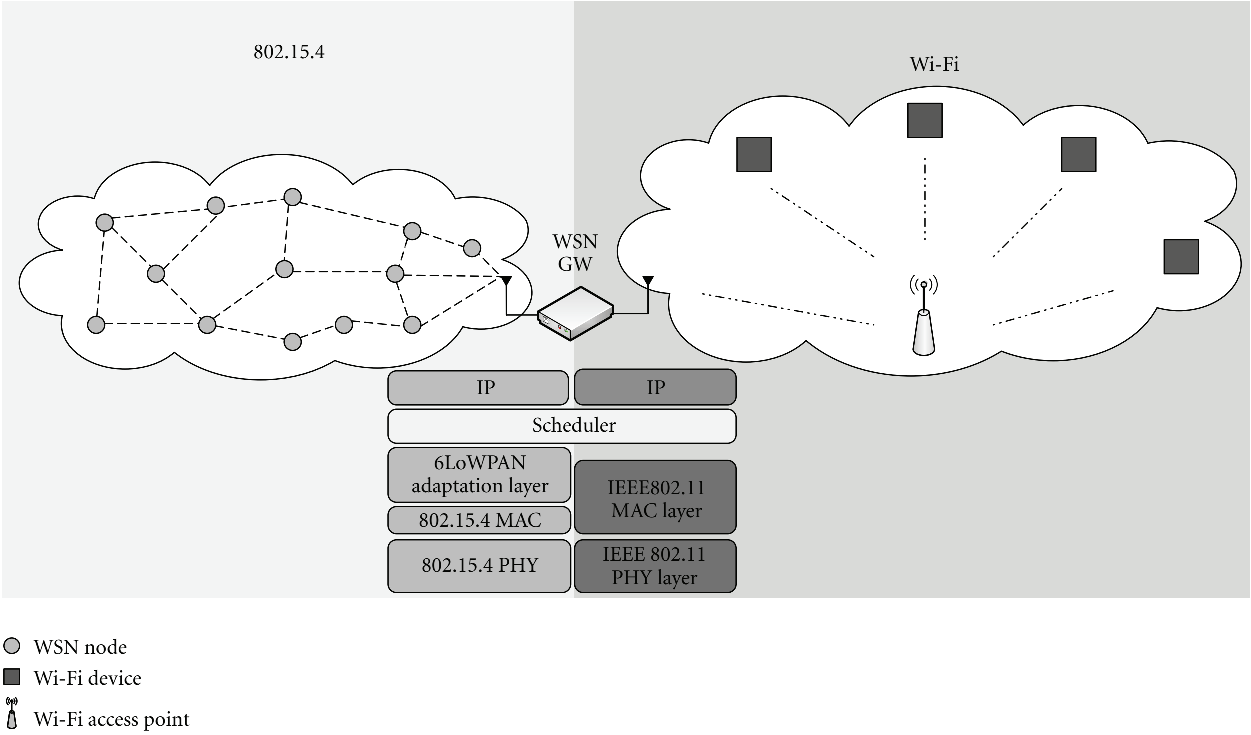


Figure 5: Interoperability network architecture.

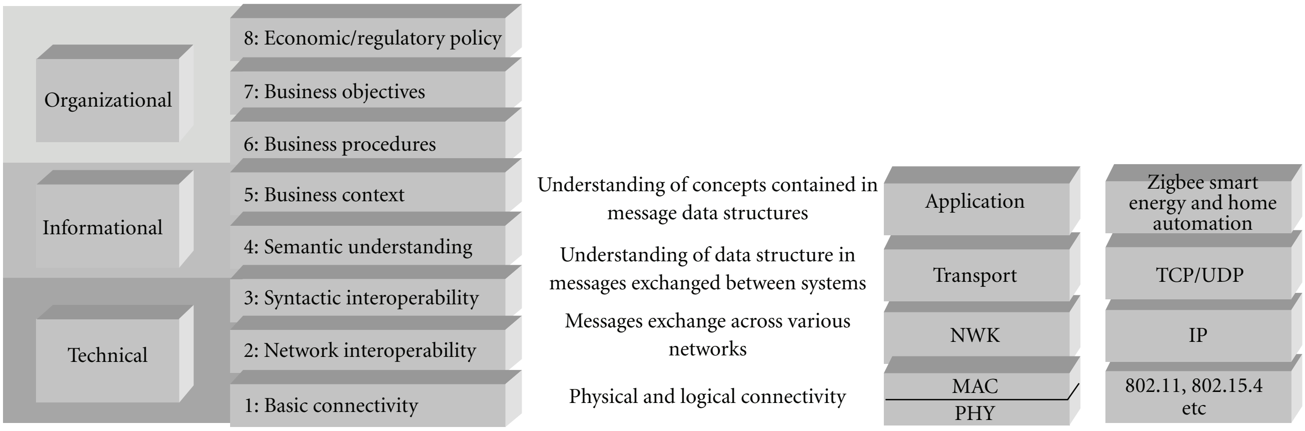

Organizational
Informational
Technical
8: Economic/regulatory policy
7: Business objectives
6: Business procedures
5: Business context
4: Semantic understanding
3: Syntactic interoperability
2: Network interoperability
1: Basic connectivity
Understanding of concepts contained in message data structures
Understanding of data structure in messages exchanged between systems
Messages exchange across various networks
Physical and logical connectivity
Application
Transport
NWK
MAC
PHY
Zigbee smart energy and home automation
TCP/UDP
IP
802.11, 802.15.4 etc

Figure 6: Interoperability framework.

Our framework facilitates the interconnection of the WSN to the BAN server via the in-building Wi-Fi system. This interconnection is achieved using a dual-stack gateway router (GR) node which performs QoS classification and packet aggregation on Zigbee application layer packets before tunneling them to the BAN server over Wi-Fi. As seen in Figure 6, we utilize the 802.11 and 802.15.4 MAC and physical layer protocols in conjunction with 6LoWPAN, the compact application protocol, and Zigbee application layer application profiles to provide end-to-end interoperability within HANs and BANs. Physical layer interoperability is provided by means of the GR's dual stack and 802.11 and 802.15.4 interfaces. Network layer interoperability is provided using IPv6 and the use of 6LoWPAN to enable the WSN to communicate using IP. Syntactic interoperability is achieved by the use of the CAP, which allows us to utilize publically defined Zigbee application profiles such as the smart energy or home automation profiles to provide application layer interoperability across multivendor devices. This frees us to use Zigbee application profiles across the HAN, on PCs, routers, and over any IP-capable device nodes all over the home or commercial building, rather than only over Zigbee 802.15.4 networks. In addition, the ability of our system to schedule 802.15.4 and 802.11 MAC frames enables us to provide quality of service prioritization to emergency Zigbee traffic.

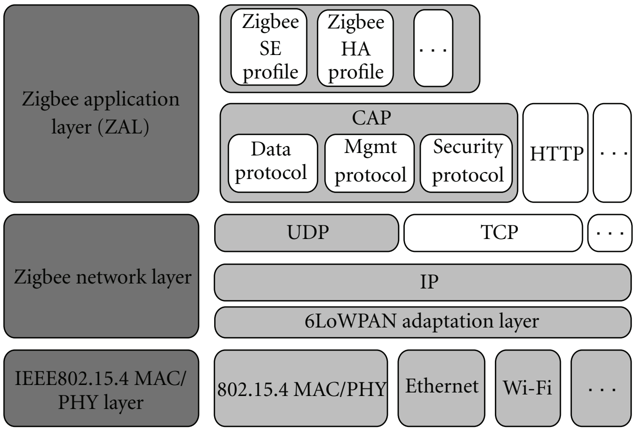


Figure 7: Zigbee, 6LoWPAN, and CAP stacks protocol stack [34, 35].

4.3. QoS of Service Framework. The GR facilitates interconnection of the 802.15.4 and Wi-Fi networks to enable end-to-end communication. The GR contains an MAC scheduler in which can communicate with 802.15.4 MAC and 802.11 MAC layer. On the basis of these assumptions, we divide the queuing model into three parts. In the first part, traffic from WSN end nodes to the coordinator is considered; in the second part, packets from the Wi-Fi access point (AP) to the GR are discussed; finally, we will focus on the queuing model of packets sent from GR. In this scheduling scheme, the use of guaranteed time slots (GTSs) can combine the task of scheduling uplink and downlink flows of a naturally distributed carrier sense medium access with collision avoidance (CSMA/CA) environment into a central scheduler residing in the GR.

As shown in Figure 8, each WSN node has two traffic queues, one for emergency or alarm traffic and the second for normal traffic [25]. Class 0 (alarm packets) are higher priority emergency/control data, while Class 1 (normal packets) contains routine data. Nodes will typically transmit two message types. The first are GTSs requests to reserve slots in CFP, and the second types are data packets containing sensor data.

Data frames are assigned to their respective queue and contend for transmission over the channel. A node contends per information frame and can only send one packet each time. If the node has an emergency message in its queue, it will request a shorter back off exponent value to enable prompt transmission of emergency traffic. Nodes which do not have emergency traffic utilize the regular value of the back off exponent, resulting in longer wait times.

Traffic differentiation at the GR is performed on the basis of destination ports. As seen in Figure 9, we use different ports for normal and emergency traffic and map them to EDCA video (AC_VI) and voice (AC_VO) access categories, respectively, before transmitting over the Wi-Fi network. A dedicated BASs server is the final recipient of the entire off network WSN traffic, and this server filters traffic based on the ports the data is received on.

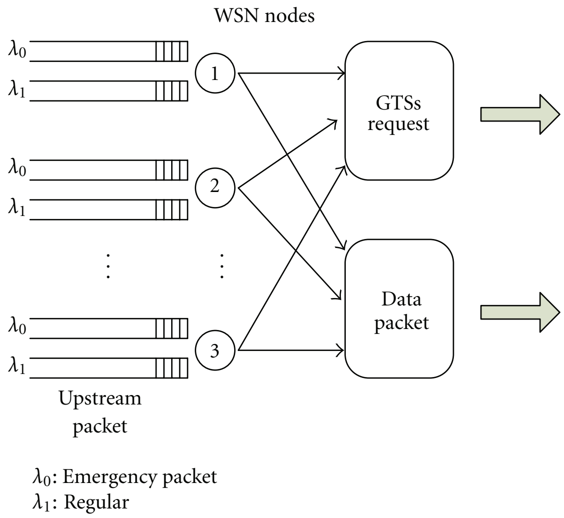


Figure 8: Queuing model from WSN end nodes to WSN coordinator.

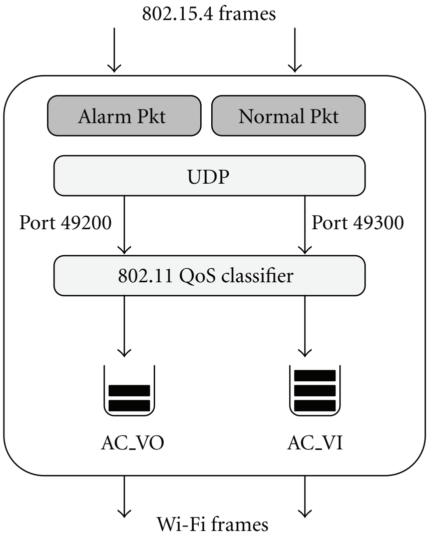


Figure 9: Queuing model from Gateway Router to Wi-Fi AP.

Due to the significant size difference between 802.15.4 and Wi-Fi frames, traffic aggregation is required for delay-tolerant traffic, while time sensitive WSN traffic is transmitted immediately. The encapsulation of individual 802.15.4 packets is very inefficient as the Wi-Fi header frame overhead is often larger than the useful information, necessitating packet aggregation to improve efficiency.

A hybrid scheduling model is used in the GR as shown in Figure 10. All packets received at the GR can be transmitted in either contention access period (CP) or contention-free period (CFP) modes. During the CP mode, nodes use a slotted CSMA/CA scheme to compete for the channel with other nodes. In CFP mode, up to seven GTS can be reserved and allocated by the coordinator. Devices which require the allocation of a new GTS transmit a GTS request command to the WSN coordinator and coordinator will assign GTS to each device. Our hybrid scheduling model adopts both EDCA in CP and point coordination function (PCF) controlled channel access (PCCA) in the CFP to achieve fairness and provide service guarantees. The GR assigns packets to different MAC schemes based on message type. Emergency/control messages which need to be sent out immediately will use EDCA contention access with smaller back off exponent. On the other hand, PCCA is used for routine messages, as these can wait for aggregation to be performed and are subsequently transmitted in reserved times slots.

Routine messages sent from the 802.15.4 PAN to the Wi-Fi access point are initially sent to the scheduler, where they are enqueued and time-stamped while a countdown timer initialized. The queue size is set to maximum size of a Wi-Fi payload, and if the queue is filled with routine messages before timer expiry, the scheduler reserves a GTS, aggregates all the enqueued traffic, and transmits them over the Wi-Fi radio. If the queue is not filled by timer expiry, then the GR reserves the number of GTSs required to transmit the queue and sends the accumulated data. The primary benefits of message aggregation with PCCA are collision and delay reduction for routine traffic.

5. Interference Avoidance Scheme

Zigbee networks operate in the license-free industrial, scientific and medical (ISM) frequency band, making them subject to interference from various devices that also share this license-free frequency band. These devices range from IEEE 802.11 wireless local area networks or Wi-Fi networks and Bluetooth devices to baby monitors and microwave ovens. Studies have shown that Wi-Fi is the most significant interference source for Zigbee within the 2.4 GHz ISM band [36, 37]. Zigbee and Wi-Fi networks are used extensively for BAN in smart grid applications, leading to coexistence problems as seen in Figure 11.

Therefore, we have performed a large amount of experiments to identify the “safe distance” and “safe offset frequency” to guide the Zigbee deployment [38]. The performance of Zigbee in the presence of IEEE 802.11 is defined and analyzed in terms of bit error rate (BER) and packet error rate (PER) by comprehensive approach including theoretical analysis, software simulation, and empirical measurement. Based on the concepts of “safe distance” and “safe offset frequency,” we propose a frequency-agility-based interference mitigation algorithm [39]. PER, link quality Indication (LQI), and energy detection mechanisms are used to detect the presence of significant levels of interference within the current channel. Once interference is detected, the coordinator instructs all the routers to perform an energy detection scan on channels and then send a report to the coordinator. The coordinator selects the channel with the lowest noise levels and then requests all nodes in the PAN to migrate to this channel. In order to improve the detection time and power efficiency, all Zigbee channels are divided into three classes based on the offset frequency. The energy detection scan will be performed from high-priority class to low-priority class channels to quickly identify the channel with acceptable interference level. The testbed implementation shows that the proposed frequency-agility-based algorithm is simple but efficient, fast, and practical.

6. Opportunistic Load Scheduling

Demand response is the technology that manages customers’ electricity usage to reduce electricity expenditure. Since customers are provided with the real-time power price by smart metering devices, load scheduling must incorporate real price in order to perform load control. The real-time price is an indicator of the system load. In general, the price is high when the load demand is high and vice versa. Some level of peak demand reduction may be automatically achieved by rational customers who aim to minimize the electricity cost. Naturally, the customers will choose to operate their flexible loads when the real-time price reaches the minimum. In this way, those flexible loads are shifted to the low demand time period, and consequently, the peak demand is reduced.

Nowadays, most existing load scheduling schemes are based on the assumption that future electricity prices are known or predictable. We propose to apply the optimal stopping rule [40] to perform distributed load scheduling. Our scheme to determines when to operate the flexible loads under the assumption that price signals are unknown and considered as random processes optimal stopping rule is proved to perform excellently in communication networks [41]. Thus, we extend the application of optimal stopping rule to power grids [42]. The time requirement of the load is taken into the consideration. If a user does not have time requirement, it will always choose to operate at the time when the electricity price is the lowest to minimize the electricity cost. However, many appliances, such as washing machine, are sensitive to the waiting time. Therefore, the spent time (which includes waiting time and service time) must be taken into consideration. The cost is modeled as the wait cost plus the electricity cost, and the objective is to minimize the total cost by choosing the best operating time. We show that the optimal scheduling scheme is a pure threshold policy; that is, each user needs to turn on the load when the electricity price is lower than a certain value; otherwise, the load remains idle. Simulation results show that the proposed low-complexity distributed scheduling scheme can dramatically reduce the cost. In other words, the loads are effectively shifted to low-demand time period. More details can be found in [6].

7. Open Issues and Future Work

7.1. Smart Grid Security. The smart grid requires detailed energy usage information in order to facilitate services such as real-time pricing and billing, customer energy management, and system load prediction. Unfortunately, as is the case with many other complex systems, the smart grid falls foul of the law of unintended consequences. The availability of such detailed usage data from every household every 5–15 minutes has created a massive security problem [43].

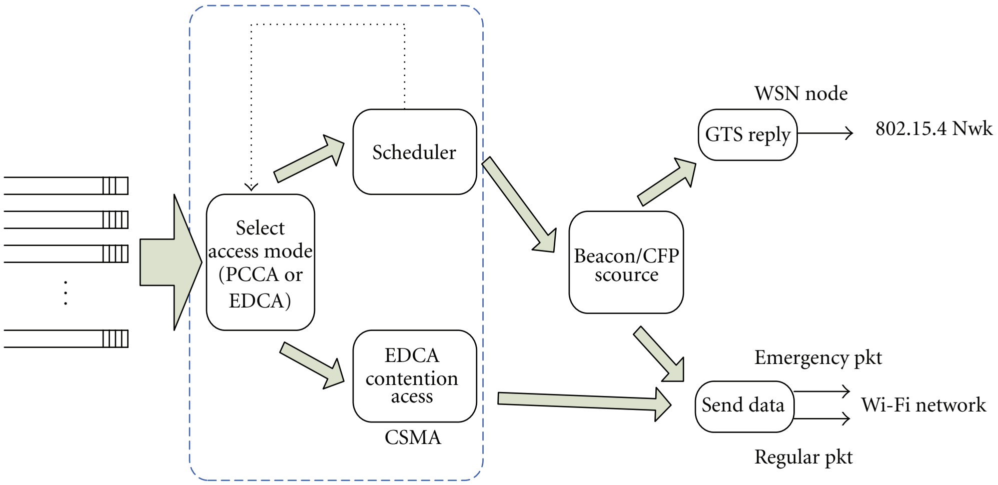


Figure 10: Queuing model in the WSN Coordinator.

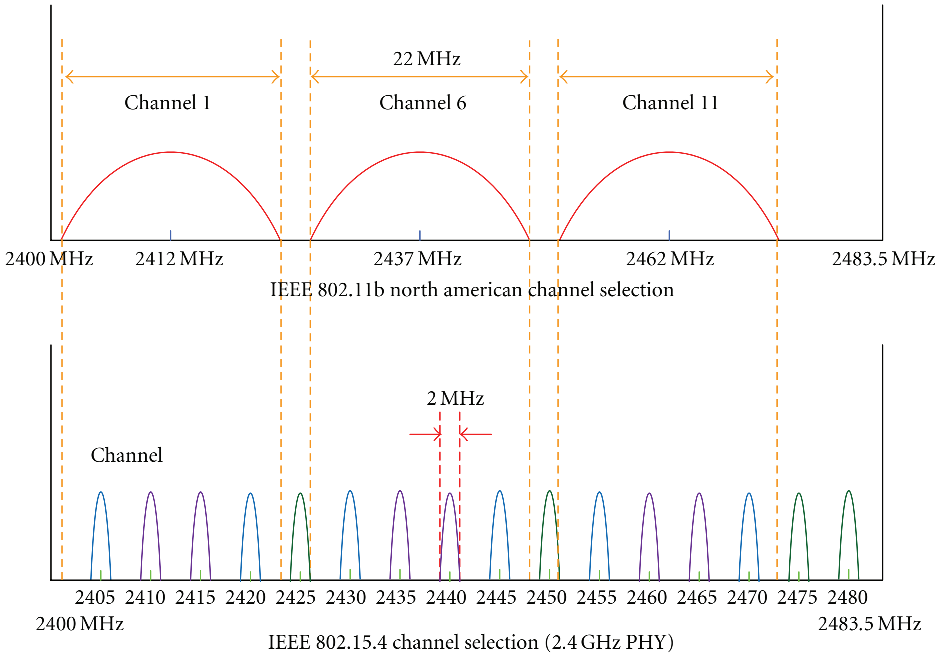


Figure 11: Zigbee and Wi-Fi channels in the 2.4 GHz band.

Smart meter data analysis provides the ability to determine which appliances are in use at any given time period. This has led to the fear that users can be spied upon by their meters, negatively impacting smart meter deployment [44]. The networking of smart meters with the electricity grid also raises the specter of smart meter fraud and increases the vulnerability of these devices to malicious attacks such as denial of service (DoS) attacks.

7.1.1. Privacy Issues. Research into nonintrusive appliance load monitoring technology (NALM) [45–47] has enabled the identification of appliances by means of their unique fingerprint or "appliance load profiles." By means of software analysis, it possible to determine which appliances are in use and at what frequency. It provides access to information including the types of appliances a resident possesses, when he/she has their shower each day (by monitoring extended usage of the heater), how many hours they spend using their PC, or whether they cook often or eat microwave meals. This has led to the very valid fear that customers can be profiled and monitored by means of their smart meter. In addition, improper access to such data can lead to violations of privacy or even make one open to burglary.

7.1.2. Smart Meter Fraud. The desire for lower electricity bills provides a compelling incentive for smart meter fraud. The ability to report inaccurate data to the utility means that customers can reduce their bills by falsely claiming to supply power the grid or consume less power than their actually do. The possibility of commercially available smart meter hacking kits is also a reality [48].

7.1.3. Malicious Attacks. The internetworking of smart meters makes them especially vulnerable to denial of service attacks in which several meters are hijacked in order to flood the network with data in order to shut down portions of the power grid or report false information which can result in grid failures.

7.1.4. Smart Grid Security Solutions. Smart grid security issues can only be solved by a combination of regulatory and technological solutions. A regulatory framework is required to specify who has access to smart meter data and under which conditions as well as enforcement of penalties for data misuse [48]. Two technological solutions have been proffered. The first is to aggregate residential data at the neighborhood transformer and then anonymize it by stripping it off its source address before transmitting it to the utility [43]. Kalogridis et al. [42] propose the use of a third party escrow service which receives the detailed meter data, anonymizes it by stripping off any information that could be used to identify a specific household, then sends the utility the aggregate data required for billing and monthly energy usage for each customer.

We propose a digital rights management system- (DRMS-) based scheme which extends that proposed in [49]. Users license permission to the utility to access their data at varying levels of granularity. By default, the utility would have access to monthly usage and billing data, but customers have to grant the utility permission to access their data at higher levels of granularity in exchange for rebates or other incentives. Such a system eliminates the need for an intermediary between the utility and the consumer but requires a means of guaranteeing that the utility cannot access restricted customer data.

7.2. Data Compression. Mitigating data surges and traffic congestion due to catastrophic events is an open research area. When emergencies such as power blackouts occur, hundreds to thousands of smart meter flood the data collection center with traffic. Reliability is an important issue, since the data needs to be transmitted effectively and efficiently, and network coding is a promising approach to improving the reliability of the wireless networks under such conditions. By means of network coding, we could potentially introduce intraflow network coding into the data transmission in Zigbee networks; that is, routers mix packets heading to the same destination. As a result of this mixing, each received packet contains some information about all packets in the original file, and thus, no coded packet is special.

Conventionally, without coding, a transmitter needs to know which exact packets the destination misses so that it can retransmit them. When the network is unreliable, communicating this feedback reliably consumes significant bandwidth. In the presence of coding, no specific packet is indispensable, and as a result, a transmitter does not need to learn which particular packet the destination misses; it only needs to get feedback from the destination once it has received enough packets to decode the whole file. The reader may have noticed that the above applies to erasure-correcting coding applied at the source too. Indeed, source coding is just a special case of intraflow network coding, where the source is the only node allowed to mix the packets in the flow.

8. Conclusion

In order for the smart grid to achieve its potential, we need the resolve the problem of interoperability between the different communications technologies deployed in the grid. In this paper, we proposed an HAN architecture for energy management within smart grid environments. Zigbee-based building energy management was demonstrated to enhance building automation systems and permit granular control of electrical and HVAC systems in a smart grid context. An open architecture of an interoperability frame work for HANs and BANs was presented in the paper. Physical layer interoperability is provided by means of a router platform with 802.11 and 802.15.4 interfaces. Network layer interoperability is provided using IPv6 and the usage of 6LoWPAN to enable the WSN to communicate using IP. Syntactic interoperability is achieved by the use of the CAP. In the QoS framework, emergency/control message need to compete with routine traffic from other nodes. The prioritized contention algorithm ensured the high priority access the channel for these messages. Use of compression and scheduling increases the efficiency of the data transferred from Zigbee to Wi-Fi frames. A frequency-agility-based interference mitigation algorithm was introduced in the paper to guarantee the performance of Zigbee and Wi-Fi coexistence. Optimal stopping rule base load scheduling scheme as a distributed load control was present in the paper. More open issues including security and data compression were discussed in the paper.

References

[1] P. Yi, A. Iwayemi, and C. Zhou, "Developing ZigBee deployment guideline under WiFi interference for smart grid applications," *IEEE Transactions on Smart Grid*, vol. 2, no. 1, pp. 98–108, 2011.

[2] US Department of Energy, "Buildings Energy Data Book," March 2009, http://buildingsdatabook.eren.doe.gov/.

[3] T. J. Lui, W. Stirling, and H. O. Marcy, "Get smart," *IEEE Power and Energy Magazine*, vol. 8, no. 3, pp. 66–78, 2010.

[4] Office of the National Coordinator for Smart Grid Interoperability, NIST, "Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0," National Institute of Standards and Technology, 2010.

[5] "The Galvin Path to Perfect Power—A Technical Assessment: Report on the Galvin Electricity Initiative, Phase II, Tasks 1 & 2," Galvin Electricity Initiative, 2007.

[6] P. Yi, X. Dong, and C. Zhou, "Optimal energy management for smart grid systems—an optimal stopping rule approach," in *IFAC World Congress Invited Session on Smart Grids*, 2001, accepted.

[7] H. Farhangi, "The path of the smart grid," *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18–28, 2010.

[8] E. Santacana, G. Rackliffe, LE. Tang, and X. Feng, "Getting smart: with a clearer vision of the intelligent grid, control emerges from chaos," *IEEE Power and Energy Magazine*, vol. 8, no. 2, pp. 41–48, 2010.

[9] S. Amin, "For the good of the grid," *IEEE Power and Energy Magazine*, vol. 6, pp. 48–59, 2008.

[10] J. A. Gutiérrez, "On the use of IEEE Std. 802.15.4 to enable wireless sensor networks in building automation," *International Journal of Wireless Information Networks*, vol. 14, no. 4, pp. 295–301, 2007.

[11] A. C. W. Wong and A. T. P. So, "Building automation in the 21st century," in *Proceedings of the 4th International Conference on Advances in Power System Control, Operation and Management*, vol. 2, pp. 819–824, February 1998.

[12] D. Snoonian, "Smart buildings," *IEEE Spectrum*, vol. 40, no. 8, pp. 18–23, 2003.

[13] W. Kastner, G. Neugschwandtner, S. Soucek, and H. M. Newman, "Communication systems for building automation and control," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1178–1203, 2005.

[14] K. Gill, S. H. Yang, F. Yao, and X. Lu, "A ZigBee-based home automation system," *IEEE Transactions on Consumer Electronics*, vol. 55, no. 2, pp. 422–430, 2009.

[15] A. Iwayemi, P. Yi, P. Liu, and C. Zhou, "A perfect power demonstration system," in *Innovative Smart Grid Technologies Conference (ISGT '10)*, pp. 1–7, January 2010.

[16] J. J. P. C. Rodrigues and P. A. C. S. Neves, "A survey on IP-based wireless sensor network solutions," *International Journal of Communication Systems*, vol. 23, no. 8, pp. 963–981, 2010.

[17] J. W. Hui and D. E. Culler, "Extending IP to low-power, wireless personal area networks," *IEEE Internet Computing*, vol. 12, no. 4, pp. 37–45, 2008.

[18] A. Dunkels, "TCP/IP for 8-bit architectures," in *Proceedings of the 1st International Conference on Mobile Systems, Applications, and Services (MOBISYS '03)*, 2003.

[19] G. Mulligan, "The 6LoWPAN architecture," in *Proceedings of the 4th Workshop on Embedded Networked Sensors (EmNets '07)*, pp. 78–82, June 2007.

[20] J. W. Hui and D. E. Culler, "IP is dead, long live IP for wireless sensor networks," in *Proceedings of the 6th ACM conference on Embedded Network Sensor Systems*, pp. 15–28, 2008.

[21] M. Sveda and R. Trchalik, "ZigBee-to-internet interconnection architectures," in *Proceedings of the 2nd International Conference on Systems (ICONS '07)*, p. 30, April 2007.

[22] R. Wang, R. Chang, and H. Chao, "Internetworking between ZigBee/802.15.4 and IPv6/802.3 network," in *SIGCOMM Workshop "IPv6 and the Future of the Internet"*, Kyoto, Japan, August 2007.

[23] G. Mulligan et al., "Seamless sensor network IP connectivity," in *Proceedings of the 6th European Conference on Wireless Sensor Networks (EWSN '09)*, 2009.

[24] G. Tolle, "A UDP/IP adaptation of the ZigBee application protocol," http://tools.ietf.org/html/draft-tolle-cap-00.

[25] X. Yuan, S. Bagga, J. Shen, M. Balakrishnan, and D. Benhaddou, "DS-MAC: differential service medium access control design for wireless medical information systems," in *Proceedings of the 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS '08)*, pp. 1801–1804, August 2008.

[26] A. Banchs, A. Azcorra, C. García, and R. Cuevas, "Applications and challenges of the 802.11e EDCA mechanism: an experimental study," *IEEE Network*, vol. 19, no. 4, pp. 52–58, 2005.

[27] Y. P. Fallah and H. Alnuweiri, "Hybrid polling and contention access scheduling in IEEE 802.11e WLANs," *Journal of Parallel and Distributed Computing*, vol. 67, no. 2, pp. 242–256, 2007.

[28] J. Leal, A. Cunha, M. Alves, and A. Koubâa, "On a IEEE 802.15.4/ZigBee to IEEE 802.11 gateway for the ART-WiSe architecture," in *Proceedings of the 12th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA '07)*, pp. 1388–1391, September 2007.

[29] U. S. Department of Energy, Office of Electricity Delivery and Energy Reliability, "Recovery Act Financial Assistance, Funding Opportunity Announcement. Smart Grid Investment Grant Program Funding Opportunity Number: DE-FOA-0000058," June 2009.

[30] GridWise Architecture Council, "GridWise Interoperability Context-Setting Framework (v1.1)," 2008.

[31] IETF, "RFC 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks," http://www.rfc-editor.org/rfc/rfc4944.txt.

[32] D. E. Culler and G. Tolle, "Compact Application Protocol (CAP): Uniting the Best of IP and ZigBee," http://www.rtcmagazine.com/articles/print_article/101065.

[33] Z. Shelby and C. Bormann, *6LoWPAN: The Wireless Embedded Internet*, Wiley, 2010.

[34] Parallax Inc., "Parallax PIR Sensor (#555-28027)," March 2010, http://www.parallax.com/dl/docs/prod/audiovis/pirsensor-v1.2.pdf.

[35] "Panasonic AQH Solid State Relay," http://pewa.panasonic.com/assets/pcsd/catalog/aq-h-catalog.pdf.

[36] Zensys, "White Paper: WLAN interference to IEEE 802.15.4," 2007.

[37] S. Y. Shin, H. S. Park, S. Choi, and W. H. Kwon, "Packet error rate analysis of ZigBee under WLAN and Bluetooth interferences," *IEEE Transactions on Wireless Communications*, vol. 6, no. 8, pp. 2825–2830, 2007.

[38] P. Yi, A. Iwayemi, and C. Zhou, "Frequency agility in a ZigBee network for smart grid application," in *Innovative Smart Grid Technologies Conference (ISGT '10)*, pp. 1–6, January 2010.

[39] G. Thonet and P. Allard-Jacquin, "ZigBee-WiFi Coexistence White Paper and Test Report," Schneider Electric White Paper, 2008.

[40] T. S. Ferguson, "Optimal Stopping and Applications," http://www.math.ucla.edu/~tom/Stopping/Contents.html.

[41] D. Zheng, W. Ge, and J. Zhang, "Distributed opportunistic scheduling for ad hoc networks with random access: an optimal stopping approach," *IEEE Transactions on Information Theory*, vol. 55, no. 1, pp. 205–222, 2009.

[42] G. Kalogridis, C. Efthymiou, S. Denic, T. Lewis, and R. Cepeda, "Privacy for smart meters: towards undetectable appliance load signatures," in *Proceedings of the 1st IEEE International Smart Grid Communications (SmartGridComm '10)*, pp. 232–237, 2010.

[43] E. L. Quinn, "Privacy and the New Energy Infrastructure," *SSRN eLibrary*, February 2009, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1370731.

[44] "IEEE Spectrum: Privacy on the Smart Grid," http://spectrum.ieee.org/energy/the-smarter-grid/privacy-on-the-smart-grid.

[45] G. W. Hart, "Nonintrusive appliance load monitoring," *Proceedings of the IEEE*, vol. 80, no. 12, pp. 1870–1891, 1992.

[46] J. G. Roos, I. E. Lane, E. C. Botha, and G. P. Hancke, "Using neural networks for non-intrusive monitoring of industrial electrical loads," in *Proceedings of the 10th IEEE Instrumentation and Measurement Technology Conference*, vol. 3, pp. 1115–1118, 1994.

[47] H.-H. Chang, C.-L. Lin, and J.-K. Lee, "Load identification in nonintrusive load monitoring using steady-state and turn-on transient energy algorithms," in *Proceedings of the 14th*

International Conference on Computer Supported Cooperative Work in Design (CSCWD '10), pp. 27–32, 2010.

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

[49] Z. Fan, G. Kalogridis, C. Efthymiou, M. Sooriyabandara, M. Serizawa, and J. McGeehan, "The new frontier of communications research: smart grid and smart metering," in *Proceedings of the 1st International Conference on Energy-Efficient Computing and Networking (e-Energy '10)*, pp. 115–118, 2010.

Hindawi Publishing Corporation
International Journal of Digital Multimedia Broadcasting
Volume 2011, Article ID 502087, 14 pages
doi:10.1155/2011/502087

Research Article

Cognitive Radio for Smart Grid: Theory, Algorithms, and Security

Raghuram Ranganathan,[1, 2] Robert Qiu,[1, 2] Zhen Hu,[1, 2] Shujie Hou,[1, 2] Marbin Pazos-Revilla,[1, 2] Gang Zheng,[1, 2] Zhe Chen,[1, 2] and Nan Guo[1, 2]

[1] *Department of Electrical and Computer Engineering, Center for Manufacturing Research, Tennessee Technological University, Cookeville, TN 38505, USA*
[2] *Cognitive Radio Institute, Tennessee Technological University, Cookeville, TN 38505, USA*

Correspondence should be addressed to Raghuram Ranganathan, raghu_ucf@yahoo.com

Received 9 February 2011; Accepted 24 March 2011

Academic Editor: Chi Zhou

Recently, cognitive radio and smart grid are two areas which have received considerable research impetus. Cognitive radios are intelligent software defined radios (SDRs) that efficiently utilize the unused regions of the spectrum, to achieve higher data rates. The smart grid is an automated electric power system that monitors and controls grid activities. In this paper, the novel concept of incorporating a cognitive radio network as the communications infrastructure for the smart grid is presented. A brief overview of the cognitive radio, IEEE 802.22 standard and smart grid, is provided. Experimental results obtained by using dimensionality reduction techniques such as principal component analysis (PCA), kernel PCA, and landmark maximum variance unfolding (LMVU) on Wi-Fi signal measurements are presented in a spectrum sensing context. Furthermore, compressed sensing algorithms such as Bayesian compressed sensing and the compressed sensing Kalman filter is employed for recovering the sparse smart meter transmissions. From the power system point of view, a supervised learning method called support vector machine (SVM) is used for the automated classification of power system disturbances. The impending problem of securing the smart grid is also addressed, in addition to the possibility of applying FPGA-based fuzzy logic intrusion detection for the smart grid.

1. Introduction

1.1. Cognitive Radio. Cognitive radio (CR) is an intelligent software defined radio (SDR) technology that facilitates efficient, reliable, and dynamic use of the underused radio spectrum by reconfiguring its operating parameters and functionalities in real time depending on the radio environment. Cognitive radio networks promise to resolve the bandwidth scarcity problem by allowing unlicensed devices to transmit in unused "spectrum holes" in licensed bands without causing harmful interference to authorized users [1–4]. In concept, the cognitive technology configures the radio for different combinations of protocol, operating frequency, and waveform. Current research on cognitive radio covers a wide range of areas; including spectrum sensing, channel estimation, spectrum sharing, and medium access control (MAC).

Due to its versatility, CR networks are expected to be increasingly deployed in both the commercial and military sectors for dynamic spectrum management. In order to develop a standard for CRs, the IEEE 802.22 working group was formed in November 2004 [5]. The corresponding IEEE 802.22 standard defines the physical (PHY) and medium access control (MAC) layers for a wireless regional area network (WRAN) that uses white spaces within the television bands between 54 and 862 MHz, especially within rural areas where usage may be lower. Details of the IEEE 802.22 standard including system topology, system capacity, and the projected coverage for the system are given in the next section.

1.2. The 802.22 System. The IEEE 802.22 is the first standardized air interface for CR networks based on opportunistic utilization of the TV broadcast spectrum [6, 7]. The main objective of the IEEE 802.22 standard is to provide broadband connectivity to remote areas with comparable performance to broadband technologies such as cable and

DSL, in urban areas. In this regard, the FCC selected the predominantly unoccupied TV station channels operating in the VHF and UHF region of the radio spectrum.

1.2.1. System Topology. The 802.22 system is a point-to-multipoint wireless air interface consisting of a base station (BS) that manages a cell comprised of number of users or customer premises equipments (CPEs) [8]. The BS controls the medium access and "cognitive functions" in its cell and transmits data to the CPEs in the downlink, while receiving data in the uplink direction from the CPEs. The various CPEs perform distributed sensing of the signal power in the various channels of the TV band. In this manner, the BS collects the different measurements from the CPEs and exploits the spatial diversity of the CPEs to make a decision if any portion of the spectrum is available.

1.2.2. Service Coverage. Compared to other IEEE 802 standards such as 802.11, the 802.22 BS coverage range can reach up to 100 KM, if not limited by power constraints. The coverage of different wireless standards is shown in Figure 1. The WRAN has the highest coverage due to higher transmit power and long-range propagation characteristics of TV bands.

1.2.3. System Capacity. The WRAN systems can achieve comparable performance to that of DSL, with downlink speeds of 1.5 Mbps and uplink speed of 384 Kbps. The system would thus be able to support 12 simultaneous CPEs, resulting in an overall system download capacity of 18 Mbps.

The specification parameters of the IEEE 802.22 standard is summarized in Table 1.

Table 1: IEEE 802.22 characteristics.

Parameter	Specification
Typical cell radius (km)	30–100 km
Methodology	Spectrum sensing to identify free channels
Channel bandwidth (MHz)	6, (7, 8)
Modulation	OFDM
Channel capacity	18 Mbps
User capacity	Downlink: 1.5 Mbps Uplink: 384 kbps

1.3. Smart Grid. Smart grid explores and exploits two-way communication technology, advanced sensing, metering and measurement technology, modern control theory, network grid technology, and machine learning in the power system to make the power network stable, secure, efficient, flexible, economical, and environmentally friendly.

Novel control technology, information technology, and management technology should be effectively integrated to realize the smart information exchange within the power system from power generation, power transmission, power transformation, power distribution, power scheduling to power utilization. The goal of smart grid is to systematically optimize the cycle of power generation and utilization.

Based on open-system architecture and shared information mode, power flow, information flow, and transaction flow can be synchronized. In this way, the operation performance of power enterprises can be increased. From power customer's perspective, demand response should be implemented. Customers would like to participate in more activities in the power system and power market to reduce their electric bills.

Distributed energy resources, for example, solar energy, wind energy, and so on, should also play an important role in the smart grid. Versatile distributed energy resources can perform the peak power shaving and increase the stability of the power system. However, distributed energy generation imposes new challenges on the power system. Power system planning, power quality issue, and so on should be reconsidered.

To support the smart grid, a dedicated two-way communications infrastructure should be set up for the power system. In this way, secure, reliable, and efficient communication and information exchange can be guaranteed. In addition, the various devices, equipments, and power generation facilities of the current power system should be updated and renovated. Novel technologies for power electronics should be used to build advanced power devices, for example, transformer, relay, switch, storage, and so on.

To incorporate the smart features into the power system, computationally intelligent techniques, that is, machine learning and dimensionality reduction, should be widely applied. Machine learning is a scientific discipline that is concerned with the design of algorithms for computers to imitate the behavior of human beings, which includes learning to recognize complex patterns and make decisions based on experience, automatically and intelligently. Dimensionality reduction is the process of reducing the number of random variables under consideration to control the degrees of freedom. Several areas for applying computationally intelligent techniques to the smart grid have been identified in [9]. These areas are smart sensing and metering, autonomous control, adaptive protection, advanced data management and visualization, intelligent interfaces with distributed resources and market, decision support systems for system operation, and planning. The concept of compressing electrical power grids using the singular value decomposition (SVD) analysis is proposed in [10] to reduce the network traffic. The main idea is to determine what parts of the system are more strongly coupled from the grid admittance matrix [10].

In the smart grid, there will be more than one element, agent, controller, or decision maker. The control algorithm for the system with a single agent cannot be well suited for the distributed control or noncooperative control. From the multiagent control issue perspective, Game theory gives a general control methodology to deal with interaction, competition, and cooperation among decision makers in the complex system. Game theory is widely used in social sciences, economics, engineering, and so on. For the smart grid, the energy consumption scheduling issue has been

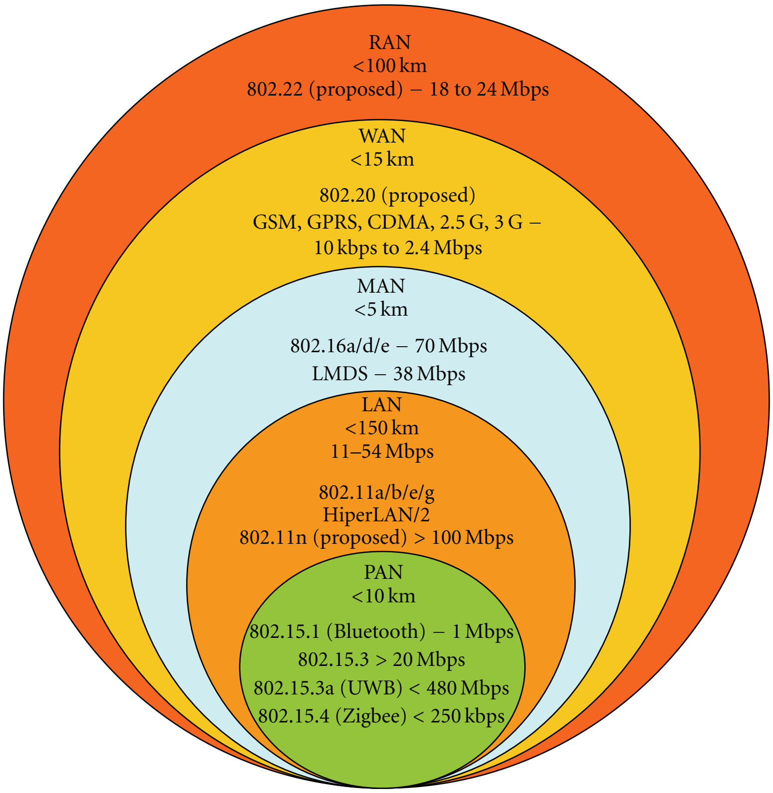

RAN
<100 km
802.22 (proposed) − 18 to 24 Mbps
WAN
<15 km
802.20 (proposed)
GSM, GPRS, CDMA, 2.5 G, 3 G −
10 kbps to 2.4 Mbps
MAN
<5 km
802.16a/d/e − 70 Mbps
LMDS − 38 Mbps
LAN
<150 km
11–54 Mbps
802.11a/b/e/g
HiperLAN/2
802.11n (proposed) > 100 Mbps
PAN
<10 km
802.15.1 (Bluetooth) − 1 Mbps
802.15.3 > 20 Mbps
802.15.3a (UWB) < 480 Mbps
802.15.4 (Zigbee) < 250 kbps

Figure 1: Comparison of 802.22 with other wireless standards.

formulated as a game theory problem [11]. The aim of scheduling is to reduce the total energy cost as well as PAR in the load demand [11]. Based on the assumption that the charge for each subscriber is proportional to his/her total daily load, the energy consumption game can be solved distributively with minimum exchanging information [11]. Meanwhile, the unique Nash equilibrium of the energy consumption game is the optimal solution to the central scheduling problem [11]. The work in [11] has been extended by [12]. Different control strategies based on the degree of information sharing in the network have been studied [12]. Partial knowledge setting and blind setting are considered. The proposed distributed stochastic energy consumption scheduling algorithms can still successfully exploit the limited information to improve the overall load profile [12]. In the context of the electrical power system, auction theory is a popular approach to deal with the power control issue from an economic point of view. Auction theory is a kind of game theory that deals with the behavior of agents in auction markets. Operation of a multiagent system for microgrid control has been presented in [13]. Auction theory has been exploited as the foundation of the proposed algorithm, the main idea being that every distributed energy resource or controllable load decides what is best for it, taking into account the overall benefit [13].

From the discussion of the control algorithm in smart grid, it is safe to say that pricing-based algorithms, pricing-based utility functions, and pricing models should be considered to optimize the system. A quasidynamic pricing model [14] has been proposed to minimize the electricity bill of cooperative users. The price comprises of a base price and a penalty term. Two methods are described. Deadline-driven continuous variable method is suitable for an energy cost optimization with less interruptible tasks, while the time slot-based method is appropriate for more interruptible tasks [14]. One optimal real-time pricing algorithm has been mentioned in [15]. Energy pricing is an essential tool to develop efficient demand-side management strategies [15]. The proposed algorithm can be implemented in a distributed manner to maximize the aggregate utility of all users and minimize the cost imposed to the energy provider [15].

1.4. Power System Disturbance Classification. It is critical for power system operators to discern power system disturbances characteristics in order to take control measures to ensure power system security and reliability. This issue has become even more challenging due to the expansion of power system interconnections and integration of distributed generators and renewable energy resources [16, 17]. Wide area measurement system (WAMS) implements the disturbance detection by collecting measurements from local sensors (wire, cable, or wireless) and managing it on a central server [18–22].

Power system disturbance classification has been conducted using pattern recognition in [23–25] based on power system measurements like voltage quality, power flow, or frequency. Artificial intelligence, such as neural networks, and particle swarm optimization have been introduced for complex signal classification [26, 27]. However, the implementation of these algorithms is too complicated and not practical. To circumvent this, a machine-learning method called support vector machine (SVM) can be employed to quickly and accurately classify various common power system disturbances using the frequency data at various points in the power system. The objective is to eventually enable automated classification of disturbances, which is currently easy for a person to accomplish, yet difficult for a computer. SVM, which was first proposed by Cortes and Vapnik [28], transforms unknown data from a nonlinear space to a linear space. Subsequently, any linear algorithm can be applied to form the knowledge for the machine operation. SVM can achieve a unique global optimum for a convex optimization problem. In addition, SVM is not affected by the uncertainty in the parameters. Due to its various advantages, SVM is increasingly preferred in the field of pattern recognition and classification [26, 27].

1.5. Securing the Smart Grid. The smart grid is aimed at transforming the already aging electric power grid in the United States into a digitally advanced and decentralized infrastructure with heavy reliance on control, energy distribution, communication, and security.

In order to develop this infrastructure, a high level of interconnectivity and reliability among its nodes is required. Sensors, advanced metering devices, electrical appliances, and monitoring devices, just to mention a few, will be highly interconnected allowing for the seamless flow of data. Reliability and security in this flow of data between nodes, as shown in Figure 2, is crucial due to the low latency and cyber attacks resilience requirements of the smart grid.

A distributed interconnection among these nodes will be ubiquitous, just as finding a similar level of connectivity among cellular phones or computing nodes in a large organization. The smart grid environment, however, poses a new set of communications and security paradigms. Due to their complexity and importance to the realization of the smart grid infrastructure, it is extremely important to study the interactions among the nodes, more specifically, in terms of their communications and security.

Taking into account that reliability and security will impose constraints on the majority of the devices connected to the Smart Grid, if not all, it would be wise to consider communication standards, protocols, and devices that are designed from the ground up to be secured, logically and physically. Since a great portion of the traffic generated within the grid will be traveling on an unsecured medium such as the Internet, it is imperative to minimize the amount of potential security loopholes. Additionally, the human variable should also be taken into account in the security model, as part of the security infrastructure.

When it comes to security, communication is key, and information should be properly disseminated to all the parties involved, ensuring that everyone has a clear and common understanding of security needs facilitating their implementation and operation. Training and informing users about processes, study of human behavior, and the perception of events related to the processes is as important to the entire security equation, as it is to engineer a secured infrastructure. As a matter of fact, the greatest security threat to any infrastructure is human error, as opposed to the technology securing it. Communications in the smart grid is a key component of the entire infrastructure, and logically we divide it into two sections, the backbone communications (interdomain), which will carry communications among domains such as those shown in Figure 2, and the communications at the local area network (intradomain) limited by perimeters such as a customer's house, or a distribution facility [29]. It would be important to note that due to current limitations, the focus of research on our testbed will be on intradomain communications, without disregard for future considerations of the interdomain aspect.

We can say that current and emerging technologies in telecommunications, most of which are expected to fall in the wireless realm (Wimax, Zigbee, 802.11, etc.), can accommodate the communications needs of both inter and intradomain environments, however, not without flaws. From a security standpoint, these technologies are not designed to be secure from the ground up. For example, Zigbee is a standard for short-range communications, and manufacturers of Zigbee compliant chips produce them without necessarily considering the security issue. In addition, chip manufacturers print the chip model on top of the chip itself as a standard practice. The chip specifications can therefore be easily downloaded, and potential flaws of the chip can be easily exploited by attackers. Additionally, by default, many of these chips do not carry any internal security features and, therefore, rely on external chips, or on higher level software applications for this purpose. An easy access to the external chip by any malicious attacker could potentially disable any installed security features. This and other similar scenarios lead us to think that the smart grid should be driven by technologies and standards that consider security as their primary concern.

The smart grid has been conceived as being distributed in nature and heavily dependent on wireless communications. Today's SOHO (small office/home office) and enterprise-graded wireless devices include security features to mitigate attacks, the vast majority still relying on conventional rule-based detection. It has been shown that conventional rule-based detection systems, although helpful, do not have the capability of detecting unknown attacks. Furthermore, as presented in [30], these conventional IDSs would not be able to detect such an attack if it is carefully crafted, since the majority of these rules are solely based on strict thresholds.

2. Review

2.1. Cognitive Radio Network Testbed. A Cognitive Radio (CR) network testbed is being built at Tennessee Technological University [31, 32]. The idea of applying a cognitive radio network testbed to the smart grid was developed at Tennessee Technological University in the middle of 2009 in a funded research proposal [33]. Subsequently, this idea has been strengthened in [31, 34–37]. The objective of this

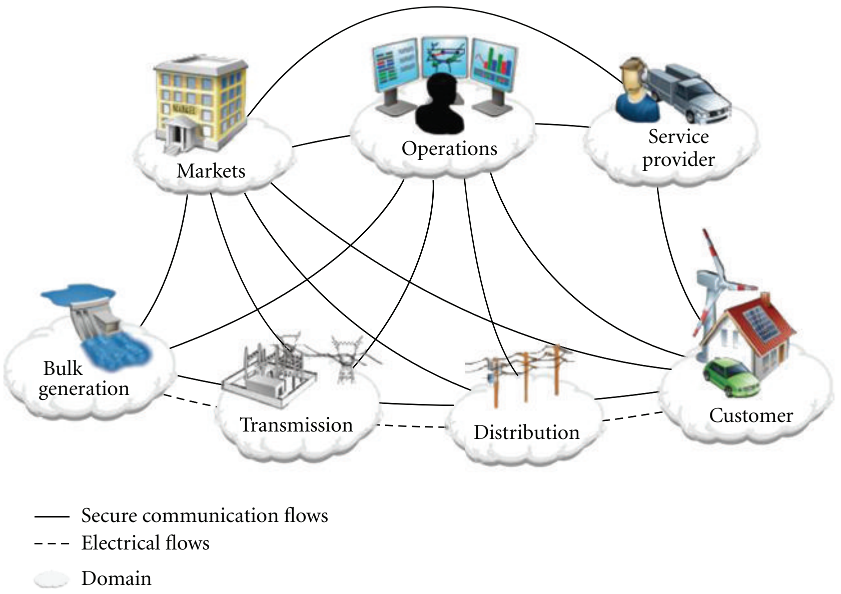


Figure 2: Interaction among actors in smart grid domains through secure communication flows and flows of electricity.

testbed is to achieve the convergence of cognitive radio, cognitive radar, and smart grid [38].

The cognitive radio network testbed being built is unique and real-time oriented. It is designed to provide much more stand-alone computing power and reduce the response time delay. The cognitive radio network testbed is comprised of tens of nodes, with each node based on a self-designed motherboard, and commercial radio frequency (RF) boards. On the self-designed motherboard, there are two advanced and powerful field programmable gate arrays (FPGAs) that can be flexibly configured to implement any function. Therefore, this network testbed can also be applied to the smart grid.

To our understanding, the benefits of applying cognitive radio to the smart grid are summarized in Table 2. Firstly, cognitive radio can operate over a wide range of frequency bands. It has frequency agility. This feature is especially useful for smart grid because the frequency spectrum today is so crowded, and cognitive radio provides the capability of reusing unused frequency bands for the smart grid. Secondly, cognitive radio enables high-speed data transmission for the smart grid. This is due to the wide-band nature of cognitive radio. The data rate can be as high as tens of Mbps, in contrast to the ZigBee that can only provide a data rate of tens to hundreds of kbps. Thirdly, cognitive radio has the potential to transmit data over a long-distance. Recently, the federal communications commission (FCC) has decided to allow using unused TV bands for wireless communications. The TV bands are ideal for long distance mass data transmission. Cognitive radio in a wireless regional area network (WRAN) scenario is designed to utilize the unused TV bands. Employing cognitive radio, the smart grid can communicate over a long distance over the air. Fourthly, cognitive radio boasts of cognitive learning and adaptation capability. It has the ability to learn the environment, reason from it, and adapt accordingly. Cognitive radio makes the smart grid "smarter" and more robust. Fifthly, cognitive radio is based on the software defined radio (SDR) platform, which is a programmable radio. Hence, cognitive radio is capable of performing different applications and tasks. In addition, security, robustness, reliability, scalability, and sustainability of the smart grid can be effectively supported by cognitive radio due to its flexibility and reprogrammability.

Table 2: Advantages of applying cognitive radio to smart grid.

Salient features	Description
Frequency diversity	CR can operate over unused frequency bands
Transmission speed	Data rates of up to tens of Mbps can be achieved
Range	CR can transmit over long distances in a WRAN scenario
Adaptability	CR has inherent intelligence to adapt to changes in the environment
Programmability	Built on an SDR platform, the CR can be selectively programmed

2.2. Smart Grid Communications. Smart grid technology has attracted significant research focus in recent years from the power and communications standpoint [39, 40]. CRs provide a promising solution to the growing spectrum scarcity problem by intelligently accessing unused regions of spectrum originally licensed to primary users (PUs). One of the key requirements for the smart grid is a robust and efficient communications infrastructure that can address both the current and future energy management needs [41, 42]. With the advent of modern communications technologies, and the recently defined IEEE 802.22 standard, CR networks are believed to be a viable choice for smart grid applications. The opportunistic access of the TV broadcast spectrum as outlined in the 802.22 standard can be realized as one of the cognitive network functions.

3. Examples

In this section, examples are presented employing machine learning and signal processing techniques for dimensionality reduction, recovery of smart meter transmissions, power system disturbances classification, and fuzzy logic-based intrusion detection. This section is divided as follows. In Section 3.1, dimensionality reduction techniques such as PCA, KPCA, and LVMU, in combination with SVM, are used as a preprocessing tool in a spectrum sensing application for Wi-Fi signals. The SVM technique is used for power system disturbances classification in Section 3.2. In Section 3.3, the sparsity of the smart meter transmissions is exploited to recover the BPSK-modulated smart meter data, by employing the recently proposed bayesian compressed sensing, and compressed sensing kalman filter methods. Finally, the critical issue of smart grid security is addressed in Section 3.4, and a possible approach to realize this is provided using FPGA-based fuzzy logic.

3.1. Dimensionality Reduction Applied to Cognitive Radio with Experimental Validation. In radar and sensing signal processing, the control of degrees of freedom (DOF)—or intrinsic dimensionality—is the first step, called preprocessing. The network dimensionality, on the other hand, has received attention in information theory literature. The techniques of the dimensionality reduction can be explored to extract the intrinsic dimensionality of the high-dimensional data.

Dimensionality reduction methods are innovative and important tools in machine learning [43]. The original dimensionality data collected from our living world may contain a lot of features however, usually these features are highly correlated and redundant with noise. Hence, the intrinsic dimensionality of the collected data is much fewer than the original features. Dimensionality reduction attempts to select or extract a lower dimensionality expression but retain most of the useful information. In the first example, both linear methods such as principal component analysis (PCA) [44], nonlinear methods such as kernel principal component analysis (KPCA) [45], and landmark maximum variance unfolding (LMVU) [46, 47] are studied, by combining them with the support vector machine (SVM) [48–53]—the latest breakthrough in machine learning, in the context of spectrum sensing for cognitive radio.

Measured Wi-Fi signals with high signal-to-noise ratio (SNR) are employed in the first example. The DOF of the Wi-Fi signals is extracted by three dimensionality reduction techniques in this example. The advantages of applying dimensionality reduction techniques are verified by comparing with the results obtained without dimensionality reduction.

3.1.1. Wi-Fi Signal Measurements. Wi-Fi time-domain signals have been measured and recorded using an advanced digital phosphor oscilloscope (DPO) whose model is Tektronix DPO72004 [54]. The DPO supports a maximum bandwidth of 20 GHz and a maximum sampling rate of 50 GS/s. It is capable of recording up to 250 M samples per channel. In the measurements, a laptop accesses the Internet through a wireless Wi-Fi router, as shown in Figure 3. An antenna with a frequency range of 800 MHz to 2500 MHz is placed near the laptop and connected to the DPO. The sampling rate of the DPO is set to 6.25 GS/s. Recorded time-domain Wi-Fi signals are shown in Figure 4. The duration of the recorded Wi-Fi signals is 40 ms.

The recorded 40 ms Wi-Fi signals are divided into 8000 slots, with each slot lasting 5 μs. These slots can be viewed as spectrum sensing slots. The time-domain Wi-Fi signals within the first 1 μs of every slot are then transformed into the frequency domain using the Fast Fourier Transform (FFT), which is equivalent to FFT-based spectrum sensing. In this paper, the frequency band of 2.411–2.433 GHz is considered. The resolution in the frequency domain is 1 MHz. Therefore, for each slot, 23 points in the frequency domain can be obtained, of which 13 points will be selected in the following experiment.

3.1.2. Experimental Validation. SVM will be exploited to classify the states (busy $l_i = 1$ or idle $l_i = 0$) of the measured Wi-Fi data with or without dimensionality reduction, given the true states. SVM will classify the states of the spectrum data at different time slots.

The DOF of the Wi-Fi frequency domain signals is extracted using the original 13 dimensions. The flow chart of the SVM processing combined with dimensionality reduction methods, including data processing, is shown in Figure 5.

The false alarm rate obtained by combining SVM with dimensionality reduction and employing only SVM is shown in Figure 6. The results are averaged over 50 experiments. In each experiment, the number of training sets is 200, and the number of testing sets is 1800.

The original dimension of the frequency domain data is varied from 1 to 13 for the SVM method. In addition, the SVM method is combined with the extracted dimensions from 1 to 13, obtained with dimensionality reduction.

In the whole experiment, a Gaussian RBF kernel with $2\sigma^2 = 5.5^2$ is used for KPCA. The parameter $k = 3$, in which k is the number of nearest neighbors of y_i (x_i) (including both training and testing sets) for LMVU. The optimization toolbox SeDuMi 1.1R3 [55] is applied to solve the optimization step in LMVU. The SVM toolbox SVM-KM [56] is used to train and test the SVM processes. The kernels selected for SVM are heavy-tailed RBF kernels with parameters $\gamma = 1$, $a = 1$, and $b = 1$. These parameters are kept constant for the whole experiment.

Experimental results show that with dimensionality reduction, the spectrum sensing performance is much better with fewer features than that without dimensionality reduction.

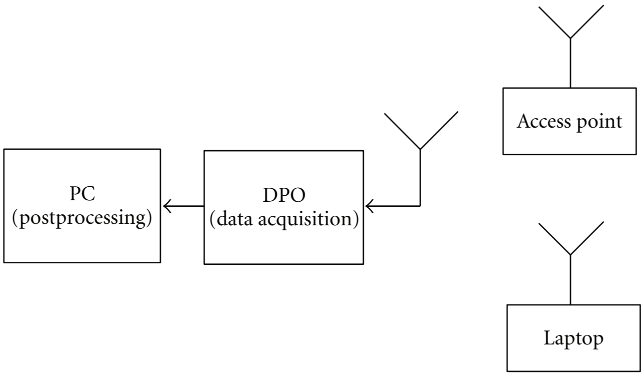


Figure 3: Setup of the measurement of Wi-Fi signals.

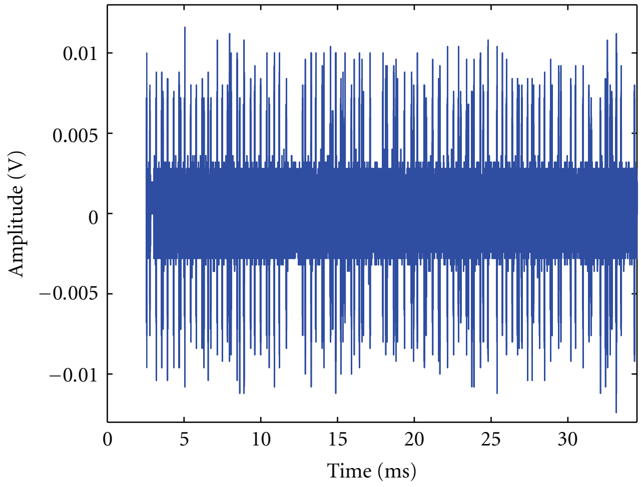


Figure 4: Recorded Wi-Fi signals in time domain.

3.2. Classifying Power System Disturbances Using SVM. Due to the large variability exhibited by the few power system disturbance data sets available, data sets are generated mathematically in this section for training purposes. In this way, a large number of data sets can be generated and used in training to ensure accurate SVM models.

Based on frequency and time domain analysis, and derived from typical disturbances, mathematical models for each disturbance can be formulated by the following signal equations:

(i) generation trip,

$$u(t) = \sin(\omega_0 t) + \alpha_1 e^{-c_1(t_{11}-t_{12})}\sin(\beta_1\omega_0(t_{11}-t_{12})) + \cdots$$
$$\alpha_2 e^{-c_2(t_{21}-t_{22})}\sin(\beta_2\omega_0(t_{11}-t_{12})) + \cdots, \qquad (1)$$

(ii) line trip,

$$u(t) = (1-\alpha(u(t_2)-u(t_1)))\sin(\omega_0 t), \qquad (2)$$

(iii) frequency oscillation,

$$u(t) = \sin(\omega_0 t) + \alpha e^{-c(t-t_1)}\sin(\beta\omega_0(t-t_1))\prod(t_2-t_1), \qquad (3)$$

where various terms are defined as follows: time window $\prod(t_2-t_1) = u(t_2)-u(t_1)$, ω_0 is a random frequency of basic frequency fluctuation, α is an additional signal factor, β is an additional frequency factor, c is the time constant, and t is the time period.

After carefully selecting the obtained parameters, such as amplitude, angles, frequency, and time period of each subfrequency component, enough examples can be generated by manipulating these parameters by random deviation within a tolerance range. Figures 7, 8, and 9 are the mesh patterns of 200 mathematical examples for the generation trip, line trip, and frequency oscillations, respectively.

SVM is a linear classifier in the parameter space, but it becomes a nonlinear classifier as a result of the nonlinear mapping of the space of the input patterns into the high-dimensional feature space [27]. Training an SVM model is a quadratic-optimization problem [57, 58]. The hyperplane represented by $\langle\omega,x\rangle + b = 0$ is constructed, so that the margin between the hyperplane and nearest point is maximized, where ω is the vector of hyperplane coefficients, b is a bias term, and $\langle\cdot\rangle$ denotes the inner product of two vectors.

Therefore, the classification function is $f(x;\omega,b) = \langle\omega,x\rangle + b$. An n-class classifier is constructed using the maximum value of the function $f_{ij}(x;\omega,b) = \langle\omega_{ij},x\rangle + b_{ij}$, $k = 1,\ldots,n$. For SVM, the problem can be solved by training data x_i^k, where $i = 1,\ldots,m$ data points.

Thus, the mathematical function between class i and class j is represented by the following equations:

$$\begin{gathered} f_{ij}(x;\omega,b) = \left\langle\omega_{ij},x\right\rangle + b_{ij} \\ \text{Minimize: } \frac{1}{2}\left\langle\omega_{ij},\omega_{ij}^T\right\rangle + \frac{C}{n}\sum_{n=1}^{N}\xi_n^{ij} \\ \text{Constraints: } y_n^{ij}\left(\left\langle\omega_{ij},\omega_{ij}^T\right\rangle + b_{ij}\right) \geq 1-\xi_n^{ij}, \\ \text{where } \xi_n^{ij} \geq 0, \\ y_n^{ij} = \begin{cases} +1 & \text{if } y_n = i\text{th class}, \\ -1 & \text{if } y_n = j\text{th class}. \end{cases} \end{gathered} \qquad (4)$$

The machine-learning package Weka is used to classify the data using an SVM multiclass algorithm. After being transformed to the Weka format, the input data includes three categories: generation trip, oscillation, and line trip. The data contains 200 examples of each category which is then divided into 2 equal sized groups. The first set is used for training, and the second set is used for verification. The verification results are as follows: generation trip can be classified with a success rate of 0.985, compared to 0.853 for the line trip, and 0.626 for the frequency oscillation.

3.3. Compressed Sensing-Based Smart Meter Reading. Compressed sensing, also known as compressive sensing, compressive sampling, or sparse sampling, is a technique for finding sparse solutions to underdetermined linear systems [59–63]. The concept of applying compressed sensing to smart meter reading was first proposed in [64]. A smart

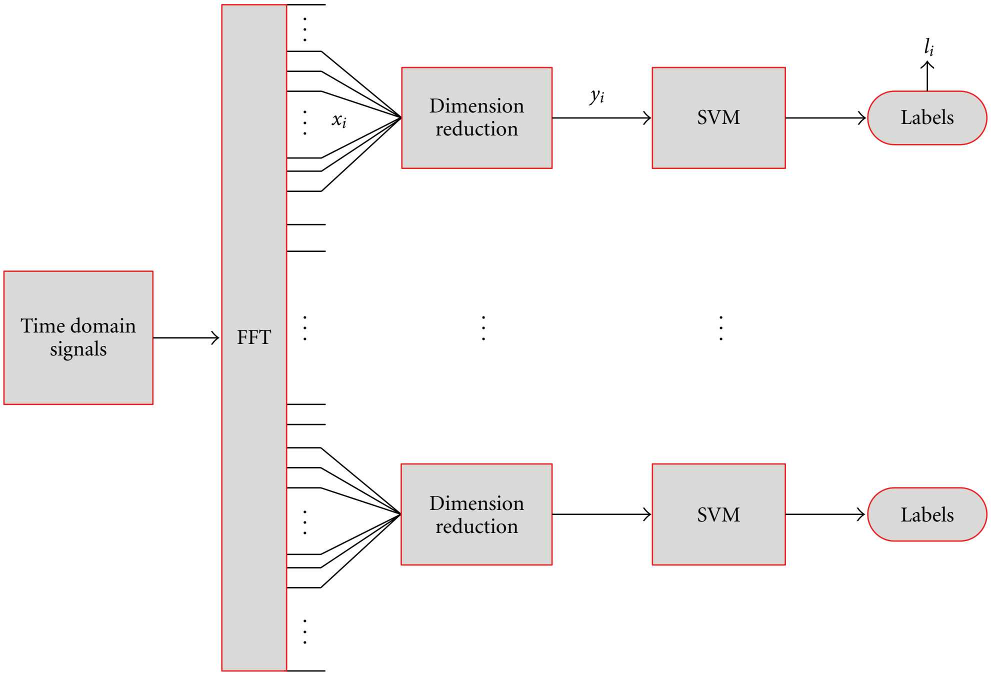


Figure 5: The flow chart of SVM combined with dimensionality reduction.

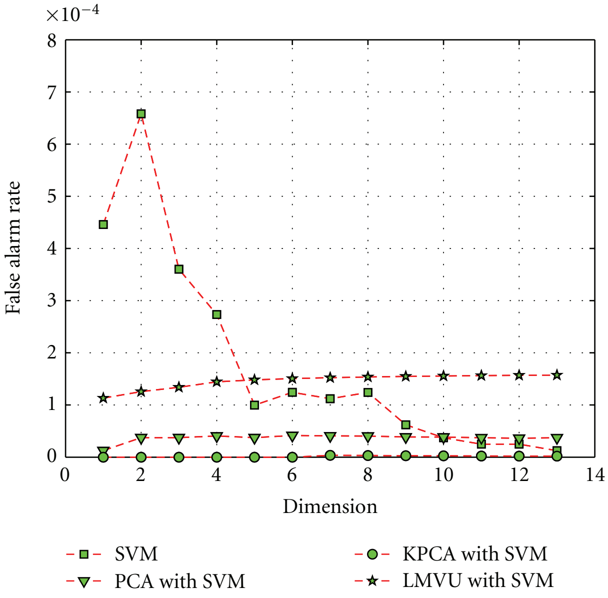


Figure 6: False alarm rate.

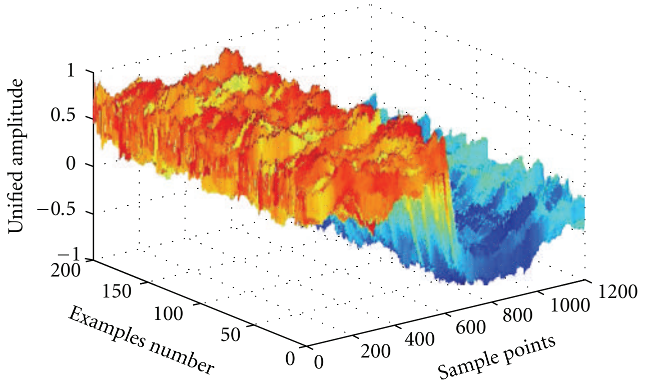


Figure 7: Mesh patterns of 200 examples for generation trip.

meter is an intelligent electrical meter that conveys information to the central power station regarding significant changes in the power load either through two-way wireless or power line communications. Since the power consumption in a particular home does not dynamically vary, the number of smart meters simultaneously transmitting is very small compared to the total number of meters in a particular cognitive smart grid network. As a result, the sparsity of the smart meter data transmission to the central processing node or access point (AP) was exploited in [64] for applying the principle of compressed sensing. However, in [64], it was assumed that the noise is bounded. In this paper, the newly proposed techniques of Bayesian compressive sensing [65], and compressed sensing kalman filter [66] are applied for smart meter reading when the noise is Gaussian distributed.

3.3.1. Bayesian Compressed Sensing. Consider an N-dimensional signal y that is compressible in some basis function A, that is, y can be accurately reconstructed with a small number K of basis-function coefficients, where $K \ll N$. In other words, the basis coefficient vector s is a sparse vector with a majority of components close to 0. Compressive sensing states that it is possible to recover these basis-function coefficients with fewer measurements $M < N$ of y. This is accomplished by a linear transformation of y

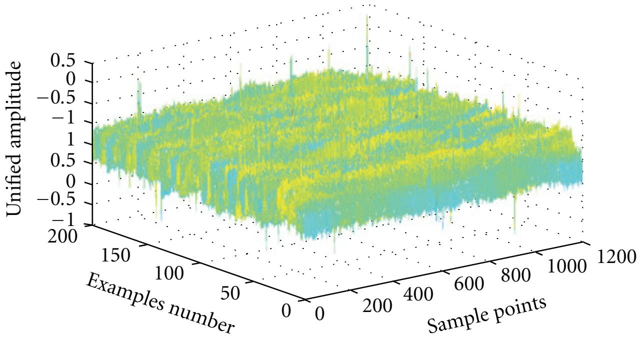


Figure 8: Mesh patterns of 200 examples for line trip.

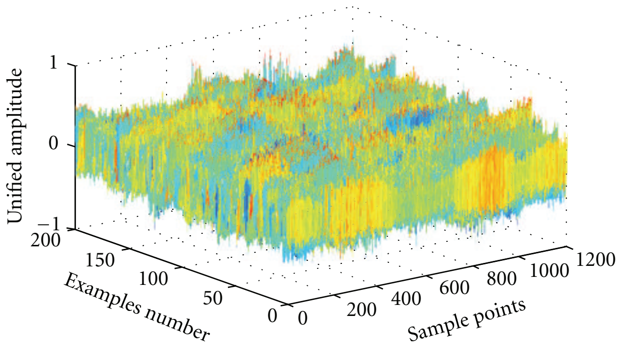


Figure 9: Mesh patterns of 200 examples for frequency oscillation.

onto an $M \times N$ matrix H to generate an M-dimensional measurement vector z. Mathematically, z can be represented as

$$z = y^T AH. \tag{5}$$

Since we have $y = As$, (5) becomes

$$z = Hs. \tag{6}$$

The expression in (6) is an underdetermined system; hence, the estimate of s is ill conditioned. However, since s is sparse with respect to A, (6) can be solved as a l_1 norm minimization problem as follows:

$$\hat{s} = \arg\min_{s}\left[\|z - Hs\|_2^2 + \lambda\|s\|_1\right]. \tag{7}$$

The scalar λ decides the weightage given to the Euclidean error and the sparseness constraints in the first and second terms of (7), respectively.

The above optimization problem can be solved using many linear programming techniques such as basis pursuit (BP) [67], matching pursuit (MP) [68], and orthogonal matching pursuit (OMP) [69]. In [65], a Bayesian approach is employed to estimate s from the compressed measurements z. Hence, by imposing a Laplace sparseness prior on s, and assuming a Gaussian likelihood model for z, the solution for (7) becomes a maximum a posterior (MAP) estimate for s.

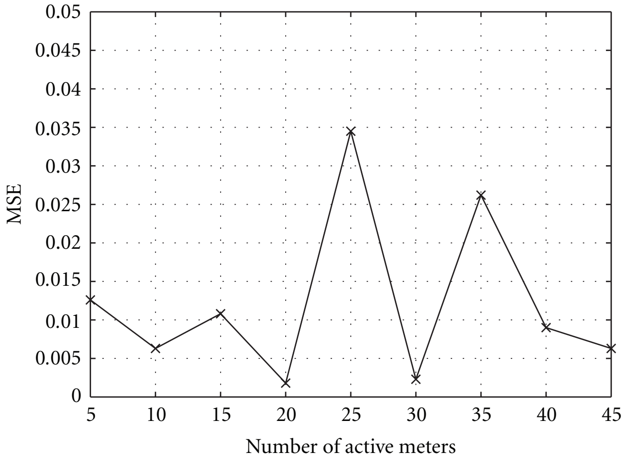


Figure 10: MSE achieved by BCS for different number of active meters.

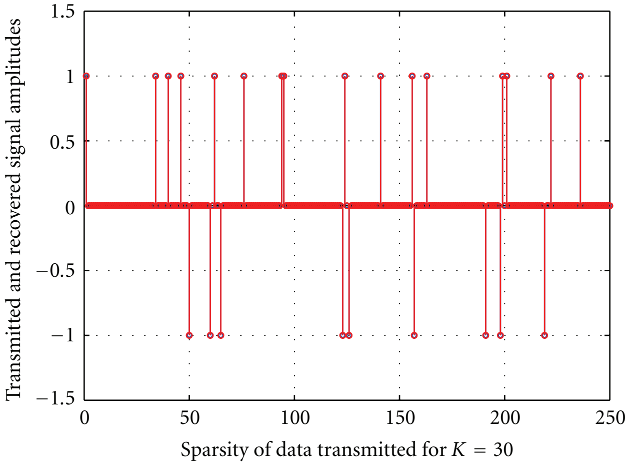


Figure 11: Sparsity of data transmitted for $K = 30$.

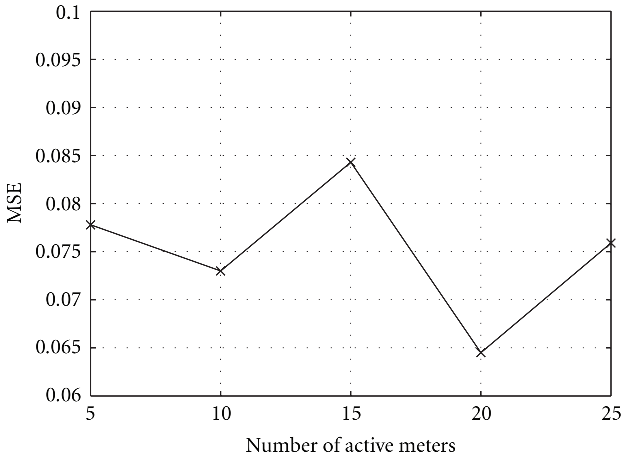


Figure 12: MSE achieved by CSKF for different number of active meters.

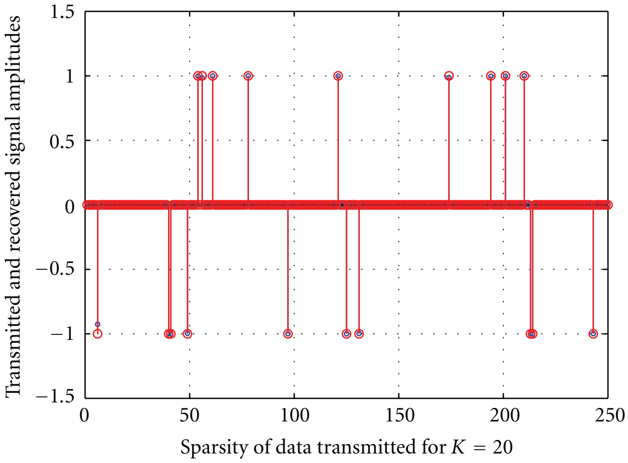


Figure 13: Sparsity of data transmitted for $K = 20$.

3.3.2. Kalman Filter-Based Compressed Sensing. The kalman filter is a recursive filter that estimates the state of a process or system from a series of noisy observations [70–72]. The kalman filter optimally estimates the true state of the system by making a prediction, estimating the error in the prediction, and computing a weighted average of the predicted value and the measured value. Therefore, the mathematical equations for the kalman filter can be separated into time updates or prediction and measurement updates or correction. Due to its versatility, the kalman filter has been used in diverse engineering applications such as digital signal processing, control systems, wireless communications, image processing, and weather forecasting [73–78].

Recently, a new kalman filtering approach for the recovery of sparse signals was proposed, called compressed sensing embedded kalman filter (CSKF-1) [66, 79]. The CSKF-1 adopts the pseudomeasurement (PM) technique [80] to incorporate a fictitious measurement in the kalman filtering process to satisfy the sparseness constraint. The PM can be expressed as

$$\begin{aligned} 0 &= \hat{H}s - \delta, \\ \hat{H} &= [\operatorname{sign}(s(1), s(2), \ldots, s(N))], \end{aligned} \tag{8}$$

where $\operatorname{sign}(s(k)) = 1$ if $s(k) \geq 0$, and -1 otherwise.

δ is the tuning parameter which controls the sparsity of the solution state vector.

3.3.3. System Description and Signal Model. As mentioned in the previous section, the smart meter data transmission to the AP is sparse in nature, that is, only a small percentage of meters would be actively transmitting data at any time. Therefore, the principles of compressed sensing can be readily applied to the recovery of the data reports. The main advantage of employing compressed sensing is that it allows the smart meters to transmit simultaneously, as opposed to the popular carrier sense multiple access (CSMA) protocol, which uses a random backoff to avoid collisions in transmissions. This could result in significant delay in data recovery.

The system consists of N smart meters managed by an AP. In each frame, synchronization and channel estimation is performed, followed by data transmission. The synchronization and channel estimation can be performed by transmitting a pilot signal to the meters during the assigned periods in the frame and is beyond the scope of this paper. However, it is assumed that the channel parameters are flat fading in nature, with a large coherence time indicating a slow time-varying channel. The data transmission section in the frame is divided into several time slots during which the active smart meters can simultaneously transmit their readings. In mathematical form, the data transmission received by the AP at time t can be expressed as

$$z(t) = \sum_{i=1}^{N} p_i(t) c_i s_i + w(t) \tag{9}$$

c_i is the flat-fading channel parameter between meter i and the AP, $p_i(t)$ is the pseudorandom spreading code at time t for meter i, s_i is the data transmitted by meter i, $w(t)$ is the Gaussian distributed noise term. The spreading code is known only to the AP and meters, preventing unauthorized people from accessing and tampering with the data. Suppose that the data transmission period has T time slots, then the above signal model can be rewritten in matrix-vector form as follows:

$$Z = HS + W, \tag{10}$$

where

$$H = PC, \tag{11}$$

$$C = \operatorname{diag}(c_1, c_2, \ldots, c_N), \tag{12}$$

$$P_{t,i} = [p_i(1), p_i(2), \ldots, p_i(T)]^T, \tag{13}$$

$$Z = [z(1), z(2), \ldots, z(T)]^T, \tag{14}$$

$$S = [s_1, s_2, \ldots, s_N]^T, \tag{15}$$

$$W = [w(1), w(2), \ldots, w(T)]^T. \tag{16}$$

Since the number K of meters simultaneously transmitting is small, $K \ll N$. As a result, the vector S in (15) is sparse. It can therefore be easily inferred that (10) is identical to the CS equation (6), with the exception of additive Gaussian noise. Hence, the recovery of the smart meter reading would correspond to the optimization problem in (7). In the simulations, the total number of smart meters, N, in the cognitive smart grid network is considered to be 250, and the length of the observation vector/time slots T is 100. Binary phase shift keying (BPSK) modulation is considered. The mean square error (MSE) between the actual data vector and the estimated data vector is used as the measure of performance. The MSE is plotted for different number of active meters K or sparsity of the data transmission.

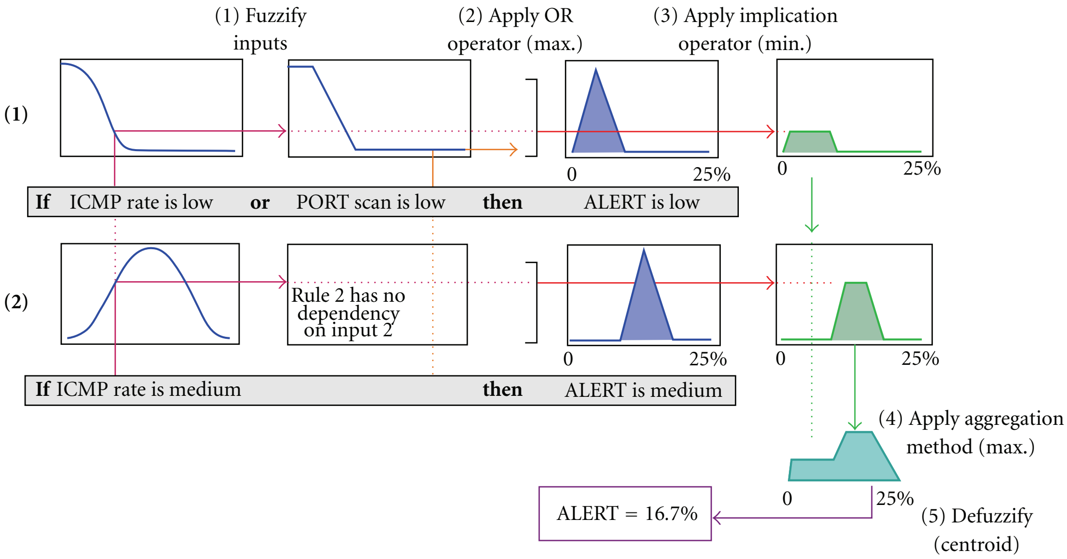

(1) Fuzzify inputs
(2) Apply OR operator (max.)
(3) Apply implication operator (min.)
(1)
0
25%
0
25%
If ICMP rate is low or PORT scan is low then ALERT is low
(2)
Rule 2 has no dependency on input 2
0
25%
0
25%
If ICMP rate is medium then ALERT is medium
(4) Apply aggregation method (max.)
0
25%
ALERT = 16.7%
(5) Defuzzify (centroid)

Figure 14: Fuzzy Logic example applied to IDS.

3.3.4. Bayesian Compressive Sensing for Smart Meter Reading. In this section, the smart grid data recovery problem in (6) is treated as a linear regression problem and is considered from a Bayesian perspective, as proposed in [65]. A hierarchical sparseness prior is imposed on S, and sparse Bayesian learning using the relevance vector machine (RVM) [81] is performed. The MSE achieved by the BCS algorithm for different values of K is illustrated in Figure 10. For the case of $K = 30$, the sparsity of the data transmitted along with the recovered data is illustrated in Figure 11.

3.3.5. Compressed Sensing Kalman Filter Approach. In this section, the recently proposed CSKF algorithm is employed for the recovery of data at the AP. The total number of smart meters in the network is assumed to be 250, and T is 150. The MSE yielded for various number of active meters K is shown in Figure 12, respectively. A comparison between the amplitudes of the transmitted and recovered signal versus the sparsity of meter transmission is shown in Figure 13.

3.4. FPGA-Based Fuzzy Logic Intrusion Detection for Smart Grid. Artificial intelligence techniques such as fuzzy logic, bayesian inference, neural networks, and other methods can be employed to enhance the security gaps in conventional IDSs. As shown in Figure 14, a fuzzy logic approach was used in [82], in which different variables that influence the inference of an attack can be analyzed and later combined for the decision-making process of a security device. Additionally, if each security device serving as an IDS is aware not only of itself, but also of a limited number (depending on local resources and traffic) of surrounding trusted IDS devices, the alerts that these other devices generate can be used to adjust local variables or parameters to better cope with distributed attacks and more accurately detect their presence.

The research and development of robust and secure communication protocols, dynamic spectrum sensing, and distributed and collaborative security should be considered as an inherent part of smart grid architecture. An advanced decentralized and secure infrastructure needs to be developed with two-way capabilities for communicating information and controlling equipment, among other tasks, as indicated in the recently published “Guidelines for Smart Grid Cyber Security Vol.1” by the National Institute of Standards and Technologies. The complexity of such an endeavor, coupled with the amalgam of technologies and standards that will coexist in the development of the smart grid, makes it extremely necessary to have a common platform of development, with flexibility and reliable performance.

Field programmable gate arrays (FPGAs) development platforms share these advantages, not to mention the fact that a single silicon FPGA chip can be used to study several smart grid technologies and their implementations. FPGA chips offer significant potential for application in the smart grid for performing encryption and decryption, intrusion detection, low-latency routing, data acquisition and signal processing, parallelism, configurability of hardware devices, and high-performance and high-bandwidth tamper-resistant applications. Dr. William Sanders, a member of the Smart Grid Advisory Committee of the National Institute of Standards and Technology (NIST), has been in the recent years among the most influential persons in the research of smart grid security. His research team and several collaborating universities proposed the use of a Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) that focuses on the security of low-level devices and communications, as well as trustworthy operation of the power grid under a variety of conditions including cyber attacks and emergencies [83]. TCIPG proposes a coordinated response and detection at multiple layers of the cyber-infrastructure hierarchy including but not limited to sensor/actuator and substation levels. At these levels of the hierarchy, software defined radio and wireless communications technologies could be used and studied to prevent attacks such as wireless jamming.

Dr. Sanders also proposes the use of specifications-based IDS in protecting advanced metering infrastructures (AMIs) [84]. A distributed FPGA-based network with adaptive and cooperative capabilities can be used to study several security and communication aspects of this infrastructure both from the attackers and defensive point of view.

4. Conclusions

In this paper, the integration of two emerging technologies, namely, the cognitive radio and smart grid is addressed. The concept of dimensionality reduction is presented as a possible preprocessing method to extract the intrinsic dimensionality of high-dimensional data. Using Wi-Fi signal measurements, the effectiveness of the PCA, KPCA, and LVMU dimensionality reduction techniques in conjunction with the SVM method is provided in a spectrum sensing application. In addition, the SVM technique is used for suitably classifying the power system disturbances. For the recovery of sparse smart meter transmissions, experimental results obtained by employing the Bayesian compressed sensing and compressed sensing kalman filter approaches are given for BPSK data. Finally, the critical issue of smart grid security is addressed, and a possible approach for achieving this is presented using FPGA-based fuzzy logic intrusion detection.

Acknowledgments

This work is funded by the National Science Foundation through Grants (ECCS-0901420), (ECCS-0821658), and (ECCS-0622125) and the Office of Naval Research through two Contracts (N00014-07-1-0529 and N00014-11-1-0006).

References

[1] J. Mitola III and G. Q. Maguire Jr., "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.

[2] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, 2005.

[3] G. Ganesan, Y. Li, B. Bing, and S. Li, "Spatiotemporal sensing in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 5–12, 2008.

[4] J. Bazerque and G. Giannakis, "Distributed spectrum sensing for cognitive radio networks by exploiting sparsity," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1847–1862, 2010.

[5] C. Cordeiro, K. Challapali, D. Birru et al., "IEEE 802.22: an introduction to the first wireless standard based on cognitive radios," *Journal of Communications*, vol. 1, no. 1, pp. 38–47, 2006.

[6] C. Cordeiro, K. Challapali, D. Birru, and N. Sai Shankar, "IEEE 802.22: the first worldwide wireless standard based on cognitive radios," in *Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN '05)*, pp. 328–337, Baltimore, Md, USA, November 2005.

[7] C. Cordeiro, K. Challapali, and M. Ghosh, "Cognitive PHY and MAC layers for dynamic spectrum access and sharing of TV bands," in *Proceedings of the 1st International Workshop on Technology and Policy for Accessing Spectrum*, vol. 222, p. 3, ACM, New York, NY, USA, 2006.

[8] C. Stevenson, G. Chouinard, Z. Lei, W. Hu, S. Shellhammer, and W. Caldwell, "IEEE 802.22: the first cognitive radio wireless regional area network standard," *IEEE Communications Magazine*, vol. 47, no. 1, pp. 130–138, 2009.

[9] Z. Jiang, "Computational intelligence techniques for a smart electric grid of the future," in *Proceedings of the 6th International Symposium on Neural Networks on Advances in Neural Networks (ISNN '09)*, pp. 1191–1201, 2009.

[10] Z. Wang, A. Scaglione, and R. J. Thomas, "Compressing electrical power grids," in *Proceedings of the 1st IEEE International Conference on Smart Grid Communications (SmartGridComm '10)*, pp. 13–18, 2010.

[11] A. Mohsenian-Rad, V. Wong, J. Jatskevich, and R. Schober, "Optimal and autonomous incentive-based energy consumption scheduling algorithm for smart grid," in *Proceedings of the Innovative Smart Grid Technologies (ISGT '10)*, pp. 1–6, Citeseer, Gaithersburg, Md, USA, January 2010.

[12] S. Caron and G. Kesidis, "Incentive-based energy consumption scheduling algorithms for the smart grid," in *Proceedings of the 1st IEEE International Conference on Smart Grid Communications*, pp. 391–396, Gaithersburg, Md, USA, October 2010.

[13] A. L. Dimeas and N. D. Hatziargyriou, "Operation of a multiagent system for microgrid control," *IEEE Transactions on Power Systems*, vol. 20, no. 3, pp. 1447–1455, 2005.

[14] S. Hatami and M. Pedram, "Minimizing the electricity bill of cooperative users under a Quasi-Dynamic Pricing Model," in *Proceedings of the 1st IEEE International Conference on Smart Grid Communications (SmartGridComm '10)*, pp. 421–426, IEEE, 2010.

[15] P. Samadi, A. Mohsenian-Rad, R. Schober, V. Wong, and J. Jatskevich, "Optimal real-time pricing algorithm based on utility maximization for smart grid," in *Proceedings of the IEEE International Conference on Smart Grid (SmartGridComm '10)*, Gaithersburg, Mass, USA, October 2010.

[16] J. F. Hauer, N. B. Bhatt, K. Shah, and S. Kolluri, "Performance of "WAMS East" in providing dynamic information for the North East blackout of August 14, 2003," in *Proceedings of the IEEE Power Engineering Society General Meeting*, pp. 1685–1690, IEEE, Denver, Colo, USA, June 2004.

[17] D. Divan, G. A. Luckjiff, W. E. Brumsickle, J. Freeborg, and A. Bhadkamkar, "A grid information resource for nationwide real-time power monitoring," *IEEE Transactions on Industry Applications*, vol. 40, no. 2, pp. 699–705, 2004.

[18] B. Qiu, L. Chen, V. Centeno, X. Dong, and Y. Liu, "Internet based frequency monitoring network (FNET)," in *Proceedings of the IEEE Power Engineering Society Winter Meeting*, vol. 3, pp. 1166–1171, IEEE, 2002.

[19] A. G. Phadke, "Synchronized phasor measurements in power systems," *IEEE Computer Applications in Power*, vol. 6, no. 2, pp. 10–15, 1993.

[20] Z. Zhong, C. Xu, B. J. Billian et al., "Power system frequency monitoring network (FNET) implementation," *IEEE Transactions on Power Systems*, vol. 20, no. 4, pp. 1914–1921, 2005.

[21] S. Tsai, Z. Zhong, J. Zuo, and Y. Liu, "Analysis of wide-area frequency measurement of bulk power systems," in *Proceedings of the IEEE Power Engineering Society General Meeting*, Montreal, Canada, June 2006.

[22] C. Chang, A. Liu, and C. Huang, "Oscillatory stability analysis using real-time measured data," *IEEE Transactions on Power Systems*, vol. 8, no. 3, pp. 823–829, 2002.

[23] C. Chunling, X. Tongyu, P. Zailin, and Y. Ye, "Power quality disturbances classification based on multi-class classification SVM," in *Proceedings of the 2nd International Conference on Power Electronics and Intelligent Transportation System (PEITS '09)*, vol. 1, pp. 290–294, IEEE, 2009.

[24] P. Gao and W. Wu, "Power quality disturbances classification using wavelet and support vector machines," in *Proceedings of the 6st International Conference on Intelligent Systems Design and Applications, (ISDA '06)*, pp. 201–206, October 2006.

[25] A. M. Gaouda, S. H. Kanoun, M. M. A. Salama, and A. Y. Chikhani, "Pattern recognition applications for power system disturbance classification," *IEEE Transactions on Power Delivery*, vol. 17, no. 3, pp. 677–683, 2002.

[26] F. Melgani and Y. Bazi, "Classification of electrocardiogram signals with support vector machines and particle swarm optimization," *IEEE Transactions on Information Technology in Biomedicine*, vol. 12, no. 5, pp. 667–677, 2008.

[27] I. Guler and E. D. Ubeyli, "Multiclass support vector machines for EEG-signals classification," *IEEE Transactions on Information Technology in Biomedicine*, vol. 11, no. 2, pp. 117–126, 2007.

[28] C. Cortes and V. Vapnik, "Support-vector networks," *Machine Learning*, vol. 20, no. 3, pp. 273–297, 1995.

[29] N. I. of Standards and Technologies, "Guidelines for grid security, vol 1," Tech. Rep., 2010, http://csrc.nist.gov/publications/PubsNISTIRs.html.

[30] M. Pazos-Revilla and A. Siraj, "An experimental model of an fpga-based intrusion detection systems," in *Proceedings of the 26th International Conference on Computers and Their Applications*, 2011.

[31] R. C. Qiu, Z. Chen, N. Guo et al., "Towards a real-time cognitive radio network testbed: architecture, hardware platform, and application to smart grid," in *Proceedings of the 5th IEEE Workshop on Networking Technologies for Software-Defined Radio and White Space*, June 2010.

[32] Z. Chen, N. Guo, and R. C. Qiu, "Building A cognitive radio network testbed," in *Proceedings of the IEEE Southeastcon*, Nashville, Tenn, USA, March 2011.

[33] R. C. Qiu, "Cognitive radio network testbed," Funded Research Proposal for Defense University Research Instrumentation Program (DURIP), August 2009, http://www.defense.gov/news/Fiscal 2010 DURIP Winners List.pdf.

[34] R. C. Qiu, "Cognitive radio and smart grid," Invited Presentation at IEEE Chapter, February 2010, http://iweb.tntech.edu/rqiu.

[35] R. C. Qiu, "Cogntiive radio institute," Funded research proposal for 2010 Defense Earmark, 2010, http://www.opensecrets.org/politicians/earmarks.php?cid=N00003126.

[36] R. C. Qiu, "Smart grid research at TTU," Presented at Argonne National Laboratory, February 2010, http://iweb.tntech.edu/rqiu/publications.htm.

[37] R. Qiu, Z. Hu, G. Zheng, Z. Chen, and N. Guo, "Cognitive radio network for the Smart Grid: experimental system architecture, control algorithms, security, and microgrid testbed," *IEEE Transactions on Smart Grid*. In press.

[38] R. C. Qiu, M. C. Wicks, Z. Hu, L. Li, and S. J. Hou, "Wireless tomography(part1): a novel approach to remote sensing," in *Proceedings of the 5th International Waveform Diversity and Design Conference*, Niagara Falls, Canada, August 2010.

[39] M. Amin and B. Wollenberg, "Toward a smart grid: power delivery for the 21st century," *IEEE Power and Energy Magazine*, vol. 3, no. 5, pp. 34–41, 2005.

[40] J. Cupp and M. Beehler, "Implementing smart grid communications," 2008.

[41] A. Ghassemi, S. Bavarian, and L. Lampe, "Cognitive radio for smart grid communications," in *Proceedings of the 1st IEEE International Conference on Smart Grid Communications (SmartGridComm '10)*, pp. 297–302, IEEE, Gaithersburg, Md, USA, 2010.

[42] N. Ghasemi and S. M. Hosseini, "Comparison of smart grid with cognitive radio: solutions to spectrum scarcity," in *Proceedings of the 12th International Conference on Advanced Communication Technology (ICACT '10)*, vol. 1, pp. 898–903, February 2010.

[43] J. Lee and M. Verleysen, *Nonlinear Dimensionality Reduction*, Springer, London, UK, 2007.

[44] I. T. Jolliffe, *Principal Component Analysis*, Springer, London, UK, 2002.

[45] B. Schölkopf, A. Smola, and K. R. Müller, "Nonlinear component analysis as a kernel eigenvalue problem," *Neural Computation*, vol. 10, no. 5, pp. 1299–1319, 1998.

[46] K. Q. Weinberger and L. K. Saul, "Unsupervised learning of image manifolds by semidefinite programming," *International Journal of Computer Vision*, vol. 70, no. 1, pp. 77–90, 2006.

[47] K. Weinberger, B. Packer, and L. Saul, "Nonlinear dimensionality reduction by semidefinite programming and kernel matrix factorization," in *Proceedings of the 10th International Workshop on Artificial Intelligence and Statistics*, pp. 381–388, 2005.

[48] V. Vapnik, *The Nature of Statistical Learning Theory*, Springer, London, UK, 2000.

[49] V. Vapnik, *Statistical Learning Theory*, Wiley, New York, NY, USA, 1998.

[50] V. Vapnik, S. Golowich, and A. Smola, "Support vector method for function approximation, regression estimation, and signal processing," in *Advances in Neural Information Processing Systems*, M. Mozer, M. Jordan, and T. Petsche, Eds., pp. 281–287, MIT Press, Cambridge, Mass, USA, 1997.

[51] C. J. C. Burges, "A tutorial on support vector machines for pattern recognition," *Data Mining and Knowledge Discovery*, vol. 2, no. 2, pp. 121–167, 1998.

[52] A. J. Smola and B. Schölkopf, "A tutorial on support vector regression," *Statistics and Computing*, vol. 14, no. 3, pp. 199–222, 2004.

[53] N. Cristianini and J. Shawe-Taylor, *An Introduction to Support Vector Machines: and Other Kernel-Based Learning Methods*, Cambridge University Press, Cambridge, UK, 2000.

[54] Z. Chen and R. C. Qiu, "Prediction of channel state for cognitive radio using higher-order hidden Markov model," in *Proceedings of the IEEE Southeast Conference*, pp. 276–282, March 2010.

[55] J. Sturm, "The advanced optimization laboratory at McMaster university, Canada. SeDuMi version 1.1 R3," 2006.

[56] S. Canu, Y. Grandvalet, V. Guigue, and A. Rakotomamonjy, *Svm and Kernel Methods Matlab Toolbox*, Perception Systmes et Information, INSA de Rouen, Rouen, France, 2005.

[57] D. Fradkin and I. Muchnik, "Support vector machines for classification," *Discrete Methods in Epidemiology*, vol. 70, pp. 13–20, 2006.

[58] K. Bennett and C. Campbell, "Support vector machines: hype or hallelujah?" *ACM SIGKDD Explorations Newsletter*, vol. 2, no. 2, pp. 1–13, 2000.

[59] D. L. Donoho, “Compressed sensing,” *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

[60] Y. Tsaig and D. L. Donoho, “Extensions of compressed sensing,” *Signal Processing*, vol. 86, no. 3, pp. 549–571, 2006.

[61] E. Candès, “The restricted isometry property and its implications for compressed sensing,” *Comptes Rendus Mathematique*, vol. 346, no. 9-10, pp. 589–592, 2008.

[62] E. Candès, J. Romberg, and T. Tao, “Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information,” *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 489–509, 2006.

[63] Z. Tian and G. B. Giannakis, “Compressed sensing for wideband cognitive radios,” in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP ’07)*, vol. 4, pp. 1357–1360, 2007.

[64] L. Husheng, M. Rukun, L. Lifeng, and R. Qiu, “Compressed meter reading for delay-sensitive and secure load report in smart grid,” in *Proceedings of the 1st IEEE International Conference on Smart Grid Communications (SmartGridComm ’10)*, 2010.

[65] S. Ji, Y. Xue, and L. Carin, “Bayesian compressive sensing,” *IEEE Transactions on Signal Processing*, vol. 56, no. 6, pp. 2346–2356, 2008.

[66] A. Carmi, P. Gurfil, and D. Kanevsky, “Methods for sparse signal recovery using Kalman filtering with embedded pseudo-measurement norms and quasi-norms,” *IEEE Transactions on Signal Processing*, vol. 58, no. 4, pp. 2405–2409, 2010.

[67] S. S. Chen, D. L. Donoho, and M. A. Saunders, “Atomic decomposition by basis pursuit,” *SIAM Review*, vol. 43, no. 1, pp. 129–159, 2001.

[68] S. G. Mallat and Z. Zhang, “Matching pursuits with time-frequency dictionaries,” *IEEE Transactions on Signal Processing*, vol. 41, no. 12, pp. 3397–3415, 1993.

[69] J. A. Tropp and A. C. Gilbert, “Signal recovery from random measurements via orthogonal matching pursuit,” *IEEE Transactions on Information Theory*, vol. 53, no. 12, pp. 4655–4666, 2007.

[70] R. Meinhold and N. Singpurwalla, “Understanding the Kalman filter,” *American Statistician*, vol. 37, no. 2, pp. 123–127, 1983.

[71] R. Kalman et al., “A new approach to linear filtering and prediction problems,” *Journal of Basic Engineering*, vol. 82, no. 1, pp. 35–45, 1960.

[72] S. Haykin, *Adaptive Filter Theory*, Pearson Education, Dorling Kindersley ,India, 2008.

[73] E. Wan and R. van der Merwe, “The unscented Kalman filter for nonlinear estimation,” in *Proceedings of the Adaptive Systems for Signal Processing, Communications, and Control Symposium (AS-SPCC ’00)*, pp. 153–158, IEEE, 2000.

[74] G. Evensen, “The ensemble Kalman filter: theoretical formulation and practical implementation,” *Ocean Dynamics*, vol. 53, no. 4, pp. 343–367, 2003.

[75] L. Ma, K. Wu, and L. Zhu, “Fire smoke detection in video images using Kalman filter and Gaussian mixture color model,” in *Proceedings of the International Conference on Artificial Intelligence and Computational Intelligence (AICI ’10)*, vol. 1, pp. 484–487, IEEE, Sanya, China, 2010.

[76] L. Ljung, “Asymptotic behavior of the extended Kalman filter as a parameter estimator for linear systems,” *IEEE Transactions on Automatic Control*, vol. 24, no. 1, pp. 36–50, 2002.

[77] R. van der Merwe and E. Wan, “The square-root unscented Kalman filter for state and parameter-estimation,” in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP ’01)*, vol. 6, pp. 3461–3464, IEEE, Salt Lake City, Utah, USA, 2001.

[78] A. Lakhzouri, E. Lohan, R. Hamila, and M. Renfors, “Extended Kalman filter channel estimation for line-of-sight detection in WCDMA mobile positioning,” *EURASIP Journal on Applied Signal Processing*, vol. 2003, pp. 1268–1278, 2003.

[79] D. Kanevsky, A. Carmi, L. Horesh, P. Gurfil, B. Ramabhadran, and T. Sainath, “Kalman filtering for compressed sensing,” in *Proceedings of the 13th Conference on Information Fusion (FUSION ’10)*, pp. 1–8, Edinburgh, UK, July 2010.

[80] S. J. Julier and J. J. LaViola, “On Kalman filtering with nonlinear equality constraints,” *IEEE Transactions on Signal Processing*, vol. 55, no. 6, pp. 2774–2784, 2007.

[81] M. E. Tipping, “Sparse bayesian learning and the relevance vector machine,” *Journal of Machine Learning Research*, vol. 1, no. 3, pp. 211–244, 2001.

[82] M. Pazos-Revilla, *Fpga based fuzzy intrusion detection system for network security*, M.S. thesis, Tennessee Technological University, Cookeville, Tenn, USA, 2010.

[83] W. Sanders, “Tcip: trustworthy cyber infrastructure for the power grid,” Tech. Rep., Information Trust Institute, University of Illinois at Urbana-Champaign, 2011.

[84] R. Berthier, W. Sanders, and H. Khurana, “Intrusion detection for advanced metering infrastructures: requirements and architectural directions,” in *Proceedings of the 1st IEEE International Conference on Smart Grid Communications (SmartGridComm ’10)*, pp. 350–355, IEEE, Gaithersburg, Md, USA, October 2010.

Hindawi Publishing Corporation
International Journal of Digital Multimedia Broadcasting
Volume 2011, Article ID 851951, 6 pages
doi:10.1155/2011/851951

Research Article

Location Discovery Based on Fuzzy Geometry in Passive Sensor Networks

Rui Wang,[1] Wenming Cao,[2] and Wanggen Wan[1]

[1] *School of Communication and Information Engineering, Shanghai University, Shanghai 200072, China*
[2] *School of Information Engineering, Shenzhen University, Shenzhen 518060, China*

Correspondence should be addressed to Rui Wang, rwang@shu.edu.cn

Received 1 November 2010; Accepted 1 April 2011

Academic Editor: Chi Zhou

Location discovery with uncertainty using passive sensor networks in the nation's power grid is known to be challenging, due to the massive scale and inherent complexity. For bearings-only target localization in passive sensor networks, the approach of fuzzy geometry is introduced to investigate the fuzzy measurability for a moving target in R^2 space. The fuzzy analytical bias expressions and the geometrical constraints are derived for bearings-only target localization. The interplay between fuzzy geometry of target localization and the fuzzy estimation bias for the case of fuzzy linear observer trajectory is analyzed in detail in sensor networks, which can realize the 3-dimensional localization including fuzzy estimate position and velocity of the target by measuring the fuzzy azimuth angles at intervals of fixed time. Simulation results show that the resulting estimate position outperforms the traditional least squares approach for localization with uncertainty.

1. Introduction

Wireless sensor network localization in smart grid is an important area that attracted significant research interest. As a national smart grid constructed, it is important for developers to consider target localization problems to ensure both the smart grid operation efficiently. The objective of location discovery in sensor networks for smart grid is to estimate the location of a target from measurements collected by a single moving sensor or several fixed sensors at distinct and known locations.

For passive bearings-only localization, the sensor node detects the signals transmitted by a target to generate directional information in the form of bearing measurements. These measurements are triangulated to estimate the target location. While triangulation yields a unique intersection point for bearing lines in the absence of measurement errors, the noise present in bearing and observer measurements requires an optimal solution to be formulated based on noisy measurements; hence, statistical techniques for bearings-only target localization is introduced.

The pioneering work of Stansfield [1] provided a closed-form small error approximation of the maximum likelihood estimator in 1947. It is shown in [2] that the Stansfield estimator is asymptotically biased, where the traditional maximum likelihood (TML) formulation is examined in detail including a bias and variance analysis. A linearized least squares approach to bearings-based localization is given in [3]. The linearized and iterative algorithms typically require an initial estimate of the target location [2–5]. Liu et al. [6] proposed a vertical localization method using Euclidean geometry theory.

The practical passive target localization in sensor networks is characterized by a certain degree of uncertainty, which may result from approximate definition of the measurand, limited knowledge of the real environment, variability of influence quantities, inexact values of reference standards or parameters used in the model, background noise of the electronic devices, and so on. Especially, there exists uncertainty (fuzziness) with sensor locations and measurements, which can be studied based on fuzzy geometry. Rosenfeld [7] first discussed some concepts and properties of fuzzy plane geometry. Buckley and Eslami [8, 9] proposed another theory of fuzzy plane geometry, where the distances between fuzzy points, fuzzy area, and fuzzy circumference is considered as fuzzy numbers. Inspired by the authors in [7–9], the approach of fuzzy geometry is introduced to investigate the passive bearings-only target localization for the case of fuzzy linear observer trajectory in passive sensor networks.

The paper is organized as follows. The concept of fuzzy geometry is provided in Section 2. A novel analysis approach of passive bearings-only target localization based on fuzzy geometry theory for the case of fuzzy linear observer trajectory is proposed in Section 3. Simulation examples are presented in Section 4 to validate the theoretical findings of the paper. Section 5 concludes the paper.

2. Fuzzy Geometry

In this section, fuzzy points and fuzzy lines in fuzzy geometry are introduced. Place a "bar" over a capital letter to denote a fuzzy subset of R^n $(n = 1, 2, 3)$ such as, $\overline{X}, \overline{Y}, \overline{A}$, and $\overline{B}$. Any fuzzy set is defined by its membership function. If $\overline{A}$ is a fuzzy subset of R^n $(n = 1, 2, 3)$, we write its membership function with $\mu((x_1, \dots, x_n) \mid \overline{A})$ in $[0, 1]$ for all x. The α-cut of any fuzzy set $\overline{X}$ of R^n, $\overline{X}(\alpha)$, is defined as $\{x : \mu((x_1, \dots, x_n) \mid \overline{A}) \geq \alpha\}$, $0 < \alpha \leq 1$, and $\overline{X}(0)$ is the closure of the union of $\overline{X}(\alpha)$, $0 < \alpha \leq 1$. $\vec{\overline{X}}$ is denoted as a fuzzy vector, and $\vec{x}$ is denoted as a traditional vector.

2.1. Fuzzy Points

Definition 1. A fuzzy point at $p = (a_1, a_2, \dots, a_n)$ in R^n $(n = 1, 2, 3)$, written $\overline{P}(a_1, \dots, a_n)$, is defined by its membership function:

(1) $\mu((x_1, \dots, x_n) \mid \overline{P}(a_1, \dots, a_n))$ is upper semicontinuous;

(2) $\mu((x_1, \dots, x_n) \mid \overline{P}(a_1, \dots, a_n)) = 1$, if and only if $(x_1, \dots, x_n) = (a_1, \dots, a_n)$;

(3) $\overline{P}(\alpha)$ is a compact, convex, subset of R^n for all α, $0 < \alpha \leq 1$.

Next; we define the fuzzy distance between fuzzy points. Let $d(u, v)$ be the usual Euclidean distance metric between points u and v in R^n; we define the fuzzy distance $\overline{D}$ between two fuzzy points $\overline{P_1} = \overline{P}(a_{11}, \dots, a_{n1})$, $\overline{P_2} = \overline{P}(a_{12}, \dots, a_{n2})$.

Definition 2. Consider $\Omega(\alpha) = \{d(u, v) : u$ is in $\overline{P}(a_1, b_1)(\alpha)$ and v is in $\overline{P}(a_2, b_2)(\alpha)\}$, $0 \leq \alpha \leq 1$, then, $\mu(d \mid \overline{D}) = \sup\{\alpha : d \in \Omega(\alpha)\}$.

Theorem 1. *One has $\overline{D}(\alpha) = \Omega(\alpha), 0 \leq \alpha \leq 1$, and $\overline{D}$ is a real fuzzy number.*

Definition 3. A fuzzy metric $\overline{M}$ is a mapping from pairs of fuzzy points $(\overline{P_1}, \overline{P_2})$ into fuzzy numbers so that

(1) $\overline{M}(\overline{P_1}, \overline{P_2}) = \overline{M}(\overline{P_2}, \overline{P_1})$,

(2) $\overline{M}(\overline{P_1}, \overline{P_2}) = \overline{0}$, if and only if $\overline{P_1}, \overline{P_2}$ are both fuzzy points at $(a_1, a_2, \dots, a_n)$,

(3) $\overline{M}(\overline{P_1}, \overline{P_2}) \leq \overline{M}(\overline{P_1}, \overline{P_3}) + \overline{M}(\overline{P_3}, \overline{P_2})$ for any fuzzy points $\overline{P_1}, \overline{P_2}$, and $\overline{P_3}$.

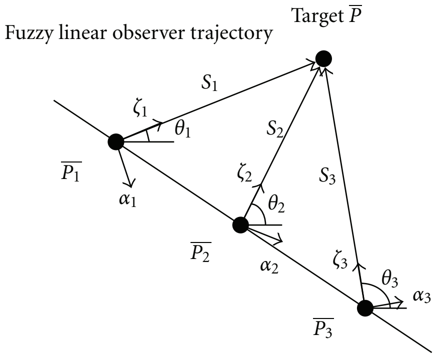


Figure 1: Fuzzy geometry for bearings-only target localization (3 sensors along fuzzy linear observer trajectory) in R^2 space.

2.2. Fuzzy Lines

Definition 4 (Two-point form). Let $\overline{P_1}, \overline{P_2}$ be two fuzzy points in R^n space $(n = 2, 3)$. Define

$$\Omega(\alpha) = \left\{ \begin{array}{c} (x_1, x_2, \dots, x_n) : \dfrac{x_1 - b_1}{a_1 - b_1} = \dfrac{x_2 - b_2}{a_2 - b_2} = \cdots = \dfrac{x_n - b_n}{a_n - b_n}, \\ (a_1, a_2, \dots, a_n) \in \overline{P_1}(\alpha), (b_1, b_2, \dots, b_n) \in \overline{P_2}(\alpha) \end{array} \right\}, \quad 0 \leq \alpha \leq 1. \tag{1}$$

Then the fuzzy line $\overline{L}$ is

$$\mu\Big((x_1, \dots, x_n) \mid \overline{L}\Big) = \sup\{\alpha : (x_1, \dots, x_n) \in \Omega(\alpha)\}. \tag{2}$$

3. Fuzzy Geometry Analysis for Bearings-Only Target Localization in R^2 Space

Based on fuzzy geometry, a detailed analysis of the interplay between the target localization geometry and the fuzzy estimation bias for the case of fuzzy linear observer trajectory in R^2 space is provided, which can realize the 3-dimensional localization including fuzzy estimate coordinate and target velocity by measuring the fuzzy azimuth angles at intervals of fixed time.

3.1. Fuzzy Geometry for Bearings-Only Target Localization in R^2 Space. Fuzzy geometry for bearings-only target localization in R^2 space is discussed. The fuzzy geometric relationship between one-sensor locations $\overline{P_i}$, and the target is shown in Figure 1. Assume a fuzzy linear observer trajectory

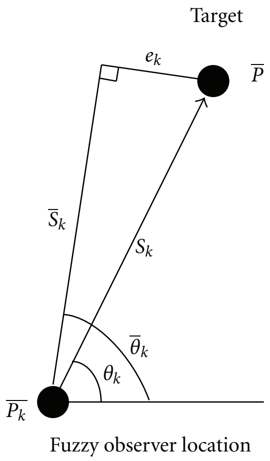


Figure 2: Fuzzy geometric relationship between a sensor and a target.

with three bearing measurements θ_1, θ_2, and θ_3 collected by three sensors at fuzzy observer locations $\overline{P_1}, \overline{P_2}$, and $\overline{P_3}$, respectively. The target localization is denoted as $\overline{P} = [x, y]$. In practical sensor networks, angle measurements are corrupted with some fuzzy factors.

Then define unit function α_k and ζ_k in Figure 1,

$$\alpha_k = \begin{bmatrix} \sin\theta_k \\ -\cos\theta_k \end{bmatrix}, \qquad \zeta_k = \begin{bmatrix} \cos\theta_k \\ \sin\theta_k \end{bmatrix}. \tag{3}$$

Using fuzzy points $\overline{P_i}$ in the plane, define

$$\text{Angle}_k(\alpha) = \left\{\theta_k \mid \theta_k \in \overline{P_i}(\alpha)\right\}, \quad 0 \le \alpha \le 1. \tag{4}$$

Then, the membership function of fuzzy angle $\overline{\Theta_k}$ is

$$\mu\left(\theta_k \mid \overline{\Theta_k}\right) = \sup\left\{\alpha : \theta_k \in \text{Angle}_k(\alpha)\right\}. \tag{5}$$

The target localization is related to the fuzzy observer locations through the fuzzy line equation. For fuzzy points $\overline{P_i}$ in the plane, by Definition 3, define

$$\Omega_{3i}(\alpha) = \left\{(x, y) : \frac{y - v_i}{x - u_i} = \frac{p_y - v_i}{p_x - u_i}, (u_i, v_i) \in \overline{P_i}(\alpha)\right\}, \quad 0 \le \alpha \le 1. \tag{6}$$

Then, the membership function of fuzzy line $\overline{P_i P}$ is

$$\mu\left((x, y) \mid \overline{P_i P}\right) = \sup\{\alpha : (x, y) \in \Omega_{3i}(\alpha)\}. \tag{7}$$

Define

$$\Omega_{3\overline{P_1P_2P_3}}(\alpha) = \left\{\begin{array}{c}(x, y) : \dfrac{y - v_1}{x - u_1} = \dfrac{v_2 - v_1}{u_2 - u_1} = \dfrac{v_3 - v_1}{u_3 - u_1}, (u_1, v_1) \in \overline{P_1}(\alpha), \\ (u_2, v_2) \in \overline{P_2}(\alpha), (u_3, v_3) \in \overline{P_3}(\alpha)\end{array}\right\} \quad 0 \le \alpha \le 1. \tag{8}$$

Then, the membership function of fuzzy line $\overline{P_1P_2P_3}$ is

$$\mu\left((x, y) \mid \overline{P_1P_2P_3}\right) = \sup\left\{\alpha : (x, y) \in \Omega_{3\overline{P_1P_2P_3}}(\alpha)\right\}. \tag{9}$$

$\overline{P_k}$ fuzzy observer location of the sensor in the plane is illustrated in Figure 2.

It is shown from Figure 2 that the fuzzy error e_k is obtained by

$$e_k = s_k \sin\left(\overline{\theta}_k - \theta_k\right), \tag{10}$$

where s_k is fuzzy distance between $\overline{P_k}$ and $\overline{P}$ which satisfies Definition 2.

Define

$$\Omega(\alpha) = \left\{\begin{array}{c} x = \overline{x_1} + d\left(\overline{P_1}, \overline{P_2}\right) \bullet \dfrac{\sin\left(\overline{\theta_2} + \psi\right)}{\sin\left(\left|\overline{\theta_2} - \overline{\theta_1}\right|\right)} \bullet \cos\left(\overline{\theta_1}\right) \\ y = \overline{y_1} + d\left(\overline{P_1}, \overline{P_2}\right) \bullet \dfrac{\sin\left(\overline{\theta_2} + \psi\right)}{\sin\left(\left|\overline{\theta_2} - \overline{\theta_1}\right|\right)} \bullet \sin\left(\overline{\theta_1}\right) \\ \psi = \operatorname{arctg}\left(\dfrac{\overline{y_2} - \overline{y_1}}{\overline{x_2} - \overline{x_1}}\right) \end{array} \middle| \left\{\begin{array}{c} (\overline{x_1}, \overline{y_1}) \in \overline{P_1}(\alpha), \\ (\overline{x_2}, \overline{y_2}) \in \overline{P_2}(\alpha) \\ \overline{\theta_1} \in \left\{\theta_1 \mid \theta_1 \in \overline{P_1}(\alpha)\right\} \\ \overline{\theta_2} \in \left\{\theta_2 \mid \theta_2 \in \overline{P_2}(\alpha)\right\} \\ 0 \le \alpha \le 1 \end{array}\right\}\right\}. \tag{11}$$

Then, the membership function of fuzzy location $(x,\ y)$ of the target is

$$\mu\left((x, y) \mid \overline{P}\right) = \sup\{\alpha : (x, y) \in \Omega(\alpha)\}, \tag{12}$$

where $d(\overline{P_1}, \overline{P_2})$ is fuzzy distance with fuzzy points $\overline{P_1}$ and $\overline{P_2}$ which satisfies Definition 2. By the formulas (3)–(12), for the case of N sensors deployed along using the fuzzy object programming, we have the fuzzy location of the target as follows:

$$\begin{aligned}&\text{Min}\quad e=\sum_k w_k e_k,\\&\text{S.T.}\quad e_k=s_k\sin\left(\overline{\theta_k}-\theta_k\right),\quad k=1,2,\dots,N,\\&\Omega_i(\alpha)=\left\{\begin{array}{c}x=\overline{x_i}+d\left(\overline{P_i},\overline{P_j}\right)\bullet\dfrac{\sin\left(\overline{\theta_j}+\psi\right)}{\sin\left(\left|\overline{\theta_j}-\overline{\theta_i}\right|\right)}\bullet\cos\left(\overline{\theta_i}\right)\\ y=\overline{y_i}+d\left(\overline{P_i},\overline{P_j}\right)\bullet\dfrac{\sin\left(\overline{\theta_j}+\psi\right)}{\sin\left(\left|\overline{\theta_j}-\overline{\theta_i}\right|\right)}\bullet\sin\left(\overline{\theta_i}\right)\\ \psi=\operatorname{arctg}\left(\dfrac{\overline{y_j}-\overline{y_i}}{\overline{x_j}-\overline{x_i}}\right)\end{array}\middle|\left\{\begin{array}{c}\left(\overline{x_i},\overline{y_i}\right)\in\overline{P_i}(\alpha),\\ \left(\overline{x_j},\overline{y_j}\right)\in\overline{P_j}(\alpha)\\ \overline{\theta_i}\in\left\{\theta_i\mid\theta_i\in\overline{P_i}(\alpha)\right\}\\ \overline{\theta_j}\in\left\{\theta_j\mid\theta_j\in\overline{P_j}(\alpha)\right\}\\ 0\le\alpha\le 1\end{array}\right\}\right\},\\&\qquad\qquad i=1,2,\dots,\ N-1,\ j=i+1,\ i+2,\dots,N.\end{aligned}\tag{13}$$

Then, the membership function of fuzzy location (x,y) of the target is

$$\mu\left((x,y)\mid\overline{P_i}\right)=\sup\{\alpha:(x,y)\in\Omega_i(\alpha)\},\tag{14}$$

where, $d(\overline{P_i},\overline{P_j})$ is fuzzy distance with fuzzy points $\overline{P_i}$ and $\overline{P_j}$ which satisfies on Definition 2. Define

$$\Omega_{3\overline{P_iP_{i+1}P_{i+2}}}(\alpha)=\left\{\begin{array}{c}(x,y):\dfrac{y-v_i}{x-u_i}=\dfrac{v_{i+1}-v_i}{u_{i+1}-u_i}=\dfrac{v_{i+2}-v_i}{u_{i+2}-u_i},\\(u_i,v_i)\in\overline{P_i}(\alpha),\ i=1,\dots,N-2\end{array}\right\},$$
$$0\le\alpha\le 1\tag{15}$$

the membership function of fuzzy line $\overline{P_iP_{i+1}P_{i+2}}$ is

$$\mu\left((x,y)\mid\overline{P_iP_{i+1}P_{i+2}}\right)=\sup\left\{\alpha:(x,y)\in\Omega_{3\overline{P_iP_{i+1}P_{i+2}}}(\alpha)\right\}.\tag{16}$$

Next, the target velocity needs to be determined, which is based on the time-neighboring estimate locations and time intervals. Similarly, there also exists some fuzziness among target locations and time intervals. Let $\overline{P_i}(\alpha),\overline{P_{i+1}}(\alpha)$ be the estimate location at time t_i, t_{i+1}, respectively. The time interval $t_{i+1}-t_i$ is denoted as the fuzzy number $\overline{T_{i+1}}=(a/b/c)$; define

$$\Omega_{v_{i+1}}(\alpha)=\left\{v_{i+1}=\frac{d(p_i,p_{i+1})}{\varepsilon_{i+1}}\ \middle|\ p_i\in\overline{P_i}(\alpha),p_{i+1}\in\overline{P_{i+1}}(\alpha),\varepsilon_{i+1}\in\overline{T_{i+1}}\right\}.\tag{17}$$

Then, the fuzzy target velocity $\overline{V_{i+1}}$ at time t_{i+1} is

$$\mu\left(v_{i+1}\mid\overline{V_{i+1}}\right)=\sup\{\alpha:v_{i+1}\in\Omega_{v_{i+1}}(\alpha)\}.\tag{18}$$

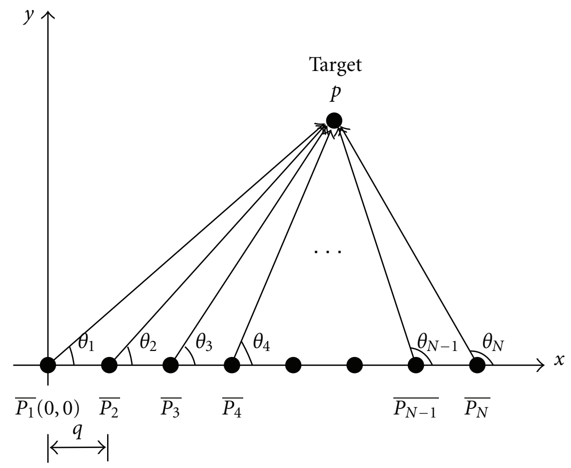


FIGURE 3: Fuzzy geometry of target localization for the case of fuzzy linear observer trajectory.

Based on the above formulas (13), (14), (17), (18), define

$$\Omega_{i+1}(\alpha)=\left\{\begin{array}{c}(x_{i+1},y_{i+1})\\v_{i+1}=\dfrac{d((x_i,y_i),(x_{i+1},y_{i+1}))}{\varepsilon_{i+1}}\end{array}\ \middle|\ \begin{array}{c}(x_i,y_i)\in\overline{P_i}(\alpha),\\(x_{i+1},y_{i+1})\in\overline{P_{i+1}}(\alpha),\\\varepsilon_{i+1}\in\overline{T_{i+1}}\end{array}\right\}.\tag{19}$$

Then, in R^2 space, the 3-dimensional fuzzy estimate $\overline{\wp_{i+1}}$ including the fuzzy target locations and fuzzy velocity at time t_i is

$$\begin{aligned}&\mu\left((x_{i+1},y_{i+1},v_{i+1})\mid\overline{\wp_{i+1}}\right)\\&\qquad=\sup\{\alpha:(x_{i+1},y_{i+1},v_{i+1})\in\Omega_{i+1}(\alpha)\}.\end{aligned}\tag{20}$$

3.2. Fuzzy Geometry Theory for the Case of Fuzzy Linear Observer Trajectory in R^2 Space. Figure 3 shows the fuzzy

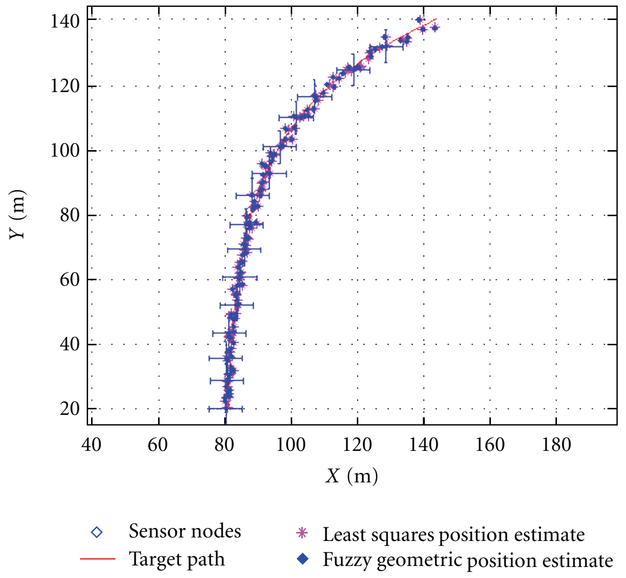


Figure 4: illustration of the moving target trajectory, defuzzified position estimate and some interval values, and least squares position estimate.

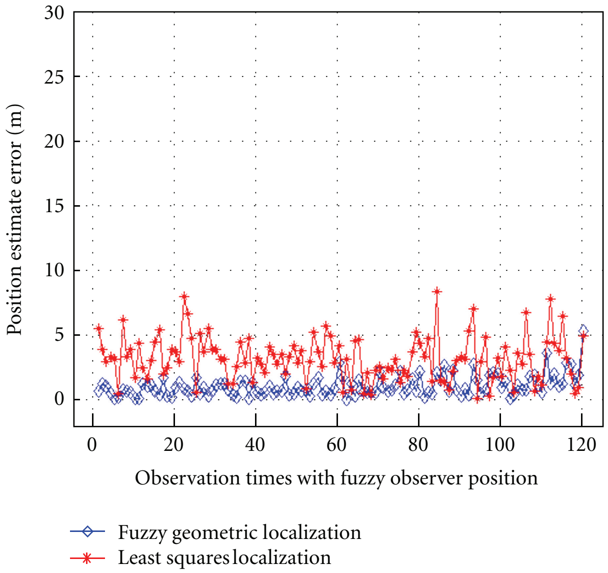


Figure 5: Position estimate error comparison with fuzzy observer positions.

geometry of target localization for the case of fuzzy linear observer trajectory. Let observer location $\overline{P_1}$ be the origin of the fuzzy plane, denoted as $\overline{P_1}(0,0)$.

Theorem 2. *Suppose that the neighboring observers are separated by the fuzzy distance q, then*

(1) *any fuzzy geometry of target localization for the case of fuzzy linear observer trajectory can be equivalently represented by Figure 3, which can be realized with the rotation and translation of absolute coordinates of the target location and observer locations,*

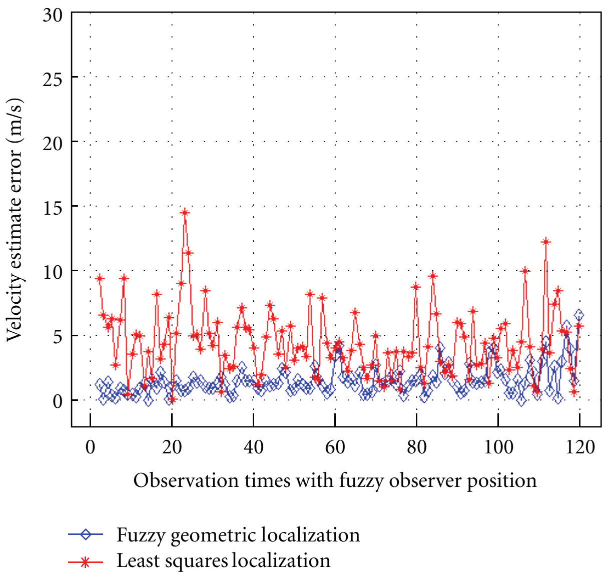


Figure 6: Velocity estimate error comparison with fuzzy observer positions.

(2) *for the fuzzy linear observer trajectory shown in Figure 3, the fuzzy centroid of the observer locations is*

$$c = \left[\frac{1}{2}(N-1)q \quad 0\right]. \tag{21}$$

Proof. Obvious by fuzzy geometry theory. □

4. Experiments Analysis

Three sensor nodes are deployed in R^2 space to implement the 3-dimensional fuzzy estimation including the target position and velocity. Due to the uncertainty in practical sensor networks, sensor observation positions are estimated by $\overline{S_1}(0,0)$, $\overline{S_2}(100,0)$, and $\overline{S_3}(200,0)$ based on fuzzy theory, where the coordinates of sensor $(\overline{X},\overline{Y})$ are a triangle fuzzy number, denoted as $(x-5/x/x+5,\ y-5/y/y+5)$, which determine a fuzzy linear observer trajectory. For the same bearing measurements, let the standard deviation of measurement error be 0.01 rad, time interval $\overline{T}(1) = 1$ s. The bearings-only localizations based on fuzzy geometry and least squares methods [10] are analyzed and compared in Figure 4.

The sensor positions are estimated as the arbitrary points which belong to the fuzzy points $\overline{S_1}(0,0)$, $\overline{S_2}(100,0)$, and $\overline{S_3}(200,0)$, respectively. Figure 4 illustrates the moving target trajectory, the defuzzified position estimate of the target using weighted average operator and some interval values, and the position estimate based on least squares method. Figures 5 and 6 compare the position estimate error and velocity estimate error between the two methods. It shows that the precision of fuzzy geometric localization is better than that of least squares localization in uncertain sensor networks. The resulting position estimate outperforms the traditional least squares approach for bearings-only localization with uncertainty. When the target arrived at the coordinate (112, 120), set $\alpha = 0.6$, then the fuzzy position estimate interval is ([110.8, 114.8], [117.3, 121.3])(0.6). The defuzzified position estimate is (112.8, 119.3), and the defuzzified estimate error is 1.05 m, and the defuzzified estimate velocity is 3.01 m/s. Therefore, the defuzzified 3-dimensional fuzzy estimation is (112.8, 119.3, 3.01). Simulation results validate the rationality and the effectiveness that fuzzy geometry is applied in the bearings-only target localization for two-dimensional sensor networks.

5. Conclusion

A fuzzy geometric localization approach using passive sensor networks in smart grid is proposed based on fuzzy geometry. The fuzzy analytical bias expressions and the constraints are derived considering fuzzy measurements and fuzzy observer positions. The interplay between the target localization geometry and the fuzzy estimation bias is analyzed in detail for the case of fuzzy linear observer trajectory. The experiment results validate that the resulting fuzzy estimate outperforms the traditional least squares approach in a number of respects for localization with uncertainty. Future work will focus on the various kinds of fuzzy observer trajectories and higher-dimensional localization problem in practical sensor networks.

Acknowledgments

This research work is supported by the National Natural Science Foundation of China (60873130, 60872115), the Shanghai's Leading Academic Discipline Project of Shanghai Municipal Education Committee (J50104), and the project of Shanghai Science Committee (10511501303, 10511501300).

References

[1] R. G. Stansfield, "Statistical theory of D. F. fixing," *Journal Institution Electrical Engineering*, vol. 94, no. 15, pp. 186–207, 1947.

[2] M. Gavish and A. J. Weiss, "Performance analysis of bearing-only target location algorithms," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 28, no. 3, pp. 817–828, 1992.

[3] D. J. Torrieri, "Statistical theory of passive localization systems," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 20, no. 2, pp. 183–198, 1984.

[4] W. H. Foy, "Position-location solutions by Taylor-series estimation," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 12, no. 2, pp. 187–194, 1976.

[5] S. Nardone, A. G. Lindgren, and K. F. Gong, "Fundamental properties and performance of conventional bearings-only target motion analysis," *IEEE Transactions on Automatic Control*, vol. 29, no. 9, pp. 775–787, 1984.

[6] Z. X. Liu, W. X. Xie, and X. Yang, "Target location method based on intersection of lines of sight in the netted passive sensor system," *Journal of Electronics and Information Technology*, vol. 27, no. 1, pp. 17–20, 2005.

[7] A. Rosenfeld, "The diameter of a fuzzy set," *Fuzzy Sets and Systems*, vol. 13, no. 3, pp. 241–246, 1984.

[8] J. J. Buckley and E. Eslami, "Fuzzy plane geometry I: points and lines," *Fuzzy Sets and Systems*, vol. 86, no. 2, pp. 179–187, 1997.

[9] J. J. Buckley and E. Eslami, "Fuzzy plane geometry II: circles and polygons," *Fuzzy Sets and Systems*, vol. 87, no. 1, pp. 79–85, 1997.

[10] D. Kutluyil, "Bearings-only target localization using total least squares," *Signal Processing*, vol. 85, no. 9, pp. 1695–1710, 2005.

Hindawi Publishing Corporation
International Journal of Digital Multimedia Broadcasting
Volume 2011, Article ID 947396, 7 pages
doi:10.1155/2011/947396

Research Article

Expected Transmission Energy Route Metric for Wireless Mesh Senor Networks

YanLiang Jin,[1] HuiJun Miao,[1] Quan Ge,[1] and Chi Zhou[2]

[1] *Key Laboratory of Special Fiber Optics and Optical Access Networks of Ministry of Education, Shanghai University, Shanghai 200072, China*
[2] *Illinois Institute of Technology, Chicago, IL 60616-3793, USA*

Correspondence should be addressed to YanLiang Jin, jinyanliang@staff.shu.edu.cn

Received 1 November 2010; Accepted 5 April 2011

Academic Editor: Robert C. Qiu

Mesh is a network topology that achieves high throughput and stable intercommunication. With great potential, it is expected to be the key architecture of future networks. Wireless sensor networks are an active research area with numerous workshops and conferences arranged each year. The overall performance of a WSN highly depends on the energy consumption of the network. This paper designs a new routing metric for wireless mesh sensor networks. Results from simulation experiments reveal that the new metric algorithm improves the energy balance of the whole network and extends the lifetime of wireless mesh sensor networks (WMSNs).

1. Introduction

Wireless sensor networks are one of the most rapidly evolving research and development fields for microelectronics. A wireless sensor network potentially comprises hundreds to thousands of nodes. These nodes are generally stationary after deployment, with the exception of a very small number of mobile sensor nodes, as shown in Figure 1. Wireless sensor networks characterize themselves in their distributed, dynamic, and self-organizing structure. Each node in the network can adapt itself based on environmental changes and physical conditions. Sensor nodes are expected to have low power consumption and simple structure characteristics, while possessing the ability of sensing, communicating, and computing. For conventional wireless networks, high degree of emphasis on mobility management and failure recovery is located in order to achieve high system performance. However, as the power of sensor nodes is usually supplied by battery with no continual maintenance and battery replenishment, to design a good protocol for WSNs, the first attribute that has to be considered is low energy consumption that could promise a long network lifetime. The recent advances of WSNs have made it feasible to realize low-cost embedded electric utility monitoring and diagnostic systems [1, 2]. In these systems, wireless multifunctional sensor nodes are installed on the critical equipment of the smart grid to monitor the parameters critical to each equipment's condition. Such information enables the smart-grid system to respond to varying conditions in a more proactively and timely manner. In this regard, WSNs play a vital role in creating a highly reliable and self-healing smart electric power grid that rapidly responds to online events with appropriate actions. The existing and potential applications of WSNs on smart grid span a wide range, including wireless automatic meter reading (WAMR), remote system monitoring, and equipment fault diagnostics.

There are lots of topology for wireless networks, such as star topology, mesh topology, and line topology. Among these topologies, mesh has large throughput and excellent stability, which is upcoming to become the model of the future network. Mesh networks, inspired from wireless neighborhood networks [3, 4], are composed of static wireless nodes that own several features, such as ample energy supplying, a distributed infrastructure, self-organizing and self-configuring capability, and ease and rapidity of network deployment, as shown in Figure 2. Each of these wireless nodes can be equipped with multiple radios, called a multiradio/multichannel node, and each of the radios can be

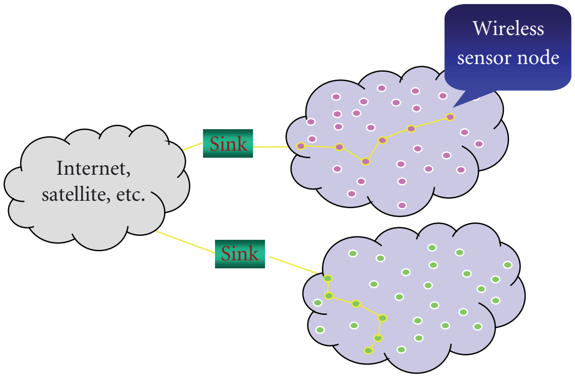


Figure 1: Wireless sensor network.

configured to a different channel to enhance network capacity. A wireless mesh network (WMN), possessing a more planned configuration, may be deployed to provide dynamic and cost-effective connectivity over a certain geographic area. Since its inception in the early years of this millennium, it has been in the limelight of all researchers.

The interest in wireless mesh networks has increased in recent years and several international standardization organizations are now developing specification for wireless mesh networking. IEEE 802.11 Task Group S (TGs), IEEE 802.16 Task Group, and IEEE 802.15.5th Task Group are standardizing wireless mesh networking. The Hybrid Wireless Mesh Protocol (HWMP) has been deemed as the mandatory routing protocol for WLAN mesh networks [5]. Although HWMP provides a mature routing scheme, merging the on-demand routing with the proactive routing, it does not present a method for WSNs, where limited energy is the crux and related works are barely done [6]. To achieve longevity in sensor networks, energy-aware architectures and protocols have been thoroughly investigated in the recent literature. The work in [7] introduced the NeLMUK algorithm to maximize the lifetime of 802.15.4-based wireless sensor networks. The work in [8] improved the ZigBee mesh routing protocol for energy-efficiency usage and proposed a routing algorithm combining AODV with the node residual energy. Mesh topology is not discussed. Sereiko firstly proposed the concept of wireless mesh sensor network (WMSN) by deploying wireless routers to connect sensor networks [9].

This paper studies the method of searching for the optimum routing paths of wireless mesh sensor networks by modifying the routing metric in HWMP. A new routing metric is proposed, considering the route effect on the energy distribution of the network, called expected transmission energy (ETE). We simulate the new metric algorithm compared with HWMP and min-hop in NS3 to evaluate the performance of the proposed routing method. Through experiments, we confirm that our proposed algorithm has better performance in prolonging the lifetime of WMSNs.

The rest of this paper is organized as follows. In Section 2, we describe on-demand routing, proactive routing, and HWMP, pointing out their advantages and disadvantages. Section 3 introduces the ETX and ETT metrics and presents the proposed ETE metric. In Section 4, we introduce the ETE into HWMP airtime metric and analyze the simulation results. Finally, Section 5 concludes this paper.

2. Routing Protocols for Mesh Networks

Routing protocols can be divided into two categories: on-demand routing and proactive routing. Different routing protocols have different costs in terms of message overhead and management complexity.

2.1. On-Demand Routing. Originally proposed for ad hoc networks, on-demand or reactive routing protocols (e.g., DSR [10], AODV [11], MCR [12], LBAR [13], and DLAR [14]) only create a route between a pair of source and destination nodes when the source node actually needs to send packets to the destination. Network-wide flooding is usually used to discover routes when they are needed. For ad hoc networks, since there are frequent link breaks caused by the mobility of nodes, flooding-based route discovery provides high network connectivity and relatively low message overhead compared with proactive routing protocols. In wireless mesh sensor networks, however, links usually have a much longer expected lifetime due to the static nature of nodes. Since the frequency of link breaks is much lower than the frequency of flow arrivals in mesh networks, flooding-based route discovery is both redundant and very expensive in terms of control message overhead. Therefore, pure on-demand routing protocols are generally not scalable and inappropriate for mesh networks.

2.2. Proactive Routing. In proactive routing protocols, each node maintains one or more tables containing routing information to every other node in the network. All nodes update these tables to maintain a consistent and up-to-date view of the network. When the network topology changes, the nodes propagate update messages throughout the network to maintain routing information about the whole network. These routing protocols differ in the methods by which packets are forwarded along routes. Every node maintains a routing table that indicates the next hops for the routes to all other nodes in the network. For a packet to reach its destination, it only needs to carry the destination address. Intermediate nodes forward the packet along its path based only on the destination address. Due to its simple forwarding scheme and low message overhead, proactive routing is dominant in wired networks.

2.3. Hybrid Wireless Mesh Protocol (HWMP). IEEE 802.11s deems HWMP as the mandatory routing protocol for WLAN mesh networks and optionally allows other routing protocols such as the Radio Aware Optimized Link State Routing (RA-OLSR) protocol. HWMP supports the two routing modes of on-demand and tree-based proactive to be cooperated. HWMP uses a common set of protocol primitives, generation, and processing rules inspired by the Ad hoc On-demand Distance Vector (AODV) protocol [11].

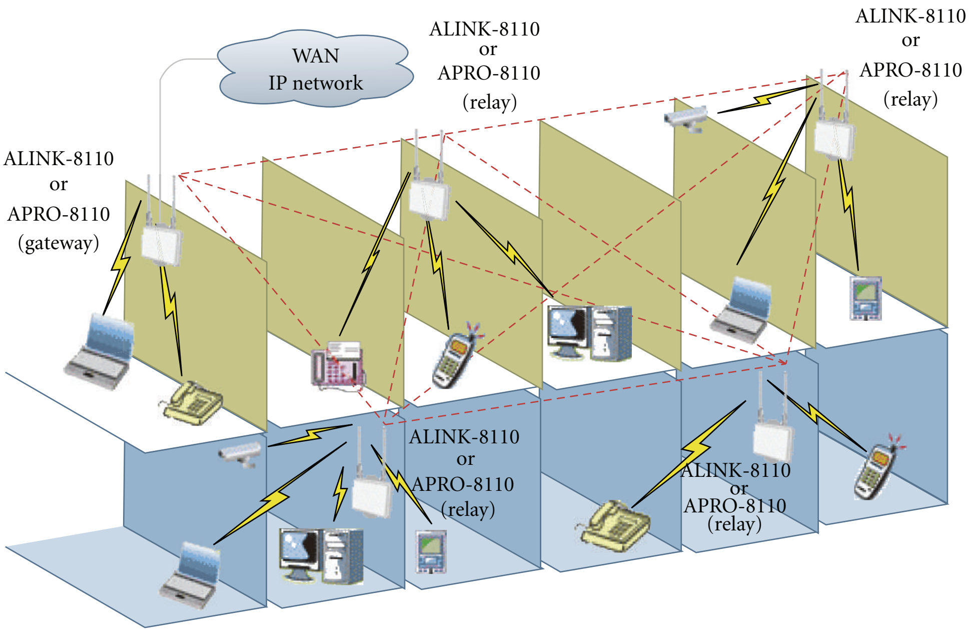


Figure 2: Wireless mesh network.

Four message frames are used in HWMP, namely, path request (PREQ), path reply (PREP), path error (PERR), and root announcement (RANN). Except for RANN that is only used in the proactive routing mode, these three message frames are mostly adopted from the AODV protocol.

HWMP, unlike traditional routing protocols on layer 3 with IP addresses, is operated on layer 2 using MAC addresses. When a routing protocol on layer 3 is used, data packets must be delivered to the IP layer to be routed. In the exchange between MAC addresses and IP addresses in the ARP table, overheads are also incurred. However, by adopting a layer 2 routing mechanism, HWMP can reduce overheads in forwarding data packets to destination nodes in WLAN mesh networks, based on multihop topologies. Consequently, high network throughputs can be achieved.

The operating method and the characteristics of the on-demand routing mode of HWMP are very similar to the existing AODV, except that HWMP uses layer 2 routing. In the on-demand routing mode, if a source node has no routing path to a destination node, it broadcasts a PREQ message inside the mesh network. The destination node that received the PREQ message sends a unicast PREP message back to the source node, and then a bidirectional routing path between the source and the destination nodes is established. During this procedure, the PREQ ID and the destination sequence number are used to prevent sending duplicated messages and to establish loop-free routing paths. The on-demand routing mode always provides the optimum routing paths by establishing its path when data transmission is required.

Figure 3 shows the instances of communication steps of mesh network. If mesh point4 wants to communicate with mesh point 9,

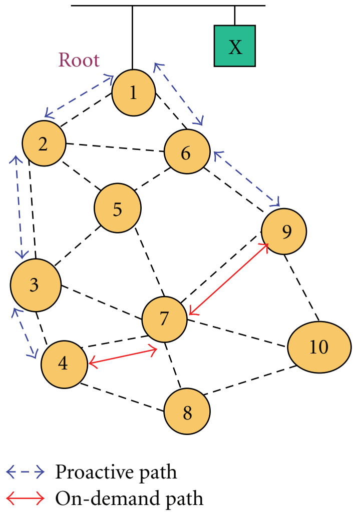


Figure 3: HWMP operation.

(1) MP 4 first checks its local forwarding table for an active forwarding entry to MP 9,

(2) if no active path exists, MP 4 may immediately forward the message on the proactive path toward the Root MP 1

(3) when MP 1 receives the message, it flags the message as “intra-mesh” and forwards on the proactive path to MP 9,

(4) when MP 9 receives the message, it may issue an on-demand RREQ to MP 4 to establish the best intramesh MP-to-MP path for future messages.

If MP 4 wants to communicate with X, who is outside of the current mesh cluster,

(1) MP 4 first checks its local forwarding table for an active forwarding entry to X,

(2) if no active path exists, MP 4 may immediately forward the message on the proactive path toward the Root MP 1,

(3) when MP 1 receives the message, if it does not have an active forwarding entry to X it may assume the destination is outside the mesh and forward on other LAN segments according to locally implemented interworking.

No broadcast discovery is required when destination is outside of the mesh. This efficient routing meets the severe energy constrains of wireless sensor networks and the flexible connectivity of mobile nodes.

3. Routing Metrics

Router metrics can contain any number of values that help the router determine the best route among multiple routes to a destination. A router metric is typically based on information like path length, bandwidth, load, hop count, path cost, delay, Maximum Transmission Unit (MTU), reliability, and communications cost. In this section, we discuss 3 traditional routing metrics that have been proposed and HWMP routing metric in 802.11s. After that, we propose a new metric which counterbalances energy consumption of the network basing on HWMP metric.

3.1. Traditional Routing Metric

3.1.1. Hop Count. Hop count is the most commonly used routing metric in existing routing protocols such as DSR [10], AODV [11], DSDV, and GSR. It reflects the effects of path lengths on the performance of flows. Efficient algorithms can find loop-free paths with minimum hop count, since hop count metrics are isotonic. However, hop count does not consider the differences of the transmission rates and packet loss ratios in different wireless links, or the interference in the network. Hence, using a hop count metric may not result in a good performance.

3.1.2. Expected Transmission Count (ETX). ETX, proposed by De Couto et al. [15], is defined as the expected number of MAC layer transmissions that is needed for successfully delivering a packet through a wireless link. The weight of a path is defined as the summation of the ETX of all links along the path

$$\mathrm{ETX} = \sum_{k-1}^{\infty} kp^{k-1}(1-p) = \frac{1}{1-p}. \tag{1}$$

Here, k means that the transmission times for node A send a packet to node B successfully. And p means error rate of the transmission.

Since both long paths and lossy paths have large weights under ETX, the ETX metric captures the effects of both packet loss ratios and path length. In addition, ETX is also an isotonic routing metric, which guarantees easy calculation of minimum weight paths and loop-free routing under all routing protocols. However, energy consumption of the devices is not taken into consideration in ETX.

3.1.3. Expected Transmission Time (ETT). The ETT routing metric, proposed by Draves et al. [16], improves ETX by considering the differences in link transmission rates. The ETT of a link l is defined as the expected MAC layer duration for a successful transmission of a packet at link.

The weight of a path p is simply the summation of the ETT's of the links on the path. The relationship between the ETT of a link l and ETX can be expressed as

$$\mathrm{ETT}_l = \mathrm{ETX}_l \frac{s}{b_l}, \tag{2}$$

where b_l is the transmission rate of link l and s is the packet size. Essentially, by introducing b_l into the weight of a path, the ETT metric captures the impact of link capacity on the performance of the path. Similar to ETX, ETT is also isotonic. However, the remaining drawback of ETT is that it still does not fully capture energy consumption in the network. For example, ETT may choose a path in which energy of the devices is quite low. Though it may achieve high throughput, the lifetime of the WMSN may be awfully short as energy consumption focuses on some nodes.

3.2. HWMP Airtime Metric. In HWMP, the cost function for establishment of the radio-aware paths is based on airtime cost. Airtime cost reflects the amount of channel resources consumed by transmitting the frame over a particular link. This measure is approximate and designed for ease of implementation and interoperability.

The airtime cost for each link is calculated as

$$c_a = \left[O_{ca} + O_p + \frac{B_t}{r}\right]\frac{1}{1-e_{pt}}, \tag{3}$$

where O_{ca}, O_p, and B_t are constants listed in Table 1, and the input parameters r and e_{pt} are the bit rate in Mb/s and the frame error rate for the test frame size B_t, respectively. The rate r represents the rate at which the mesh point would transmit a frame of standard size (B_t) based on current conditions, and its estimation is dependent on local implementation of rate adaptation; the frame error rate e_{pt} is the probability that when a frame of standard size (B_t) is transmitted at the current transmission bit rate (r), the frame is corrupted due to transmission error, and its estimation is a local implementation choice. Frame drops due to exceeding TTL should not be included in this estimate as they are not correlated with link performance. This metric algorithm only takes the communication channel between nodes into account. However, it does not consider the condition of node's itself.

TABLE 1: Airtime cost constants.

Parameter	Value (802.11a)	Value (802.11b)	Description
O_{ca}	75 ms	335 ms	Channel access overhead
O_p	110 ms	364 ms	Protocol overhead
B_t	8224	8224	Number of bits in test frame
r			Current bit rate in use
e_{pt}			Packet error rate at the current bit rate

3.3. Expected Transmission Energy (ETE). All the algorithms mentioned above do not take the energy factor into account which is one of the most important problems of wireless sensor network. Our assumption is that all nodes are considered equally important in a WMSN. If a node died, we will lose control of a certain space in the sensing field. To prevent this situation, we would like to ensure that no node consumes energy at a rate significantly higher than other nodes, while simultaneously keeping the average power consumption rate low.

This conception can be formulated as two important parameters:

$$\sigma_E^2 = \frac{\sum_{i=1}^{n}\left(E_i - \overline{E}\right)}{n}, \qquad \overline{E}_c = \frac{\sum_{i=1}^{n_j} E_{ic}}{n_j}. \tag{4}$$

E_i is the remaining energy of node i after the transmission, E_{ic} is the energy consumption of the node i in the transmission which related to the distant, n is the number of nodes of the whole network, and n_j is the number of nodes along the selected route.

The route judgment can be concluded as the following four steps.

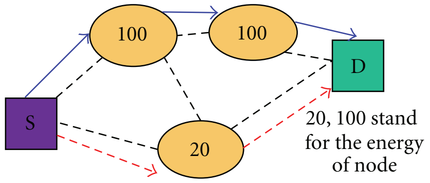
(1) $\overline{E}_c$ must be less than some maximum budget threshold $\overline{E}_t$.

(2) σ_E^2 should be minimized after the transmission.

(3) Once (1) and (2) are satisfied, the less $\sum_{i=1}^{n_j} E_{ic}$ it has, the better route it is.

(4) Once a node's energy is below a designated threshold, the node will not join the calculation of route metric which means it only sends his new packets and will not forward packets for others.

The routing metrics must ensure that optimum paths can be found by efficient algorithms with polynomial complexity. However, the expression of the σ_E^2 makes the algorithm too complex to realize. So the algorithm needs to be simplified. The minimization of σ_E^2 is equal to choosing route with the maximum $\overline{E}_c$. If the number is different, the situation could be simplified as Figure 4. The path with powerful nodes in solid line will be chosen as the transmission path. While the dotted line path, though has less hop count, does not help to do energy balance of the network and will not be chosen.



20, 100 stand for the energy of node

FIGURE 4: Route selection based on ETE metric.

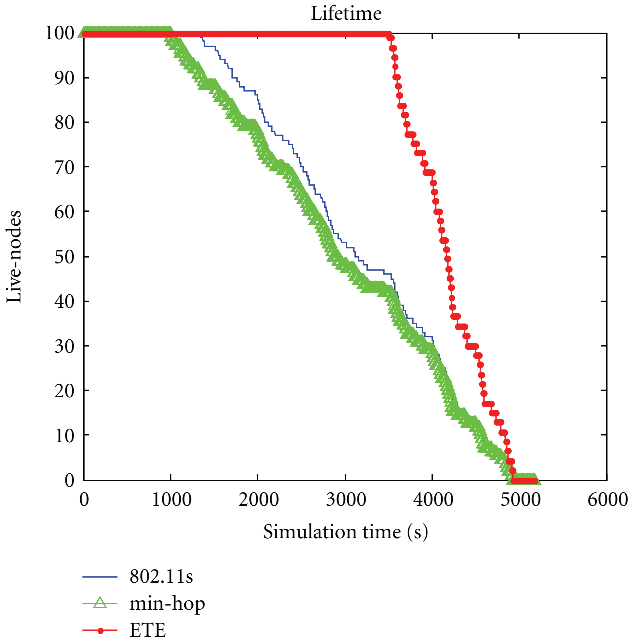


FIGURE 5: Lifetime of WMSN.

Focusing the energy consumption on the route consisting of nodes with more power will help to the balance of the energy distribution of the whole network. But it will take a further path which contains more powerful nodes that help to increase the average energy $\overline{E}_c$. So, our simplified metric can be modified as $\sum_{i=1}^{n_j} 1/E_i$. To combine with the 802.11s airtime metric, it is normalized as $\sum_{i=1}^{n_j} 1/(100(E_i/E_{\text{init}}))$ and $\overline{E}_c$ is normalized as $\sum_{i=1}^{n_j}(E_{ic}/E_{\text{init}})/n_j$. And the full expression of our metric at last could be concluded as the following:

$$c'_a = \left[O_{ca} + O_p + \frac{B_t}{r} + \sum_{i=1}^{n_j}\frac{E_{\text{init}}}{100E_i}\right]\frac{1}{1-e_{pt}} + \frac{\sum_{i=1}^{n_j}(E_{ic}/E_{\text{init}})}{n_j}. \tag{5}$$

As $1/(1-e_{pt}) < 1$, $\sum_{i=1}^{n_j}(E_{ic}/E_{\text{init}})/n_j$ contributes less than $\sum_{i=1}^{n_j}(E_{\text{init}}/100E_i)$ to the result of c'_a.

In case there exist two routes with approximately equal energy. To prevent extra energy consumption in route establishment, the route metric will not be recalculated until the tenth transmission on the old route.

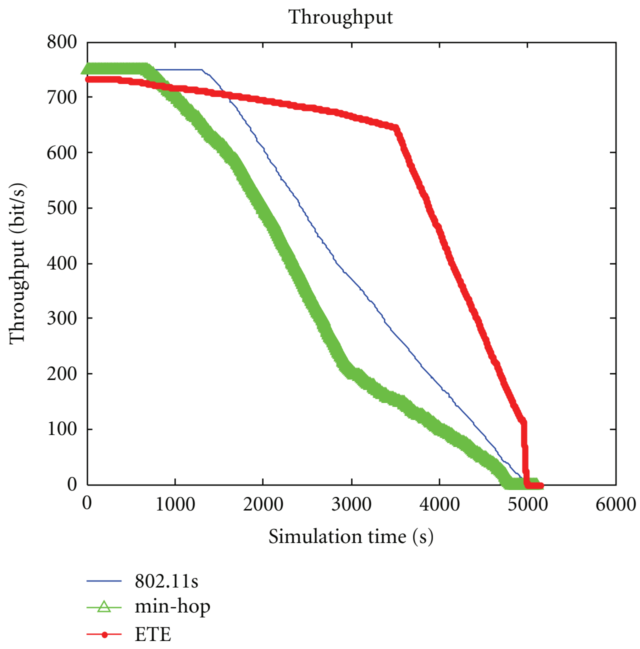


Figure 6: Throughput of WMSN.

4. Simulation and Analysis

All of our simulations are performed in the NS3 simulator. And the figures are printed by Matlab after the process of awk script. One hundred nodes are regularly placed over a 10 × 10 grid. The sources and destinations of the data flows are randomly located in the mesh network while the root of mesh network is designated. To simplify the simulation, we set the initial energy of a node 100. If a node sends a packet, it will cost 1, same as its receiving process. This means the node will lose 2 of energy when it forwards a packet. If a node's energy is less than 20% of E_{init}, this node will refuse to forward packets for other nodes. The remaining energy of it will only be used to send its own new data.

4.1. Lifetime. In Figure 5, the line with triangle, the leftmost one, represents the min-hop metric, and its lifetime is the shortest. This is because it just considers the minimization of hop count. However, even though some paths have less hop counts, the error rate is awful. Thus, forcing the nodes to retransmit their packets and causing a waste of energy. The line with asterisk in the rightmost represents the improved algorithm. Simulation result shows that the modified algorithm balances the energy consumption more effectively, that is, the lifetime of the WMSN is prolonged.

4.2. Throughput. As is shown in Figure 6, ETE achieves higher throughput. In the improved algorithm, the nodes with energy under the threshold will refuse to forward packets for others, helping extend the lifetime of low power nodes and balance the energy distribution of the network. Moreover, these nodes with low power will consume energy only when they have their own new data sent. Hence, we have a higher throughput in the last part of the simulation, the rightmost one. Compared with ETE, low power nodes in 802.11s and min-hop routing die away more quickly and the total amount of data the nodes sensed become less which pull down the throughput.

5. Conclusion

In this paper, we study the traditional route metrics and point out their common deficiency-neglecting energy consumption. We proposed a new route metric called ETE and introduced it into 802.11s airtime metric. The simulation reveals that the new algorithm improves the energy balance of the whole network and extends the lifetime of wireless mesh sensor network. In the future, the proposed algorithm may be further considered for multichannel wireless mesh sensor networks. In addition, it will be used in the existing and potential applications of WMSNs on smart grid.

Acknowledgments

The authors would like to thank the reviewers for their detailed comments on earlier versions of this paper. This work was supported by Shanghai Leading Academic Discipline project (S30108, 08DZ2231100), Shanghai Education Committee (09YZ33), Shanghai Science Committee (08220510900, 10511501303) and Shanghai SMIT Fund.

References

[1] L. Lo Bello, O. Mirabella, and A. Raucea, "Design and implementation of an educational testbed for experiencing with industrial communication networks," *IEEE Transactions on Industrial Electronics*, vol. 54, no. 6, pp. 3122–3133, 2007.

[2] B. Lu and V. C. Gungor, "Online and remote motor energy monitoring and fault diagnostics using wireless sensor networks," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 11, pp. 4651–4659, 2009.

[3] R. Karrer, A. Sabharwal, and E. Knightly, "Enabling large-scale wireless broadband: the case for TAPs," in *Proceedings of the Workshop on Hot Topics in Networks (HotNets '03)*, no. 1, pp. 27–32, Cambridge, Mass, USA, 2003.

[4] V. Gambiroza, B. Sadeghi, and E. W. Knightly, "End-to-end performance and fairness in multihop wireless backhaul networks," in *Proceedings of the 10th Annual International Conference on Mobile Computing and Networking (MobiCom '04)*, pp. 287–301, October 2004.

[5] IEEE Std 802.11TM–2007, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Computer Society, June 2007.

[6] J. D. Camp and E. W. Knightly, "The IEEE 802.11s extended service set mesh networking standard," *IEEE Communications Magazine*, vol. 46, no. 8, pp. 120–126, 2008.

[7] M. U. Ilyas and H. Radha, "Increasing network lifetime of an IEEE 802.15.4 wireless sensor network by energy efficient routing," in *Proceedings of the IEEE International Conference on Communications (ICC '06)*, pp. 3978–3983, July 2006.

[8] F. Zhang, H. Zhou, and X. Zhou, "A routing algorithm for zigbee network based on dynamic energy consumption decisive path," in *Proceedings of the International Conference*

on Computational Intelligence and Natural Computing (CINC '09), pp. 429–432, June 2009.

[9] P. Sereiko, "Wireless Mesh Sensor Networks Enable Building Owners, Managers, and Contractors to Easily Monitor HVAC Performance Issues," 2004, http://www.automatedbuildings.com/news/jun04/articles/sensicast/Sereiko.htm.

[10] D. B. Johnson and D. A. Maltz, "Dynamic source routing in AdHoc wireless networks," in *Mobile Computing*, vol. 353, Kluwer Academic, Boston, Mass, USA, 1996.

[11] C. Perkins, "Ad-Hoc on-demand distance vector routing," in *Proceedings of the IEEE Military Communications Conference on Ad Hoc Networks (Milcom '97)*, 1997.

[12] P. Kyasanur and N. Vaidya, "Multi-channel wireless networks: capacity and protocols," Tech. Rep., University of Illinois at Urbana-Champaign, Urbana, Ill, USA, 2005.

[13] H. Hassanein and A. Zhou, "Routing with load balancing in wireless ad hoc networks," in *Proceedings of the 4th ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems (ACM MSWiM '01)*, pp. 89–96, July 2001.

[14] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.

[15] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A High-Throughput Path Metric for Multi-Hop Wireless Routing," in *Proceedings of the Ninth Annual International Conference on Mobile Computing and Networking (MobiCom '03)*, pp. 134–146, September 2003.

[16] R. Draves, J. Padhye, and B. Zill, "Routing in multi-radio, multi-hop wireless mesh networks," in *Proceedings of the 10th Annual International Conference on Mobile Computing and Networking (MobiCom '04)*, pp. 114–128, October 2004.