Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2012, Article ID 492819, 8 pages
doi:10.1155/2012/492819

Review Article

Wireless Sensor Network Applications in Smart Grid: Recent Trends and Challenges

Yide Liu

Faculty of Management and Administration, Macau University of Science and Technology, Taipa, Macau

Correspondence should be addressed to Yide Liu, ydliu@must.edu.mo

Received 28 April 2012; Revised 11 July 2012; Accepted 16 July 2012

Academic Editor: An Liu

Smart grid revolutionizes the current electric power infrastructure by integrating with communication and information technologies. With wireless sensor network, smart grid enables both utilities and customers to transfer, monitor, predict, and manage energy usage effectively and costly. However, the increased application of wireless sensor network also introduce new security challenges, especially related to privacy, connectivity, and security management, causing unpredicted expenditure and disaster to both utilities and consumers. In order to build a reliable wireless sensor network for smart grid, an application review and taxonomy of relevant cyber security and privacy issues is presented in this paper. A unified framework for identification of applications and challenge issues of wireless sensor network in smart grid is developed. Future research directions are discussed at the end of this paper.

1. Introduction

Smart grid can provide efficient, reliable, and safe energy automation service with two-way communication and electricity flows. Through wireless sensor network, it can capture and analyze data related to power usage, delivery, and generation efficiently. According to the analysis results, smart grid can provide predictive power information (e.g., meter reading data, monthly charge, and power usage recommendation) to both utilities and consumers. It can also diagnose power disturbances and outages to avoid the effect of equipments failure and natural accidents. Wireless senor network is adopted by utility companies and suppliers for substation automation management, and it is also widely applied in wireless automatic meter reading (WAMR) system. Based on wireless sensor network, energy usage and management information, including the energy usage frequency, phase angle and the values of voltage, can be read real time from remote devices. Therefore, utility companies can manage electricity demand efficiently. They can reduce operational costs by eliminating the need for human readers and provide an automatic pricing system for customers. Customers can enjoy highly reliable, flexible, readily accessible and cost-effective energy services.

However, wireless sensor network also brings cyber security and privacy challenges to smart grid—many security, privacy and reliability issues appear during electric power delivery. For example, cascading-failure-induced disasters might appear if attackers disrupt the grid at a later date from a remote location; smart grid customers' privacy information might be accessed illegally through wireless sensing network; the adversary might also compromise selected nodes in a tactical delay-tolerant network and thus fail the critical mission of the supervisory control and data acquisition (SCADA) systems [1, 2]. Any of these forms of attack can be highly dangerous to the grid—millions of homes might be left without electric power and businesses could be closed. Besides, power grids are a major resource to the national defense. Therefore, a secure wireless ad hoc and sensor network communication with high capacity must be addressed to ensure a reliable and efficient smart grid.

However, some of current guidelines for electric power system were designed for connectivity, without consideration of wireless risks [3], and some of electric power system security standards do not cover threats through wireless sensor network communication. It may lead to an unsatisfied result to simply transplant wireless sensor network security techniques into the smart grid. An understanding of system

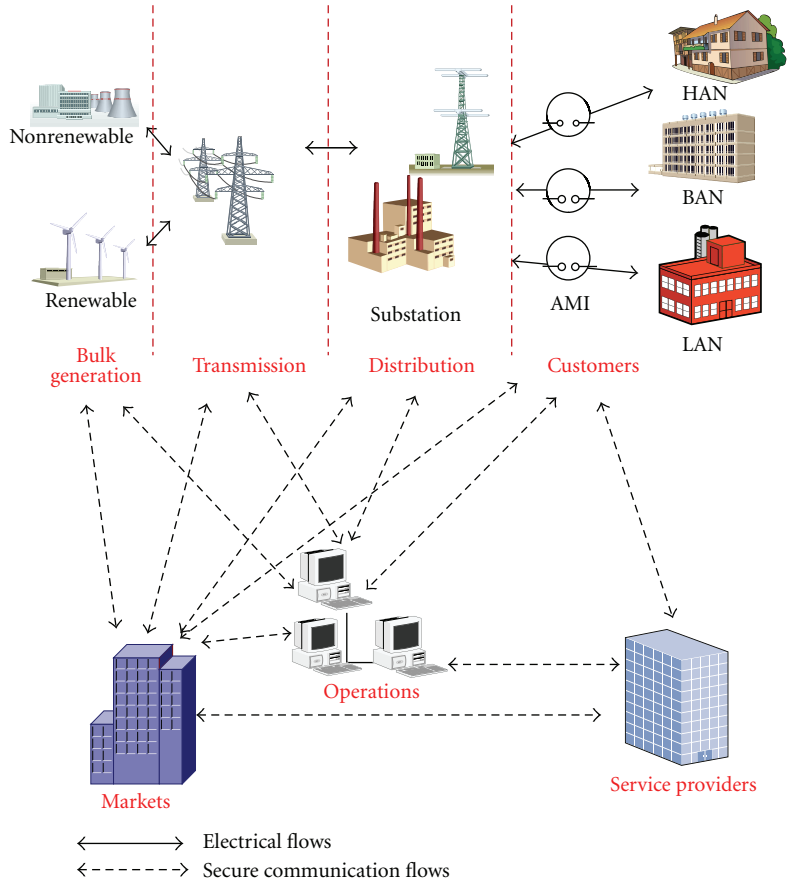

Figure 1: NIST reference model for the smart grid [5].

components with wireless sensor network and associated cyber vulnerabilities is therefore necessary for the smart grid deployments and is the motivation of this paper.

The remainder of this paper is organized as follows. Section two reviews the application of wireless sensor network in smart grid, including WirelessHART, International Society of Automation (ISA) 100.11a, and ZigBee. In Sections three and four, related cyber security and privacy issues in the smart grid are discussed and classified. Section five provides several potential research fields.

2. Wireless Sensor Network Applications in Smart Grid

For distributing energy power from power plants to end customers, smart grid contains three major processes: power generation, power delivery, and power utilization, wherein seven specific domains are going on: power plant domain, substation domain, distribution domain, market domain, operation domain, service provider domain, and customer domain (as show in Figure 1). Recently, WSN has been widely recognized as a vital component of the electric power system, different from wireless ad hoc networks, wireless sensor network contains a large number of low cost, low power, and multifunctional sensor nodes which can be of benefit to electric system automation applications, especially in urban areas [4]. These sensor nodes take advantage of demographic, action, communication, situation, or other data (physical environment, location data, distance, temperature, sound, air pressure, time, lighting levels, people nearby, customer preferences and even customer emotional state, etc.). They can also map the physical characteristics of the environment to quantitative measurements [4].

The collaborative and context-awareness nature of WSN brings several advantages over traditional sensing including greater fault tolerance, improved accuracy, larger coverage area, and extraction of localized features. Sensor nodes can monitor the overall network and to communicate with the control center in the power utility (e.g., a substation), in order to help operators decide the appropriate actions. The sensor node can communicate with the task manager via Internet or satellite. As shown in Figure 2, for developing a wireless sensor network for smart grid, there are three alternatives based on the IEEE 802.15.4 protocol: ZigBee, WirelessHART, and ISA100.11a. For example, ZigBee is a choice for smart grid system networking within home. WirelessHART or ISA100.11a can be used in substation or a generation plant. In this section, the wireless sensor network

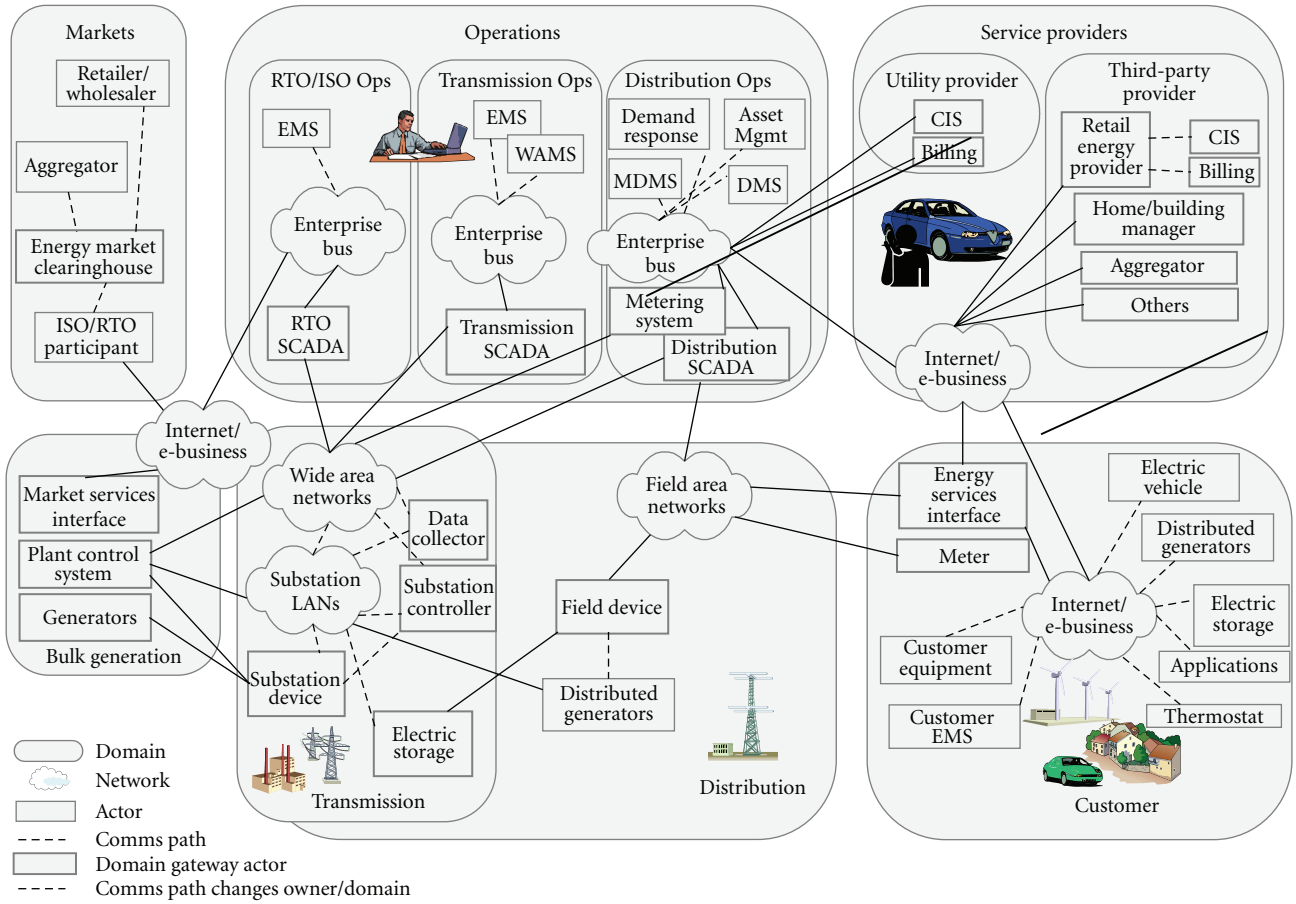

Figure 2: NIST Smart Grid Framework 1.0, September 2009 [6].

application for smart grid will be discussed separately in the context of power generation, power delivery, and power utilization.

2.1. Power Utilization. Wireless sensor network can be used in home area networks (HANs). As mentioned, ZigBee is a suitable choice for HANs. It provides the reliable wide-area coverage and predictable latencies that are expected for smart grid. A typical application of WSN for smart grid is wireless automatic meter reading (WAMR) systems, which can determine real-time energy consumption of the customers as customers can download their archives and take it to meter reading through a mobile device. WAMR can also improve business performance and technical reliability for power utility operations, as utility companies can identify more valuable customers by comparing the data between the distributed generation sources and overall power consumption [4]. WAMR system can remotely control light, heat, air conditioning, and other appliances of different customers.

Smart grid system needs to provide benefits to both the customer and the utility, and the smart meter within HANs perform as an interface that translates, summarizes, and aggregates data of power usage and presents it to the power utility [9]. Inside home, a wireless sensor network can link the various equipments and a central power router as shown in Figure 3. This network could connect to the utility network via a smart meter. The smart meter serves as an interface for a variety of operational signals so that both metering and operational data are carried on the wireless sensor network. For example, a utility can implement the "demand response" function within a home through a price-based incentive signal, and the smart meter infrastructure carry the signal [9]. Specifically, in areas of high population

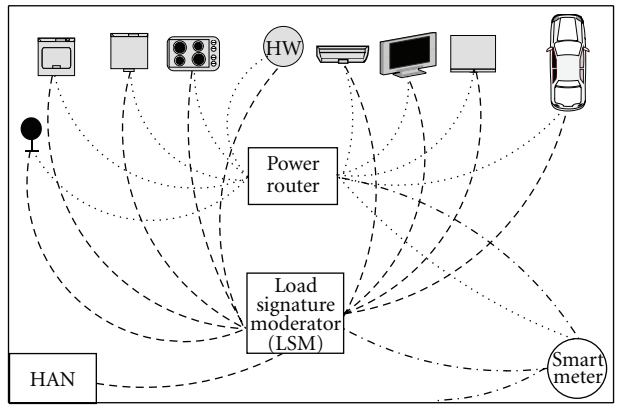

Figure 3: Home area networks (HANs) example [7].

density, the smart meter must be able to different smart grid nodes (SGNs) that belong to each customer by collecting usage information through SGNs [9]. The smart meter may also assert an incentive signal to cause the SGNs to switch to a power-saving profile when the amount of information exchanged is not large [9].

2.2. Power Delivery. Wireless sensor networks can also be used in electric power system operations and substation automation. For example, sensors could be installed to monitor the delivery systems and power use in the system, and sensors can be further classified according to their location. Substations could also be monitored as circuit currents, power usage and station apparatus are checked here [9]. WSNs can also provide a feasible and cost-effective sensing and communication solution for remote system monitoring systems. The conditions of different smart grid operation process, (e.g., generation units, transformers, transmission lines, and motors), can be monitored by the large-scale deployment of smart sensor nodes in a remote, and these nodes can be installed on the critical equipment of smart grid. Therefore, a single system contingency in the power grid can be detected and isolated before it causes cascading effects [10]. Besides, measuring voltages and currents associated with transformers, circuit breakers, and switches in a substation or a distribution station, power quality sensors, transformer temperature sensors, and breaker position indicators may also be monitored [9].

2.3. Power Generation. A bulk generation plant may contain several generation units, and several hundred actuators may control fuel, air, and water flows to optimize heat rate (efficiency of the generator) control emissions, and adjust generator output within each unit [9]. Wireless sensors could be installed to monitor the generation systems in power plants, and WirelessHART or ISA100.11a could be used to deploy sensors here.

Sensors that use IEEE 802.15.4-based radio transceivers can function for several years in harsh environments without requiring any external power (e.g., WirelessHART can route around not only single but also multiple node failures) [9]. Besides, sensors can be easily relocated and supplementary sensors can be deployed within a few hours. Therefore, each generation unit may measure parameters such as steam temperature and air, water, or fuel flow rates based on sensors. This information is fed into the data acquisition system in the power plant [9].

3. Challenges of Wireless Sensor Network in Smart Grid

Although the wireless sensor networks have been facilitating different smart grid operation processes, the characteristics of different WSNs applications are vastly different in features, data rate, and related standards. Therefore, different challenges might appear in different application contexts, which increase the risk of smart grid operation and maintenance.

Common challenges associated with wireless sensor networks are probabilistic channel behavior, accidental and directed interference or jamming, and eavesdropping or unauthorized modification of the communications if not protected by authentication and encryption [9]. Customers' metering information must also be secure. In this section, we detail challenges found in the research literature and map them onto the CERT taxonomy [8].

CERT taxonomy provides a useful framework and uniform terminology to security researchers (see Figure 4).

3.1. Security Requirements. Secrecy, integrity, and availability are three fundamental security requirements, and previous research has provided several basic goals for establishing secure smart grid over the wireless sensor network [1–3, 11–14].

3.1.1. Secrecy. The target of secrecy is to prevent passive attacks and unauthorized access to sensitive data, that is, power usage and billing information. In a wireless sensor network, the issue of confidentiality should address the following requirements [15–17]: (i) a sensor node should not allow its neighbors to read its readings unless they are authorized, (ii) key distribution mechanism should be robust, and (iii) public information (e.g., sensor identities and public keys of the nodes) should be encrypted to protect against traffic analysis attacks. Early detection method could be used for preventing unwarranted communication delays, any manipulation of information must be detected as early as possible. Early detection can also eliminate or reduce false alarms. Besides, privacy is also a critical issue and can be attacked easily, especially in context such as submitting service request for emergency and checking energy usage from smart meters. However, it is not easy to describe the scope of privacy issues for smart grid, as privacy problems can exit not only in personal communications, but also in business transaction among power plant, substations and customers. Unfortunately, there has not been a well-established standard for smart grid privacy issues. Standard-based privacy protection schemes could be a solution. For example, EG2 made a suggestion to separate the smart metering data into low-frequency attributable data (e.g., data used for billing) and high-frequency anonymous technical data (e.g., data used for demand side management) aiming to protect privacy [18].

3.1.2. Integrity. The target of integrity is to ensure that the transmitted data is not illegally modified (e.g., changing, deleting, creating, delaying, or replaying data) from the sender to the recipient, and the identity and content of the received data must be verified to be the same as the original source. An authentication method could be developed for ensuring that the origin and destination of information is correctly identified, the injection of corrupted data by unauthorized entities must be prevented.

3.1.3. Availability. The target of availability is to ensure the wireless sensor network services to be available to authorized users on time, even in presence of an internal or external attack (e.g., denial of service attack). To reach this target, both additional communication among nodes and a central

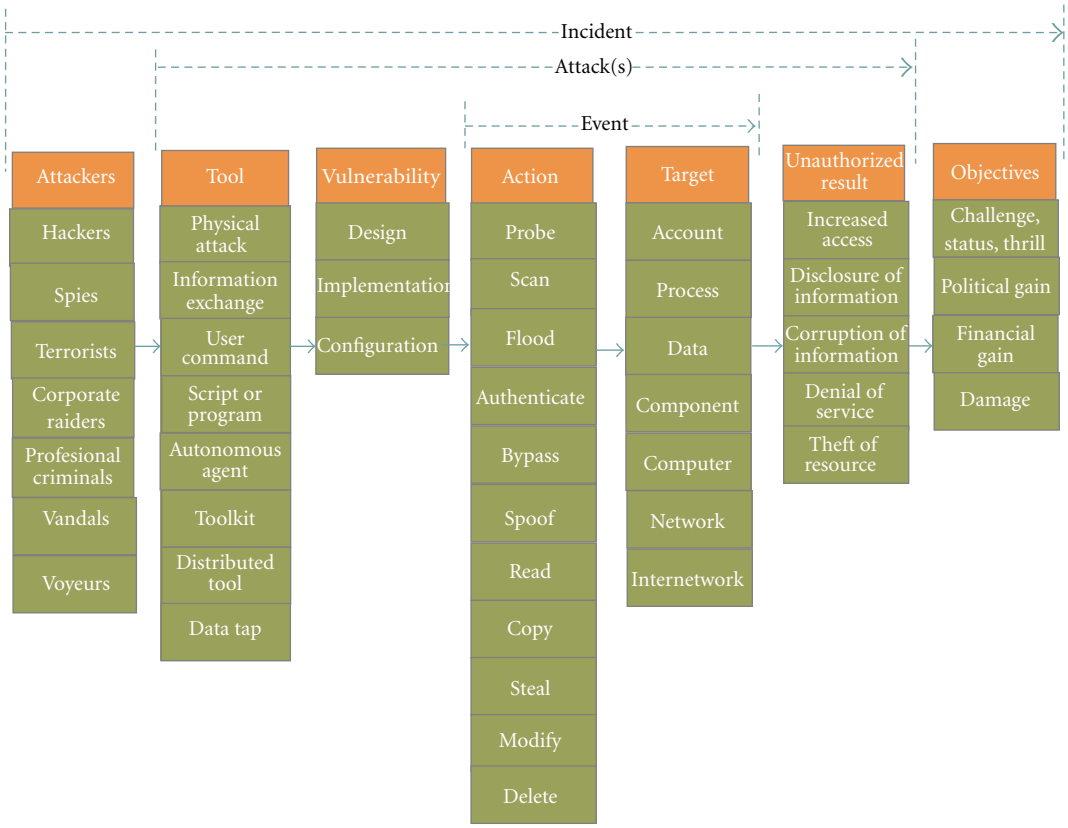

Figure 4: Attack taxonomy by CERT Coordination Center [8].

access control system may be adopted for successful delivery of every message to its recipient [15, 19]. A solution is to make sure all actions performed on any information must be logged for a time period.

3.2. Attacks Taxonomy. CERT taxonomy focuses on incidents, and an incident within CERT taxonomy means that an attacker executes one or more attacks to achieve specific objectives. Additionally, based on the target each incident, different tools are used to exploit vulnerabilities to produce an unauthorized result. Table 1 listed the main attackers and objectives.

Table 1: Attackers and objectives of wireless sensor network in smart grid.

Attacker	Objective
Professional criminals	Damage or steal smart grid devices like smart meters and home appliances
Terrorists	Cause harm
Vandals	Crack
Hackers	Crack
Voyeurs	Gain access to related devices and related data

3.2.1. Device Issues. Devices related with wireless sensor network include smart meter and AMI devices. These devices bring significant advantages for users and create challenge issues at the same time because date and signals transmitted by these devices contain the information about presence of people at their residence and what appliances are in use. Depuru et al. listed certain sections of people who might be interested in collecting and analyzing the data transmitted through wireless network, including revengeful exspouses, civil litigant, illegal consumers of energy, extortionists, terrorists, political leaders with vested interests, thieves, and so forth [4]. For example, professional criminals may damage smart grid devices and steal costly device components for financial gain. Therefore, the location of smart meters should not be easy to touch. Hackers may gain access to related devices and related data (e.g., metering database, meters battery change, removal, and modification information) for challenging themselves [20, 21]. Voyeurs may remote connect/disconnect meters and outage reporting [20, 22]. Therefore, it needs high security to protect customer information and devices. Possible solutions include ensuring the integrity of meter data, detecting unauthorized changes on meter, and authorizing all accesses to/from AMI networks [23]. In fact, challenges are not only from deliberate attacks, but also include other possible human errors and system vulnerabilities, such as weak smart grid user authentication

Table 2: Attacks of wireless sensor network in smart grid.

Target	Vulnerability	Actions	Unauthorized result	Tool
Device	Design/implementation	Steal, destroy, or replace devices	Meter storage tampering	Thieves tools
Sensor data	Inadequate physical tamper protections	Jamming attacks	Service or data lost	Jamming
Communication ability	Network failures/crypto or protocol issues	Jamming attacks/spoof/scan	Communication interception	Script or program
Account/data	No firmware integrity protections	Spoof/scan/read	Password extraction	Malicious software

control, weak communication protocol, and improper communication management.

3.2.2. Networking Issues. Routing information in wireless sensor networks can be changed, and this challenge can result in unauthorized control of the communication network. For example, an intruder can take over vulnerable equipments and mislead the data presented to smart grid operators.

Jamming attacks could be seen as the most well-known attacks that compromise availability of wireless sensor networks. The possibility of jamming may appear with any radio-based medium, and the sensor nodes may be deployed in hostile or insecure environments where an attacker has the physical access. Jamming is a type of attack which interferes with the radio frequencies that the sensor nodes use for communication [15, 19, 24]. A jamming source may be powerful enough to disrupt the entire network. Even an intermittent jamming may cause negative effect as the message communication in a WSN may be extremely time-sensitive [15, 25]. Besides, the integration of other communication systems might result in arduous challenges of protecting smart grid, especially when integrating smart gird with existing public network [3]. AES (advanced encryption standard) encryption [26, 27] could be a possible solution for protecting sensor network.

WSNs' vulnerabilities include design and implementation of wireless sensor networks for smart grid. The design and implementation of WSNs are constrained by three types of resources: (i) energy, (ii) memory, and (iii) processing [23]. During different communication processes, the lack of sensor battery may lead to the failure of smart grid. Sensor nodes have limited battery energy supply [28], but in smart grid, the batteries of the sensors can be charged by the energy supplies [23]. The collaborative effort of sensor nodes can handle the problems of limited memory and processing capabilities of the sensor nodes [23]. Table 2 described the wireless sensor networks attacks.

3.2.3. Other Technical Challenges. Other technical challenges for wireless sensor network in smart grid include harsh environmental conditions, reliability and latency requirements, and packet errors and variable link capacity [10]. In smart grid environment, sensors may also be subject to RF interference, highly caustic or corrosive environments, high humidity levels, vibrations, dirt and dust, or other conditions; furthermore, the topology and wireless connectivity of the network may vary [10]. The harsh environmental conditions may disturb a portion of sensor nodes in information delivery process.

When wireless sensor communicating across power utilities and customers, the power plants are in charge of exchanging data (e.g., peer transmission and distribution system operation) or regional transmission organization (e.g., substations, end users, or other power plants), and substations are in charge of exchanging important information (e.g., protection data among substations) and alarms. In short, power plants provide operation services such as switching operation, changing setups, recommendation of optimized operations, starting emergency procedure and performing system restorations [3], and substations always take the responsibility of power system protection, load shedding, recovery from load shedding, shunt control and compensation control [3]. Therefore, the wide variety of applications of WSNs in smart grid will have different requirements on quality-of-service (QoS), reliability, latency, network throughput, and so forth [10]. In addition, sensor data are typically time sensitive [10].

In WSNs, the bandwidth of each wireless link depends on the interference level of the receiver, and high bit error rates (BER $= 10^{-2} - 10^{-6}$) are required in communication [10]. Deliberate attacks which can overwhelm the forwarding capability of nodes, and they can also consume sparsely available bandwidth. These challenges can result in a denial of service to advanced metering infrastructure (AMI) applications based on WSNs. In addition, wireless links perform varying characteristics over time and space due to obstructions and harsh environment in smart grid. Therefore, it may be difficult for wireless links to meet QoS requirements due to the bandwidth and communication latency at each wireless link are location-dependent and can vary continuously [10]. Figure 5 is a modified version of CERT taxonomy based on what we discussed, and it can be seen as a unified framework for identification challenge issues of wireless sensor network in smart grid.

4. Conclusion

The number of applications of smart grid over wireless sensor networks has been steadily increasing, such as wireless

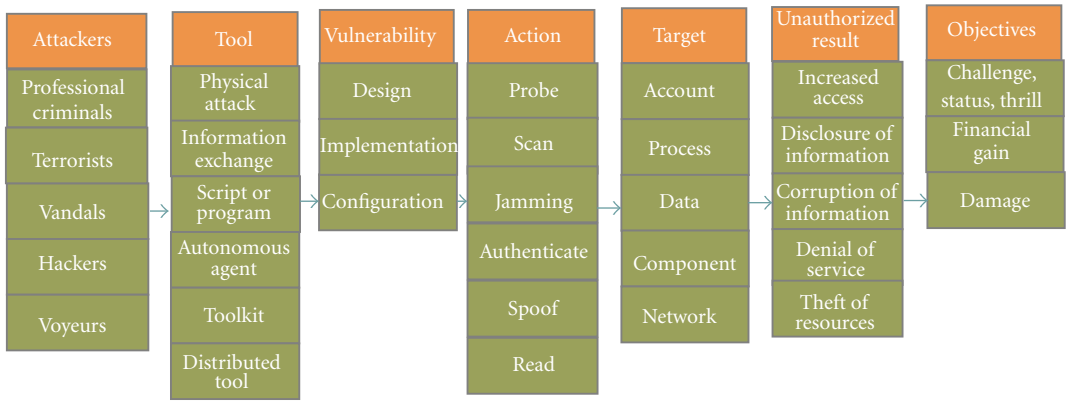

Figure 5: Modified attack taxonomy.

automatic meter reading (WAMR) and remote monitoring systems. However, since radio waves in wireless communication spread in the air, one common risk is that wireless channels are more insecure and susceptible to numerous attacks than wired networks [1]. Much existing work has attempted to incorporate security into smart grid.

To better understand securing service for smart grid over wireless networks, we have presented known attacks that can disrupt wireless sensor network in smart grid communication based on CERT taxonomy. We modified the taxonomy in Figure 5 based on the security analysis in Section 3. We have discussed the recent trends of wireless sensor networks and illustrated basic security requirements to safeguard smart grid against these attacks. We have also reported several existing solutions to wireless sensor network security in smart grid.

It is important to note that there is no single implementation that will define the communications architecture of smart grid. Although we realized security issues, the solutions may also require management effort with policy. For example, a power plant could dine security policies and procedures for maintaining and controlling collaboration with both substations and market, and the next generation of smart metering technology might depend on the policies of utility companies and respective governments [18]. It is misleading to suggest that IT people should take the full responsibility for wireless smart grid network security. However today, there are little common rules or standards for the data exchange or resources usage in the wireless smart grid communication. We are studying this challenge in a case study in related companies.

Acknowledgment

This work was supported by Faculty Research Grant of Macau University of Science and Technology (Project 0236 name: Research on Key Technologies of Context-Aware Computing Based on Mobile Social Network and System Design).

References

[1] 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.

[2] P. Sakarindr and N. Ansari, "Security services in group communications over wireless infrastructure mobile ad hoc, and wireless sensor networks," *IEEE Wireless Communications*, vol. 14, no. 5, pp. 8–20, 2007.

[3] D. Wei, Y. Lu, M. Jafari, P.M. Skare, and K. Rohde, "Protecting smart grid automation systems against cyberattacks," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 782–795, 2011.

[4] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Smart meters for power grid: challenges, issues, advantages and status," *Renewable and Sustainable Energy Reviews*, vol. 15, no. 6, pp. 2736–2742, 2011.

[5] U.S. NIST, "NIST framework and roadmap for smart grid interoperability standards, release 1. 0," NIST Special Publication 1108, 2010, http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

[6] A draft version of this publication by NIST, http://www.nist.gov/public_affairs/releases/upload/smartgrid_092409_fr.pdf.

[7] G. Kalogridis, C. Efthymiou, S.Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: towards undetectable appliance load signatures," in *Proceedings of the 1st IEEE International Conference on Smart Grid Communications*, pp. 232–237, Gaithersburg, Md, USA, October 2010.

[8] J. D. Howard and T. A. Longstaff, "A common language for computer security incidents," Sandia National Laboratories, Sandia Representative, SAND98-8867, 1998.

[9] B. A. Akyol, H. Kirkham, S. L. Clements, and M. D. Hadley, "A survey of wireless communications for the electric power system," U.S. Department of Energy, 2010.

[10] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 10, pp. 3557–3564, 2010.

[11] V. C. Gungor and F. C. Lambert, "A survey on communication networks for electric system automation," *Computer Networks*, vol. 50, no. 7, pp. 877–897, 2006.

[12] 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.

[13] W. Lou and K. Ren, "Security, privacy, and accountability in wireless access networks," *IEEE Wireless Communications*, vol. 16, no. 4, pp. 80–87, 2009.

[14] H. S. Yang, H. S. Jang, Y. W. Kim et al., "Communication networks for interoperability and reliable service in substation automation system," in *Proceedings of the 5th ACIS International Conference on Software Engineering Research, Management, and Applications (SERA'07)*, pp. 160–165, Busan, Korea, August 2007.

[15] J. Sen, "A survey on wireless sensor network security," *International Journal of Communication Networks and Information Security*, vol. 1, no. 2, pp. 59–82, 2009.

[16] D. W. Carman, P. S. Krus, and B. J. Matt, "Constraints and approaches for distributed sensor network security," Tech. Rep. 00-010, NAI Labs, Network Associates Inc., Glenwood, Md, USA, 2000.

[17] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, 2002.

[18] F. Zhong, S. Gormus, C. Efthymiou et al., "Smart grid communications: overview of research challenges, solutions, and standardization activities," *IEEE Communications Surveys and Tutorials*, vol. PP, no. 99, pp. 1–18, 2012.

[19] Z. Lu, W. Wang, and C. Wang, "From jammer to gambler: modeling and detection of jamming attacks against time-critical traffic," in *Proceedings of the IEEE INFOCOM 2011*, pp. 1871–1879, Shanghai, China, April 2011.

[20] U.S. NIST, "Guidelines for smart grid cyber security (vol. 1 to 3)," NIST IR-7628, 2010, http://csrc.nist.gov/.

[21] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An integrated security system of protecting smart grid against cyber attacks," in *Proceedings of the Innovative Smart Grid Technologies Conference (ISGT'10)*, pp. 1–7, Gaithersburg, Md, USA, January 2010.

[22] R. Anderson and S. Fuloria, "Who controls the off switch?" in *Proceedings of the 1st IEEE International Conference on Smart Grid Communications (SmartGridComm'10)*, pp. 96–101, Gaithersburg, Md, USA, 2010.

[23] Y. Xiao, Y. Xiao, S. Li, W. Liang, and C. Chen, "Cyber security and privacy issues in smart grids," *IEEE Communications Surveys and Tutorials*, vol. PP, no. 99, pp. 1–17, 2012.

[24] Q. Zeng, H. Li, and P. Dai, "Frequency hopping based wireless metering in smart gird: code design and performance analysis," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM'11)*, pp. 1–5, Houston, Tex, USA, December 2011.

[25] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[26] P. Zhang, O. Elkeelany, and L. McDaniel, "An implementation of secured Smart Grid Ethernet communications using AES," in *Proceedings of the IEEE SoutheastCon 2010 Conference: Energizing Our Future*, pp. 394–397, Concord, NC, USA, March 2010.

[27] A. Bartoli, J. Hernández Serrano, M. Soriano et al., "Secure lossless aggregation for smart grid M2M networks," in *Proceedings of the 1st IEEE International Conference on Smart Grid Communications (SmartGridComm'10)*, pp. 333–338, Gaithersburg, MD, USA, October 2010.

[28] Idaho National Laboratory, "Common cyber security vulnerablilities observed in control system assessments by the INL NSTB program," Idaho National Laboratory Technical Report INL/EXT-08-13979, Idaho National Laboratory, 2008, http://www.inl.gov/scada/publications.