2010 International Conference on Power System Technology

Study on Security of Wireless Sensor Networks in Smart Grid

Yufei Wang, Weimin Lin, Tao Zhang

***Abstract*—WSNs (Wireless Sensor Networks) have been considered one of the very promising technologies for the implementation of smart grid. And security of WSNs becomes a central concern. The security solutions for generic wireless sensor networks cannot be directly used in smart grid WSNs. In this paper, the applications of sensor networks in electric power systems are discussed and analyzed first. Then, the characteristics of smart grid WSNs are summarized. Threats and security requirements special for wireless sensor networks used in smart grid systems are presented. Based on these works, reference security architecture was proposed to guide the development and the design of the security solutions of wireless sensor networks in smart grid systems, considering the information security requirements of electric power systems. Moreover, open security issues needed solve to protect WSNs applied in smart grid, and research challenges are introduced.**

***Index Terms*-- Electric Power Systems; Information Security Requirements; Multimedia Sensor Networks; Open Security Issues; Security Architecture; Smart Grid; Security Mechanisms; Sensor Networks; Survey; Threats;**

I. INTRODUCTION

The demands for abundant, clean, and sustainable electric energy is rapidly increasing because of the global climate change and the growing populations over the last decades[1]. Many critical issues, such as generation diversification, optimizing expensive assets deployment, demand response, energy saving, and reduction of carbon footprint, cannot be solved by the utility industry across the world within the existing electricity grid, which is unidirectional in nature[2]. The next-generation electricity grid, a "smart grid" or "intelligent grid," has emerged to address these challenges[1], (1) the network congestion and safety related factors; (2) the lack of pervasive and effective communications, monitoring, fault diagnostics, and automation; (3) power grid integration , system stability, energy storage , which are introduced by the adaptation of renewable and alternative energy sources.

The smart grid, is a modern electric power grid infrastructure using intelligent transmission and distribution networks to deliver electricity[1, 3]. The smart grid aims to improve the the efficiency, reliability and safety of the electric system through modern communication technologies, automated control, and dynamic optimization of electric-system operations, maintenance, and planning[1, 3]. The main characteristics of the smart grid are informatization, automation, and interaction, such as the two-way communication of consumption data.

Recent years, wireless sensor networks (WSNs)[4-6] and wireless multimedia sensor networks (WMSNs)[7-8] have been rapidly developed. Various sensors nodes or video sensors deployed in physical environment can sense scale data and multimedia information from surroundings, such as temperature, humidity, and acoustic and visual data. WSNs and WMSNs consist of wirelessly interconnected sensor nodes which can collaboratively and low-costly sense, collect, deliver, and process information in various application areas[4], such as military applications, environmental monitoring, commercial or human centric applications, applications to robotics [9]. And WSNs have been considered one of the very promising technologies for the implementation of Smart Grid [1, 10-12].

However, the smart grid will incur increased risks, some are caused by the adoption of the digital communications and computer infrastructure, some come from the interactions between power companies and consumers[3]. In [3], the smart grid security challenges are considered in four areas, including trust for control systems, communication and device security, privacy, and security management.

With the extensive application of WSNs in almost every aspect of smart grid, including power generation, power transmission, substation, power distribution, utilization and power dispatch, security of WSNs becomes a central concern. The security solutions for generic WSNs cannot be directly used in Smart Grid WSNs, because WSNs are application-specific and sensor networks used in smart grid systems have characteristics different from that of other sensor networks.

The applications of sensor networks in electric power systems such as SCADA, power distribution systems, smart substation, monitoring of transmission and distribution lines, and Advanced Metering Infrastructure (AMI), are discussed and analyzed. The deployment and topology of sensor networks in these systems are studied. Then, the characteristics of Smart Grid WSNs are summarized. Threats

Yufei Wang is with Information Security Lab, Research Institute of Information Technology & Communication, SGEPRI (State Grid Electric Power Research Institute), Nanjing, China (e-mail: wangyufei@sgepri.sgcc.com.cn).

Weimin Lin is with Research Institute of Information Technology & Communication, SGEPRI (State Grid Electric Power Research Institute), Nanjing, China (e-mail: linweimin@sgepri.sgcc.com.cn).

Tao Zhang is with Information Security Lab, Research Institute of Information Technology & Communication, SGEPRI (State Grid Electric Power Research Institute), Nanjing, China (e-mail: zhangtao@sgepri.sgcc.com.cn).

978-1-4244-5940-7/10/$26.00©2010 IEEE

and security requirements special for wireless sensor networks used in smart grid systems are presented. Based on these works, reference security architecture was proposed to guide the development and the design of the security solutions of wireless sensor networks in smart grid systems, considering the information security requirements of electric power systems. Moreover, open security issues needed solve to protect WSNs applied in smart grid, and research challenges are introduced. Finally, we conclude our research work.

II. Characteristics of sensor networks used in Smart Grid

The wireless sensor networks used in smart grids have some characteristics different than the common characteristics of sensor networks, and even WSNs used in different electric power systems have different characteristics, in terms of functional, deployment, networking, topology, QoS requirements, sensors' resource, and so on. And these will influence the design of the WSNs security mechanisms in smart grids.

A. Characteristics of traditional sensor networks

Traditionally, wireless sensor networks and wireless multimedia sensor networks have been conceived to consist of networked sensor nodes that sense scalar, image or video data, communicate and interconnect with each other wirelessly, and are deployed in a physical area to capture, monitor, or possibly control the interesting phenomenon[13]. And WSNs have many distinctive features as follows [4, 7, 13-14]:

(1) Distributed, sensor nodes rapidly interconnect with each other through distributed network protocols and algorithms. Failure of any sensor node will not be influence the whole network;

(2) Redundant and densely deployed, sensor nodes usually are distributed densely deployed to obtain more accurate and complete information from the observed region;

(3) Resource constrained, resource constraints is one of the biggest design challenges for WSNs. The energy, processing, memory, and communication range of sensor nodes is very limited because of its low cost, small size and low power. And wireless communication bandwidth is also constrained.

(4) Multi-hop routing, sensor nodes, which cannot communicate with each other directly, using multi-hop routing to exchange information. The intermediate nodes relay data as routers.

(5) Dynamic network topology, sensor networks have the adaptability to change in network topology and self-heal from node failure quickly.

(6) Security and reliability, sensor networks may be deployed in ugly, hostile, and unattended environments. Sensor nodes must be strong and security enough to avoid broken and information leak.

(7) Collaborative, sensor networks usually complete a global task with better scalability using coordination of localized algorithms.

(8) Application-specific, sensor networks for different applications have different requirements for the network system, and the related hardware, software, and communication protocols will different.

(9) Data-centric, the main task of sensor networks is sensing, deliver, processing, and abstract meaningful data for user. Network processing and control are dependent on the nature of the sensed data.

B. Applications of wireless sensor networks in smart grid

WSNs can be used in the electric power systems to realize smart grid. They have the opportunities and potential to be applied in power generation, power transmission, substation, power distribution, utilization and power dispatch. It is distinct that WSNs will be a vital component and supporting technology of the next generation electric power systems.

One example of sensor networks application is Supervisory Control and Data Acquisition (SCADA) systems, which refers to large scale, distributed measurement, monitoring, and control networks[12]. WSNs can improve the sensing capability of the wired sensor systems and significantly reduce the wiring costs. For other smart grid systems, like power distribution systems, smart substation, monitoring of transmission and distribution lines, Advanced Metering Infrastructure (AMI), and Home Area Networks (HAN), WSNs is also a very promising technology [1, 10-11].

According to the applications, the roles of sensor networks in electric power systems may be sensing, monitoring (and controlling), meter reading, and equipment fault diagnostics:

(1) Sensing and monitoring, safety and reliability are the most critical for electric power systems. And system could be breakdown by environmental factors, such as power grid ice disaster. Sensor networks can be used to monitor the power plant, wind farms, transmission and distribution lines, and substation. The information, can be collected by sensor networks, include wind speed, wind direction, line temperature, humidity, air pressure, rainfall, radiation, line icing, electrical insulator polluted, image, video, and so on.

(2) Meter reading, wireless sensor networks can be widely used in AMI. And WSNs enable low-cost wireless automatic meter reading (WAMR) for electric utilities[1]. WAMR and AMI systems require reliable two-way communications between utilities and the customer's metering devices. Low-cost, low-power wireless smart meters, which are one kind of the sensors, have been recognized as one of the most cost-efficient way to collect meter data by wireless communication[1].

(3) Equipment fault diagnostics[1], wireless sensor networks can be deployed to well monitor the critical system components and coordinate the protection device, in order to avoid and alleviate power grid and facility breakdowns. Compare with the existing sensing, monitoring, and fault diagnostic methods which are too expensive to be large-scale

applied; WSNs provide a feasible and cost-effective technology for the remote equipment monitoring and diagnosis systems.

C. Characteristics of wireless sensor networks in smart grid

The sensor networks applied in the smart grid have some different characteristics from generic ones of traditional sensor networks, which can be outlined as follows [1, 10-12]:

(1) Deployment topology, most of current sensor networks deployed in smart grid systems, use a single hop between sensors and gateway. WSNs in some applications can be multi-hop, such as wireless sensor network for monitoring the status of power transmission lines. And almost all smart grid sensor networking systems have an online trusted third party (monitoring station).

(2) Data processing, all the data obtained by the sensors should be delivered to the controller of monitoring station.

(3) Energy less sensitive, the energy efficiency of the protocols and algorithms is not the first consideration because the battery life of the sensors usually can last several years.

(4) Remote maintenance and configuration, sensors must be remotely accessible and configurable, so that the sensor networks could be maintenance remotely, conveniently and promptly.

(5) Harsh environmental conditions, in electric power system environments, wireless communications may be subject to link failures, RF interference, caustic or corrosive environments, humidity, vibrations, dirt and dust, and other conditions. These will result in dynamic network topologies, nodes malfunction, and information obsolete.

(6) Reliability and latency Quality of Service (QoS) requirements, different WSNs applications for smart grid usually have different QoS requirements in terms of reliability, latency, and network throughput. For most smart grid systems, sensor data are typically time sensitive, even must be real-time in order to be processed timely and leading to right decisions, such as alarm notifications and equipment fault signatures.

(7) High security requirements, security is very important for electric power systems. Sensor networks integrated in smart grid must be well secured to ensure the systems run securely and stably.

III. Threat and Security Factors

Though the usage of WSNs brings significant advantage in smart grid, threats and attacks are also introduced in electric power systems. Availability of the services supported by WSNs, and integrity and the confidentially of the information in WSNs must be achieved in practical WSNs systems. The methods used to protect the security of WSNs should be well developed according to the practical deployments.

A. Security issues in smart grid

With the adoption of information & communication technology in smart grid, and the integration of cyber and information systems, numerous security issues will arise. Any complex system has vulnerabilities and challenges, and the smart grid is no exception[3]. In smart grid, the increasing interaction and integration of electric power systems information systems, and the two-way communication make the security protection more and more difficult. Also wireless communication technologies, such as GPRS/CDMA, 3G/4G, WiFi, WiMax, and ZigBee, have been or will be widely adopted in smart grid systems. And lots of smart meters, mobile smart devices, and smart sensors have been widely used. These make the communication environment more complicated, and increase the difficulty of safety protection.

Some security challenges of smart grid will be quite similar to those of traditional networks, but involving more complex interactions[3] and some new technologies, such as wireless sensor networks, cloud computing, and service-oriented architecture (SOA). The threat and security factors introduced by the new business patterns and new technologies must be well analyzed and solved.

B. Threat and security factors of wireless sensor networks

Security factors may be considered when dealing with security issues of wireless sensor networks can be summarized as follows [15-16].

(1) Availability, Integrity, and Confidentiality: the three main principles in all security programs, which referred to as the AIC triad. Availability ensures reliability and timely access to security objectives (data, resources and network services) to authorized parties when needed. Denial-of-service attacks can destroy the availability of wireless sensor networks. Integrity provides the information and sensor network systems the assurance of the accuracy and reliability, and prevents any unauthorized modification. Confidentiality ensures that the necessary level of secrecy is enforced while data data resides on systems and devices within the sensor network, as it is transmitted, and once it reaches its destination.

(2) Authentication and Authorization: authentication ensures that the communication between one node and another is legal and genuine. Authorization ensures that only authorized nodes can be involved in the sensor networks.

(3) Non-repudiation and Freshness: Non-repudiation denotes that a node cannot deny sending a message it has previously sent. Freshness implies that each data and key is recent, and ensures that no adversary can replay old messages.

(4) Forward and Backward secrecy: Forward secrecy means that a sensor node should not be able to read or know any future messages once it leaves the network. Backward secrecy implies that a newly joining sensor node should not be able to read or know any previously transmitted message.

Security threats of wireless sensor networks in smart grid mainly focus on sensor nodes, wireless networking, and communication protocols. And sensor node compromise and chip compromise are major threat to sensor networks in smart grid, which can lead to internal attacks.

(1) Sensor node and chip attack: attackers capture sensor nodes and reprogram them, such as smart meters. For example[17], an attacker first steals a meter sensor through lock picks, screwdrivers, hacksaw, or other tools. Then he does circuit analysis and device firmware/ configuration data extraction through total phase beagle sniffer, bus pirate, syringe probes, JTAG programmers. And common key material can be recovered through firmware disassembly, entropy analysis techniques. With key content, command and control messages to smart meters can be decrypted and observed by attackers. Then attacker may be able to manipulate and impersonate meters by reversing the protocol through protocol reverse engineering tools. Finally, attacker can select target area to attack, and disable power for target for brief duration for various purposes.

(2) Wireless networking attack: the same as traditional wireless network, wireless communication of sensor networks may be listened or blocked up by the adversary. And messages may be tampered or fabricated.

(3) Communication protocols attack: attacks could be launched at any OSI (Open System Interconnect) layer of a sensor network[15]. For example, congestion attacks at physical layer; collision attacks, exhausting attacks, unfair competition at MAC layer; flooding attack, loss of synchronism attack at network layer.

C. Challenges to secure wireless sensor networks in smart grid

We summarize main security challenges in smart grid sensor networks as follows.

(1) How to secure sensor nodes in smart grid, such as smart meters, and other smart sensor terminals.

(2) When designing the security mechanisms, we should identify the common architecture and resource constraints of the specific sensor networks.

(3) Identifying the security requirements, threat models, and the incentives and methods an attacker can follow[12].

(4) Providing a holistic view of smart grid security vulnerabilities, and design an architecture-based solutions.

In next section, reference security architecture will be designed to provide guidance for securing sensor networks in smart grid.

IV. Security Architecture of Sensor Networks in Smart Grids

Based on the threats, special security requirements, and the characteristics of information security in electric power systems, the reference security architecture of WSNs we proposed for smart grids can be used as a guidance to establish and improve the WSNs security guarantee system in electric power systems. The proposed reference security architecture includes several aspects, such as the security of sensor nodes, protocol stack, authentication, authorization, encryption, secure network access control, introduction detection, management and maintenance of the WSNs.

A. Security model

Fig. 1 shows our security model for smart grid sensor networks.

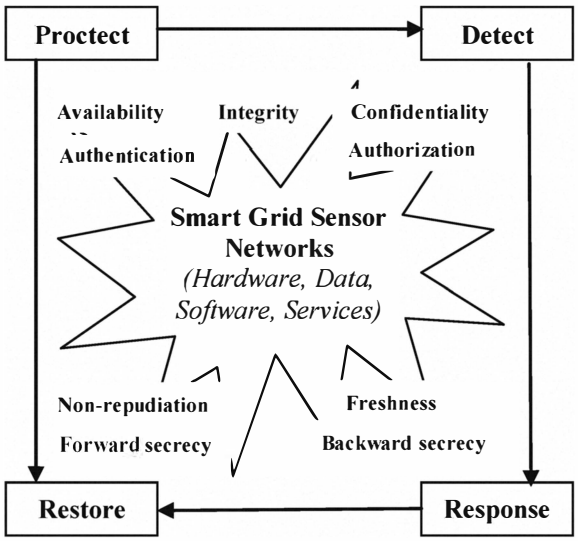

Fig. 1. Security model for smart grid sensor networks

The security model specifies the security objectives, including hardware (for example, sensor nodes), software, data, and network services in smart grid sensor networks; security attributes, including availability, integrity, confidentiality, authentication, authorization, non-repudiation, freshness, forward secrecy, and backward secrecy; and vital security links, including protect, detect, response, and restore.

B. Reference security architecture for the smart grid sensor networks

Fig. 2 shows the reference security architecture we proposed for smart grid sensor networks.

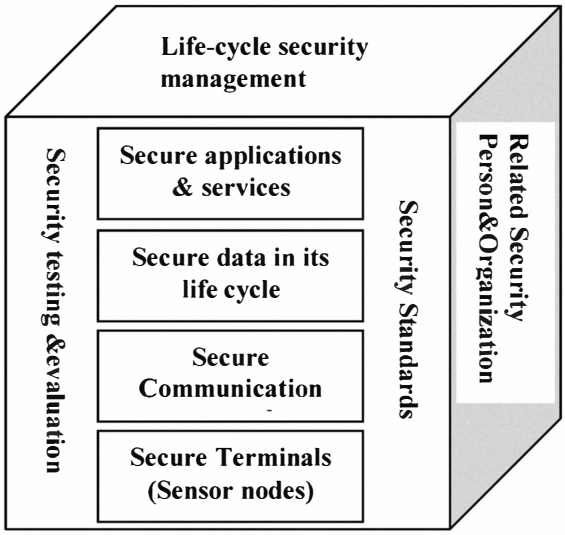

Fig. 2. Reference security architecture for sensor networks in smart grid

The proposed security architecture consists of three main elements: Person & Organization, Management, and Technology. It means that person or organization secure the

wireless sensor networks in smart grid through technological and management measures. Security standards and security testing and evaluation are important support to secure the smart grid sensor networks.

C. Security standards for wireless sensor networks in smart grid

Fig. 3 shows the security standard system for wireless sensor networks applied in electrical power grids.

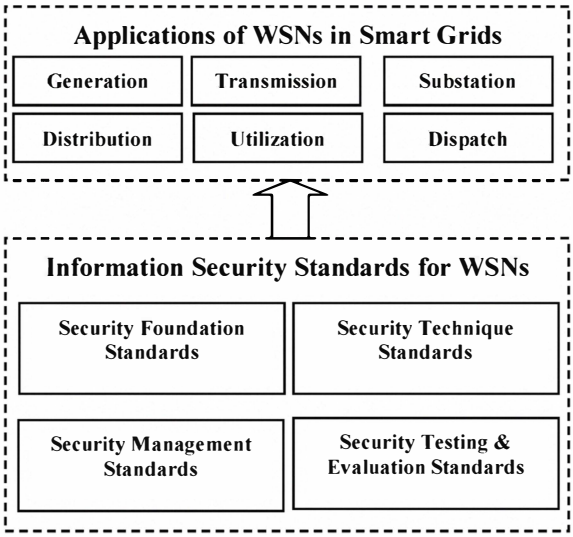

Fig. 3. Security standard system for sensor networks in smart grid

Information security standards for WSNs can be classified into four categories: security foundation standards, security technique standards, security management standards, and security & evaluation standards. The existing security standards of being mature, which are suit for wireless sensor networks, can be tailored according to the application requirements of WSNs in smart grid.

Security foundation standards include security architecture and framework of smart grid WSNs, security technique specification of WSNs applications and services, and other common and fundamental standards suitable for WSNs.

Security technique standards include security equipment standards, security communication protocols standards, data encryption and security transmission standards, authentication standards, and authorization standards.

Security management standards will pay more attention to the terminal & equipment management.

Security testing and evaluation standards include equipment security testing standards, system security testing standards, software security testing standards, and security performance testing standards.

D. Security Technique measures for wireless sensor networks in smart grid

Fig. 4 shows the security technique measures and security objectives for wireless sensor networks applied in electrical power grids.

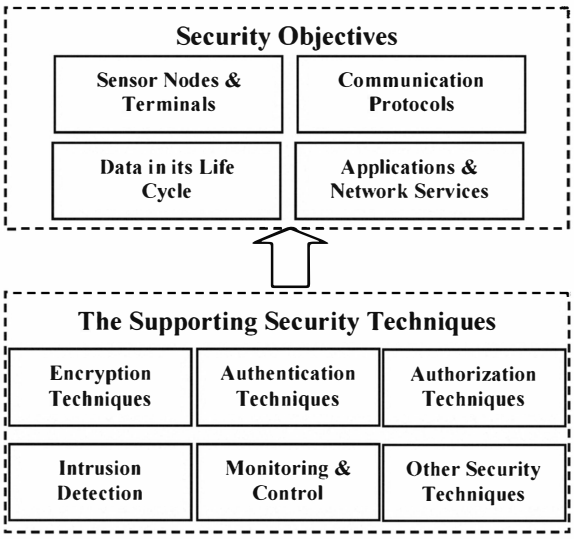

Fig. 4. Security technique measures for sensor networks in smart grid

The supporting security techniques, including encryption techniques, authentication techniques, authorization techniques, intrusion detection techniques, security monitoring and control techniques, and others, can be adapted or tailored according to the characteristics and requirements of the applications of WSNs in smart grid. And these adapted or tailored security techniques can be used to provide secure sensor nodes & terminals, secure communication protocols, secure data in its lifecycle (generation, storage, transmission, usage, and destroy), and secure application & network services.

E. Security management for wireless sensor networks in smart grid

Fig. 5 shows the security management measures for smart grid wireless sensor networks covering all stages of the system life cycle.

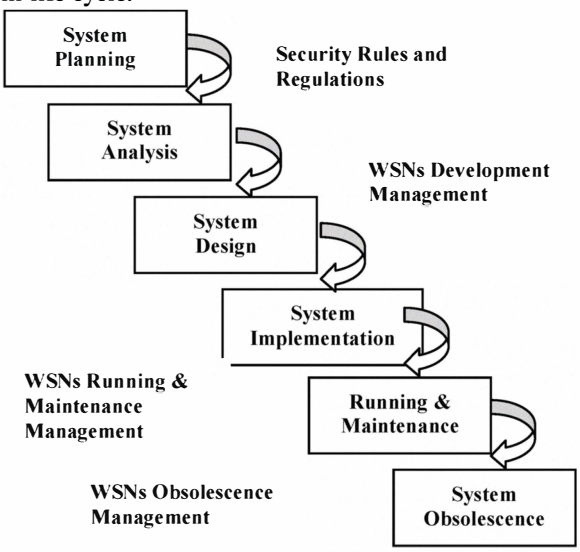

Fig. 5. Life-cycle security management measures for smart grid sensor networks

The lifecycle of WSNs application system mainly consists of six stages: system planning, system analysis, system design,

system implementation, system running and maintenance, and system obsolescence. Through all the states of WSNs system lifecycle, security management measures must be enforced.

F. Security testing and evaluation for wireless sensor networks in smart grid

Fig. 6 shows the security testing and evaluation objectives and the stages of a smart grid WSNs system life cycle in which the security testing and evaluation should be done.

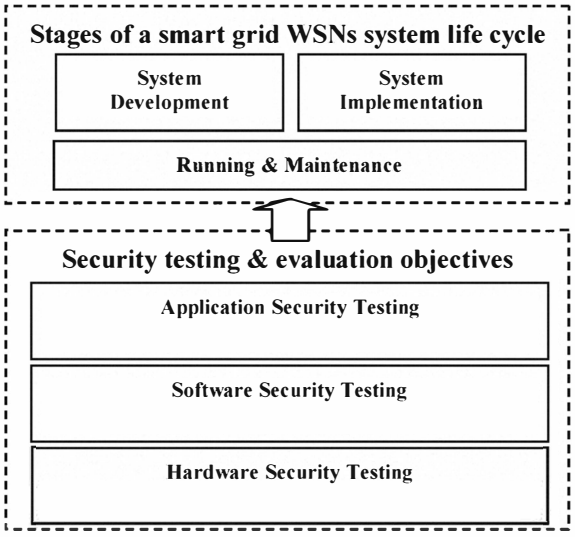

Fig. 6. Security testing and evaluation for sensor networks in smart grid

The security testing and evaluation is necessary in three stages of a smart grid WSNs system life cycle: system development, system implementation, and system running & maintenance.

The objectives of security testing & evaluation should include hardware, software, and application level security testing. Hardware security testing aims to ensure that the sensor nodes, smart meters, and other equipments are secure. Software security testing aims to ensure that the protocols, coding, operating systems, and other software are secure. Application security testing ensures that all the services provided by wireless sensor networks are secure.

G. Persons and Security Organizations in the security architecture

Persons and Security Organizations is the most important in the security protection. They are all the related persons and organizations during the realization of a secure wireless sensor network application in smart grid.

V. Open Issues and Research Challenges

With the rapid development of the smart grids, WSNs will play an important role in the next generation power system. Security issues of WSNs in smart grids should be well researched and solved.

(1) The opportunities and challenges of wireless sensor networks in smart grid must be well analyzed according to the conditions and characteristics of the electric power systems. The advantages and security must be well compromised.

(2) Security standard system for WSNs applications in smart grid is also need to be established, such as standards of secure communication protocols are very important when implementing a wireless sensor networks.

(3) New security technologies should be studied to protect the terminals which were deployed in open areas.

(4) Security testing and evaluation technologies should be developed.

VI. Conclusions

In this paper, we first summarized the characteristics of traditional sensor networks, analyzed the applications of wireless sensor networks in smart grid, and concluded the characteristics of smart grid wireless sensor networks. Then, security issues in smart grid, threat and security factors of wireless sensor networks, and challenges to secure wireless sensor networks in smart grid are deeply studied. Based on these works, the reference security architecture for the smart grid sensor networks was proposed, including security models, reference security architecture, security standard system, security technique and management measures, and security testing and evaluation system.

The proposed reference security architecture provides a holistic view of safeguards for information security and comprehensive security of wireless sensor networks in smart grid. It can be used to guide the security protection through the lifecycle of the WSNs systems. This architecture is appropriate for other WSNs application areas with slight adaptation.

VII. References

[1] V. C. Gungor, et al., "Opportunities and Challenges of Wireless Sensor Networks in Smart Grid - A Case Study of Link Quality Assessments in Power Distribution Systems," Industrial Electronics, IEEE Transactions on, vol. PP, pp. 1-1, 2010.

[2] H. Farhangi, "The path of the smart grid," Power and Energy Magazine, IEEE, vol. 8, pp. 18-28, 2010.

[3] H. Khurana, et al., "Smart-Grid Security Issues," Security & Privacy, IEEE, vol. 8, pp. 81-85, 2010.

[4] I. F. Akyildiz, et al., "A survey on sensor networks," IEEE Communications Magazine vol. 40, pp. 102-114, 2002.

[5] K. R. Fowler, "The future of sensors and sensor networks survey results projecting the next 5 years," in Sensors Applications Symposium, 2009. SAS 2009. IEEE, 2009, pp. 1-6.

[6] K. Fowler, "Sensor survey: Part 2 sensors and sensor networks in five years [Sensor Survey Results]," Instrumentation & Measurement Magazine, IEEE, vol. 12, pp. 40-44, 2009.

[7] I. F. Akyildiz, et al., "A survey on wireless multimedia sensor networks," Computer Networks, vol. 51, pp. 921-960, 2007.

[8] A. Sharif, et al., "Wireless multimedia sensor network technology: A survey," in Industrial Informatics, 2009. INDIN 2009. 7th IEEE International Conference on, 2009, pp. 606-613.

[9] T. Arampatzis, et al., "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks," in Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation Intelligent Control 2005, pp. 719-724.

[10] M. di Bisceglie, et al., "Cooperative sensor networks for voltage quality monitoring in smart grids," in PowerTech, 2009 IEEE Bucharest, 2009, pp. 1-6.

[11] D. Pendarakis, et al., "Information Aggregation and Optimized Actuation in Sensor Networks: Enabling Smart Electrical Grids," in INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE, 2007, pp. 2386-2390.
[12] A. A. Cardenas, et al., "Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems," Ad Hoc Networks, vol. 7, pp. 1434-1447, 2009.
[13] D. Kundur, et al., "Security and Privacy for Distributed Multimedia Sensor Networks," Proceedings of the IEEE, vol. 96, pp. 112-130, 2008.
[14] J. Yick, et al., "Wireless sensor network survey," Computer Networks, vol. 52, pp. 2292-2330, 22 August 2008 2008.
[15] X. Chen, et al., "Sensor network security: a survey," IEEE Communications Surveys & Tutorials, vol. 11, pp. 52-73, 2009.
[16] W. Yong, et al., "A survey of security issues in wireless sensor networks," IEEE Communications Surveys & Tutorials, vol. 8, pp. 2-23, 2006.
[17] W. Sikora, et al. (2009, Smart grid and AMI security concerns. Available: http://inguardians.com/pubs/Smart_Grid_AMI_Security_Concerns-20090723.pdf

VIII. BIOGRAPHIES

Yufei Wang received his PhD at the Department of Computer Science, Nanjing University of Posts and Telecommunications in May 2010. His research interests include wireless and mobile computing, wireless communications, smart gird, information security, and ad hoc and sensor networks.

He is an engineer working in Information Security Lab, Research Institute of Information Technology & Communication, SGEPRI (State Grid Electric Power Research Institute).

Weimin Lin is a Professor Status high level senior engineer working in Research Institute of Information Technology & Communication, SGEPRI (State Grid Electric Power Research Institute). His research interests include information network security of electric power systems.

Tao Zhang is a senior engineer working in Information Security Lab, Research Institute of Information Technology & Communication, SGEPRI (State Grid Electric Power Research Institute). His research interests include information network security of electric power systems.