Cyber Security and Privacy Issues in Smart Grids

Jing Liu and Yang Xiao, *Senior Member, IEEE,* Shuhui Li, Wei Liang, C. L. Philip Chen, *Fellow, IEEE,*

***Abstract*—Smart grid is a promising power delivery infrastructure integrated with communication and information technologies. Its bi-directional communication and electricity flow enable both utilities and customers to monitor, predict, and manage energy usage. It also advances energy and environmental sustainability through the integration of vast distributed energy resources. Deploying such a green electric system has enormous and far-reaching economic and social benefits. Nevertheless, increased interconnection and integration also introduce cyber-vulnerabilities into the grid. Failure to address these problems will hinder the modernization of the existing power system. In order to build a reliable smart grid, an overview of relevant cyber security and privacy issues is presented. Based on current literatures, several potential research fields are discussed at the end of this paper.**

***Index Terms*—smart grid; SCADA; AMI; security; privacy; accountability**

I. Introduction

WHILE technology and innovation continue to modernize industry, our electric power system has been maintained in the same way for decades. The increasing load and consumption demands increase electricity complications, such as voltage sags, black outs, and overloads. Meanwhile, the current electrical network contributes greatly to carbon emissions. The United States' power system alone takes up 40% of all nationwide carbon dioxide emissions [46]. Considering both economic and environmental interests, substantial changes must be made to such an unstable and inefficient system. Therefore, many nations (e.g., U.S., EU, Canada, China, Australia, South Africa, etc.) are now modernizing their power grids [42]. They believe that they not only require reliability, scalability, manageability, and extensibility, but also that they should be secure, interoperable, and cost-effective. Such an electric infrastructure is called a "smart grid."

Generally speaking, the smart grid is a promising power delivery infrastructure that is integrated with two-way communication and electricity flows. Through advanced sensing technologies and control methods, it can capture and analyze data regarding power usage, delivery, and generation in near-real-time [1]. According to the analysis results, the smart grid may provide predictive information and corresponding recommendations to all stakeholders (e.g., utilities, suppliers, and consumers) regarding the optimization of their power utilization [1]. It may also offer services like intelligent appliance control for energy efficiency and better integration of distributed energy resources (DERs) to reduce carbon emissions [2]. Apparently, it is not a simple grid in the sense of our current power grid. It can be regarded as a "system of systems" that involves both information technology (IT) and electricity system operations and governance. Such a complex system undoubtedly presents many challenges, especially in cyber security and privacy aspects [3]. Based on experiences gained from developed IT and telecommunication systems, we know that the envisioned grid will be a potential target for malicious, well-equipped, and well-motivated adversaries. Specifically, the grid can be subject to physical attacks by a human being, by malicious software that can harm the control system, or by using up the systems' resources to perform the attacker's own tasks. Any of these forms of disruption occurring to the grid can be highly dangerous. Threats such as fiddling with billing information of particular users can cause a major economical disturbance, if they are not monitored carefully. The power grids, on the other hand, are a major resource to the national defense, and any form of attack on these can cause havoc. Furthermore, increased connectivity of the grid will enable personal information collection, which may invade consumers' privacy. Failure to eliminate these threats

TABLE I
Differences Between IT Networks and Smart Grid

Categories	IT Networks	Smart Grid
Security Objectives	Confidentiality > Integrity > Availability	Availability > Integrity > Confidentiality [3]
Architecture	1) flexible and dynamic topology; 2) center server requires more protection than periphery hosts [30].	1) relatively stable tree-like hierarchy topology; 2) some field devices require the same security level as the central server [30].
Technology	1) diverse operating systems; 2) public networks; 3) IP-based communication protocols	1) proprietary operating systems; 2) private networks; 3) IEC61850- and DNP (Distributed Network Protocol) - based communication protocols.
Quality of Service	1) transmission delay and occasional failures are tolerated; 2) allow rebooting [30].	1) high restrictions on transmission delay and failures; 2) rebooting is not acceptable [30].

Manuscript received 27 October 2010; revised 3 August 2011, 11 November 2011, and 19 November 2011.

J. Liu and Y. Xiao are with Department of Computer Science, The University of Alabama, Tuscaloosa, AL 35487 USA (e-mail: jliu39@crimson.ua.edu, yangxiao@ieee.org).

S. Li is with Department of Electrical and Computer Engineering, The University of Alabama, Tuscaloosa, AL 35487, USA (e-mail: sli@eng.ua.edu).

W. Liang is Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang, 110016 China (e-mail: weiliang@sia.ac.cn).

C. L. P. Chen is Faculty of Science of Tech., University of Macau (e-mail: Philip.Chen@ieee.org).

Y. Xiao is with the Department of Computer Science, The University of Alabama, 101 Houser Hall, Box 870290, Tuscaloosa, AL 35487-0290 USA (e-mail: yangxiao@ieee.org). Corresponding author.

Digital Object Identifier 10.1109/SURV.2011.122111.00145

will hinder the modernization of the existing power industry. Although contemporary security technologies, such as virtual private networks (VPNs), intrusion detection systems (IDSs), public key infrastructure (PKI), anti-virus software, firewalls, etc., have well protected the IT infrastructure, they still cannot be very effective by directly deploying them without changes in the smart grid due to their inherent differences, as described in Table I. For example, intruders may utilize VPN to hack the power grid. The North American Equipment Council (NREC) reported the effects of a slammer worm on the power utilities used over in North America [48]. In a quoted example they claim: "The worm migrated through a VPN connection to a company's corporate network until it finally reached the critical supervisory control and data acquisition (SCADA) network. It infected a server on the control-center LAN that was running MS-SQL. The worm traffic blocked SCADA traffic."

In fact, we may transplant some IT security techniques into the smart grid to meet its security and privacy requirements. However, while choosing any of the possible security measures, there always exists a tradeoff among security, cost, and performance. Employing firewall or proxy systems may reduce the risk of having a denial of service attack on the servers, but these strategies fail when there is an attack on the application layer, such as planting a Trojan. A Trojan horse referred to here is malicious software that acts as if it performs the intended functionality, but secretly passes credentials and other secure information to the attacker. Power grids usually are equipped with their own subnets and IP segments. These measures tend to make them a little more secure when compared to general systems built off the Internet, but an attack by gaining physical access to the system can rarely be avoided. An understanding of system components 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 II briefly gives an overview of the smart grid and relevant technologies. In Sections III and IV, cyber security and privacy issues in the smart grid are discussed, respectively. Section V provides future research directions. Finally, we conclude this paper in Section VI.

II. Overview of Smart Grid

A. Features

In 2007, the U.S. National Energy Technology Laboratory (NETL) [6] identified seven principal characteristics for modern power grid design. Later in 2009, the U.S. Department of Energy (DOE) merged two of them (self-heals and resists attack) and restated the design features and benefits for smart grid as follows [2]:

1) Enabling Informed Participation by Customers: Unlike traditional power systems, customers are better informed by a two-way communication technology. The entire smart grid becomes an active electricity market that allows customers to shift load and to generate and store energy based on near-real-time prices and other economic incentives. Through bi-directional electricity flow, customers are also able to sell surfeit stored energy back to the grid when the price is high. Such demand-response mechanisms help the grid balance power supply and demand, thus enhancing the efficiency of power usage.

2) Accommodating All Generation and Storage Options: The smart grid not only accommodates remote centralized power generation, but also adopts diverse and widespread distributed energy resource (DER) (e.g., solar, wind, or geothermal energy) through flexible network architecture and distributed management. This concept is proposed to alleviate peak load, to support back-up energy during emergencies, and to satisfy the grid's developing in accordance with the natural environment, society, and the economy.

3) Enabling New Products, Services, and Markets: New products and services are essential parts of the smart grid that can promote low-cost and green solutions for all power users. By using consumer-oriented "smart appliances" or intelligent electronic devices (IEDs), for instance, customers or authorized service providers can remotely control IEDs' power usage. Markets act as coordinators managing a series of independent grid parameters, such as time, capacity, the capacity rate of change, service quality, etc. When necessary, markets will adjust those variables to balance the power supply and demand of the entire grid.

4) Providing the Power Quality for the Range of Needs: Power quality involves factors like voltage flicker, voltage volume, momentary interruptions, etc. Different consumers may have distinct power quality requirements (e.g., industrial vs. residential users). To satisfy a particular consumer's power usage, the smart grid must meet a wide range of power quality needs in terms of architectural designs and contract concerns.

5) Optimizing Asset Utilization and Operating Efficiently: The smart grid is a complex system of systems that manages a variety of appliances, facilities, and DERs. Optimizing the utilization of those assets and enabling efficient operation and maintenance will reduce both whole life-cycle and investment costs and power consumption. A reasonable and robust management method should therefore be developed.

6) Operating Resiliently to Disturbances, Attacks, and Natural Disasters: This concept is proposed to ensure the reliability of the power grid. Regardless of the type of physical damages or cyber attacks, the smart grid can effectively resist these problematic events through local, regional, and national coordination. As a countermeasure, authorized operators can quickly isolate the suspected grid components and readjust nearby DERs to support the affected areas. The smart grid is also able to "self-heal" hidden faults by using technologies such as advanced sensing systems, timely detection, automatic control devices, etc.

B. Architecture

To date, the architectural framework and implementation standards of the smart grid are still under investigation by the academic [7], [8], [16], industrial [1], [17], [18], [30], and government sectors [2], [4], [6]. Although there are various designs for the grid architecture, almost every case follows the common reference model [4] proposed by the U.S. National Institute of Standards and Technology (NIST).

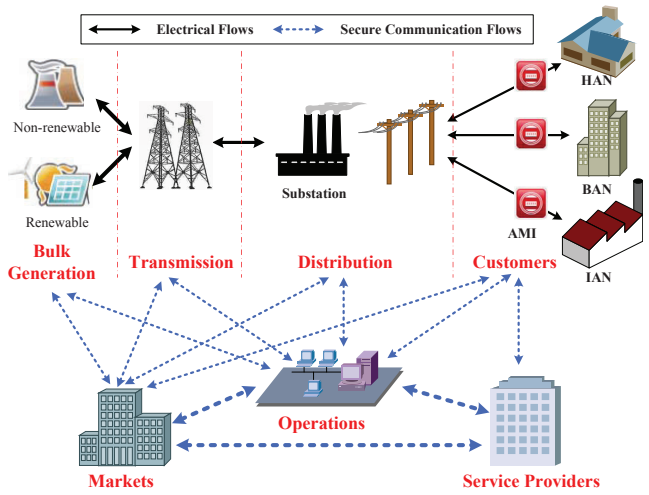


Fig. 1. NIST reference model for the smart grid [4]

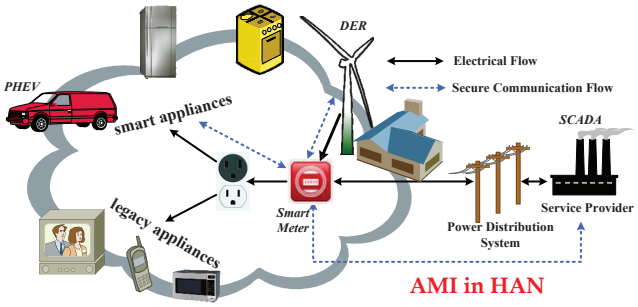


Fig. 2. A use case of AMI in HAN

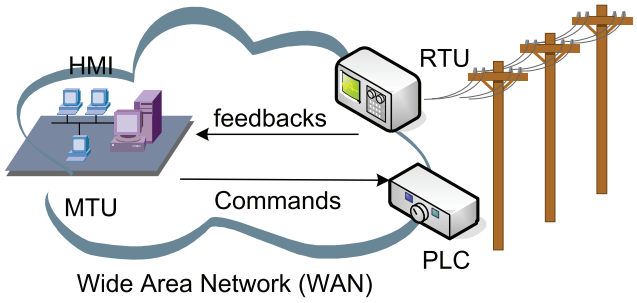


Fig. 3. A typical SCADA architecture [37]

As shown in Fig. 1, NIST's model consists of seven logical domains [4]. Each one of the above four (Bulk Generation, Transmission, Distribution, and Customers) can generate, store, and deliver electricity in two-way. The bottom three (Markets, Service Providers, and Operations) mainly manage the movement of electricity and provide relevant information or services to power consumers and utilities. Three types of customers are present in this model: HAN (Home Area Network), BAN (Building Area Network), and IAN (Industrial Area Network). Within those areas, AMI (Advanced Metering Infrastructure) is deployed to monitor all incoming and outgoing electrical and communication flow.

To interconnect these domains, Cisco [1] argued that the whole system should use an independent "network of networks." It also claimed that the best standard suite of protocols for the smart grid is the Internet Protocol (IP) [1]. Since IP has already achieved great success in the current Internet in terms of flexibility, security, and interoperability, Cisco believes that the interoperability standards of the smart grid should use IP architecture as reference [1]. In addition, several researchers have proposed their own opinions on how to implement this model. Clark and Pavlovski [7] studied the pros and cons of wireless network applications for the smart grid and then suggested adopting 3G/4G technology for the architectural design. Gadze [8] presented a hierarchical architecture for the operations domain, which is a multi-level decentralized control platform dealing with the potential impacts of emergencies. Wei [16] proposed a peer-to-peer structure for the power delivery system. Basically, every consumer and power generator acts as an interconnected node in a web-like network. Such grids can dynamically balance power supply and demand, but they require more flexible and robust management. The rest of the presented architectures [9]–[11], [22] are in some way focused on one of four technical issues of the grid: (1) transmitting data over multiple media, (2) collecting and analyzing massive amounts of data rapidly, (3) connecting large numbers of devices and systems, and (4) ensuring reliability and security.

C. Key Components

1) AMI (Advanced Metering Infrastructure): AMI is an integration of multiple technologies that provides intelligent connections between consumers and system operators [5]. Major applications include smart meters, HAN, meter data management systems (MDMS), and operational gateways (as shown in Fig. 2) [5]. It is designed to help consumers know the near-real-time price of electricity and thus to optimize their power usage accordingly [4], [5]. It also helps the grid obtain valuable information about consumers' power consumption in order to ensure the reliability of the electrical power system [6].

2) SCADA (Supervisory Control and Data Acquisition): SCADA system is responsible for the real-time monitoring and control of the power delivery network [17], [30]. Through intelligent remote control and distributed automation management at medium voltage substations, it can both help the grid reduce operation and maintenance costs and ensure the reliability of the power supply [17], [22]. Two related subsystems are the energy management system (EMS) and the distribution management system (DMS) [18], [28].

Basically, SCADA systems consist of four parts (as shown in Fig. 3) [37]: 1) field data interface devices such as remote terminal units (RTUs) and programmable logic controllers (PLCs), 2) a communication system (e.g., telephone, radio, cable, satellite, etc.), 3) a central master terminal unit (MTU), and 4) human machine interface (HMI) software or systems. By using RTUs and PLCs, most control actions can be performed automatically and remotely [17], [18]. The Idaho National Laboratory (INL)'s report [15] claimed that the current SCADA system has lots of vulnerabilities (discussed in Section III-C), but that many of them are proprietary. Creery *et al.* [47] discussed a few realistic situations of attack on phys-

ical SCADA systems that caused a major stir in the industry. To secure a SCADA network, a variety of technologies are involved, including user and device authentication, firewalls, IPSec (Internet Protocol Security), VPN, intrusion detection systems (IDSs), etc. [40].

3) PHEV (Plug-in Hybrid Electric Vehicle): Many studies [3], [4], [6], [19]–[21] have found that PHEVs, in addition to reducing carbon emissions and reliance on fossil fuels, could also provide a means to support DER in the smart grid. Since most PHEV batteries are designed to speed up rapidly for fast discharge, parked PHEVs can supply electric power to the grid [19]. This vehicle-to-grid concept may improve the efficiency and increase the reliability of the power grid [19]. However, it is still under development and the tradeoff between costs and benefits is still uncertain [2].

4) Communication Protocols and Standards: The communication standards for the power industry were developed by five leading organizations including the IEEE, the IEC (International Electro-technical Commission), and the DNP3 (Distributed Network Protocol) Users Group [37]. The most prevalent protocols for SCADA communication systems are IEC 60870-5 and DNP3 [37]. The IEC protocol is typically used in Europe for communication between MTU and RTUs in SCADA systems [38], [39]. The DNP3, which is derived from IEC 60870-5 and recognized by the IEEE 1379 standard, is widely used in Asia and North America [38], [39]. IEC 61850 has now been released to support more enhanced capabilities including a peer-to-peer communication mode for field devices [39]. It can be regarded as a successor to the DNP3 [29].

IEC 62351 [41] is a standard that specifies security constraints and concerns of the above communication protocols and standards. It consists of eight parts. The first two parts present an introduction to its background and a glossary of terms. Part-3 specifies the security requirements for TCP/IP profiles in IEC 60870 and IEC 61850. In particular, it describes the TLS (Transport Level Security) configuration for secure interactions [29], [38], [41]. Part-4 addresses MMS (Manufacturing Message Specification, ISO 9506) protocol security in the IEC 61850 standard. Specifically, the MMS will work with the TLS to secure communications [38]. Not all components are required to adopt this secure mechanism [38]. Part-5 focuses on the security of serial communication in IEC 60870 and DNP3. It suggests that the TLS (Transport Layer Security) encryption mechanism can be utilized for serial communication to enable confidentiality and integrity [38]. As for the authentication, the serial version can only address replay, spoofing, modification, and some DoS attacks [38]. It cannot prevent eavesdropping, traffic analysis, or repudiation due to its limited computing capability. However, it could be protected by alternate methods, such as VPNs or "bump-in-the-wire" (a scheme that use an IPSec device as a firewall to filter unwanted packages from the Internet) technologies, depending upon the capabilities of the devices and communications involved [38]. Relevant key management measures are also described in this part [29]. Part-6 provides security for non-routable peer-to-peer communications. Since the interval of transmitting messages over SCADA networks is limited to 4 milliseconds (according to the IEC 61850-8-1), general encryption or other security methods are not feasible [38]. Authentication therefore becomes the only option that is used for P2P security [38]. Part-7 and Part-8 are still at draft specification and require further study. The objective of Part-7 is to secure the network and system management (NSM) of the information infrastructure. Two existing technologies will be utilized: the simple network management protocol (SNMP) and the ISO common management information protocol (CMIP) [38]. Part-8 is designed to address authorization problems in control centers. One promising mechanism that is mentioned is role-based access control strategy [29]. There are also some related papers in [68]–[116].

III. Cyber Security Issues on Smart Grid

The traditional power delivery system focuses on developing equipment to improve integrity, availability, and confidentiality. Until recently, contemporary communication technologies and equipment were typically regarded as supporting the power industry's reliability. Nevertheless, increased connectivity is becoming more critical to the cyber security of the power system. In a broad sense, the cyber security of the power industry covers all IT and communications issues that affect the operation of power delivery systems and the management of the utilities [3]. Specifically, securing the power grid prevents, prepares for, protects against, mitigates, responds to, and recovers from unexpected cyber events or natural disasters [3]. Wei *et al.* [30] pointed out that the development of a secure smart grid would encounter the following four challenges:

1) The power delivery system has new communication requirements in terms of protocols, delay, bandwidth, and cost. Avoiding early obsolescence is essential in smart grid security development.
2) Many legacy devices have been used in power automation systems for decades. Most of them only focus on a certain functionality and thus lack sufficient memory space or computational capability to deal with security problems. Integrating the existing legacy equipment into the smart grid without weakening their control performance is a challenge.
3) Networking in the current power grid uses heterogeneous technologies and protocols such as ModBus [50], ModBus+ [50], ProfiBus (Process Field Bus) [51], ICCP (Inter-control Center Communication Protocol), DNP3 [37], etc. Nevertheless, most of them were designed for connectivity without cyber security.
4) Current power systems are usually proprietary systems that provide specific performances and functionalities but not security.

Many organizations are currently involved with the development of smart grid security requirements, including NERC CIP (North American Electrical Reliability Corporation - Critical Infrastructure Protection), ISA (International Society of Automation), NIPP (National Infrastructure Protection Plan), IEEE (1402), and NIST. One prominent set of requirements has been reported by the NIST Cyber Security Coordination Task Group (CSCTG) [3]. After reviewing the NIST CSCTG report [3] and existing research [13]–[15], [17], [21], [22], [24]–[36], [39]–[43], [48], [52]–[67] on cyber security, we

have categorized the relevant issues into five groups (shown in Table II and Table III). Notice that general security problems such as software engineering practices, firewalls, circuit designs, and patch management will not be included in the tables.

A. Device Issues

Devices like PLCs (Programmable Logical Controllers), RTUs, and IEDs are widely deployed in power delivery systems to allow administrators to perform maintenance or to dispatch functionalities from a remote location [30]. This function also enables malicious users to manipulate the device and disrupt normal operations of the grid, such as shutting down running devices to disconnect power services or tampering with sensing data to misguide the decisions of the operators [30]. The authors in [53] discussed such a cyber vulnerability, in which an attacker could switch-off hundreds of millions of smart meters with remote off switches. Although no agreed solutions are proposed in present standards and regulations, some recommended countermeasures in [53] may be considered in further discussions. For the devices, the IEEE 1686-2007 standard has specified security requirements. However, experience shows that typical IEDs are far from complying with this standard. As described in Table II, potential security problems may present in the applications of smart meter, customer interfaces, and PHEVs.

As for the meter device, a conventional physical meter can be modified by reversing the internal usage counter (aka. meter inversion) or be manipulated to control the calculation of the electric flow [14]. Addressing this problem may require hardware support. We will therefore not focus on its solutions in this paper. Besides, data aggregation is generally perceived as a main function for the smart meter. Several algorithms [60], [61] have been proposed to prevent the meter data from being compromised. Authors in [61] analyzed the tradeoff between security and efficiency and designed two algorithms for per-hop and end-to-end communication protocol respectively. They used AES-CCM with 128 bit shared key to encrypt the line between the meter and the gateway, which showed their protocol is reliable and energy efficient (according to their experiment results).

As for the customer interfaces and PHEVs, not too many papers are presented to address potential security problems. Ongoing relevant research mainly focuses on issues of malware attacks and fast encryption. Metke and Ekl [27] proposed some suggestions for malware protection on embedded systems and general purpose computer systems. For embedded systems, manufacturers should take full responsibility for securing software development and upgrade procedures. To meet this requirement, three possible approaches are discussed. First, the manufacturer may issue a public key to each device and encrypt all new software with the corresponding private key. The device can then validate the source of the updated patch and thus secure the system. The second method is called the "high assurance boot" (HAB) method. The embedded system will be validated once it boots up. The validation script is safely coded into its hardware by the manufacturer. Since not all devices can be rebooted very often, secure validation software is considered as the third solution. By using a device attestation technique, devices can be validated while running. When it comes to general purpose computer systems, the authors in [27] argue that current antivirus software cannot prevent the system from suffering malware attacks. Although there is currently no solution, one thing is recommended: all mobile code (e.g., ActiveX, JavaScript, Flash animation, etc.) in the smart grid should be strictly controlled from suppliers to operators.

As we know, tens of millions of sensors or RTUs are deployed in the grid for distributed automation (DA). These devices have limited bandwidth, power (battery or long sleep cycles), storage, memory, and intermittent connections [3]. Because of these constraints, applications like key management should require less centralization and more persistent connectivity than current approaches; it should also retain a certain level of trust and security for the entire infrastructure [3]. NIST requirements [3] suggest that each device has unique key and credential materials such that, if one has been compromised, others will not be affected. Zhang *et al.* [31] proposed a 256-bit AES-based solution to secure the traffic between two smart grid devices in Ethernet networks. AES algorithms have inherent requirements for the smart grid: it must only require a few memory spaces and be able to be used for wireless sensor networks (WSNs). In their design, all data packets in Ethernet networks consist of four fields: one header and three data fields. Specifically, the header contains the destination IP address. All other nodes except the recipient cannot read the data payload and will simply discard it. The data payload includes 3 fields. Each of them is 16 bytes, since AES will only process 16-byte sized data. To indicate whether a message is encrypted or not, the header adds an extra AES_status flag; thus this message may be transmitted through other networks. By using the Altera Cyclone-2 FPGA (Field Programmable Gate Array) based platform, they have successfully implemented their design into the hardware. Experiment results indicate that the data transmission is secure only if no eavesdroppers exist on the Ethernet network and that the throughput (bytes encrypted per second) can be 1,202 bps [31].

B. Networking Issues

Potential security problems of networking in smart grids mainly focus on issues of the Internet, wireless networks, and sensor networks. Just like the Internet, multiple networking technologies can be utilized for the smart grid, including fiber optics, land mobile radio (LMR), 3G/4G (WiMax), RS-232/RS-485 serial links, WiFi, and so on [27]. Which one will be used depends on the requirements of the grid environment and is an open issue in the development of smart grid communication standards.

For wired networks, Sun *et al.* [28] claimed that Ethernet Passive Optical Networks (EPON) would be a promising solution for the smart grid broadband access networks due to the following metrics: 1) backward compatibility, 2) low-cost fiber deployment and maintenance, and 3) minimal protocol overhead. EPON also has been regarded as next-generation Gigabit-Ethernet by IEEE 802.3ah standard. As shown in

TABLE II
CYBER SECURITY ISSUES ON SMART GRID - PART I

Topics	Cyber Security Issues		
	Key Words	*Potential Problems*	*Possible Solutions*
Device	Smart Meter	• Customer tariff varies on individuals, and thus, breaches of the metering database may lead to alternate bills [3] • Meters may suffer physical attacks such as battery change, removal, and modification [3], [30]. • Functions like remote connect/disconnect meters and outage reporting may be used by unwarranted third parties [3], [53].	• Ensure the integrity of meter data. • Secure meter maintenance. • Detect unauthorized changes on meter. • Authorize all accesses to/from AMI networks [3].
	Customer Interface	• Home appliances can interact with service providers or other AMI devices. Once manipulated by malicious intruders, they could be unsafe factors in residential areas [3], [14]. • Energy-related information can be revealed on IEDs or on the Internet. Unwarranted data may misguide users' decisions [3].	• Access control to all customer interfaces. • Validate notified information. • Improve security of hardware and software upgrades [3].
	PHEV	• PHEV can be charged at different locations. Inaccurate billing or unwarranted service will disrupt operations of the market [3].	• Establish electric vehicle standards [3].
Networking	Internet	• Certain applications may be built on the Internet. Inherent problems like malicious malware and denial of service (DoS) attacks are threats to the grid operations [1], [3], [17], [30], [32].	• Adopt TCP/IP for smart grid networks [1], [3]. • VPN (IPSec), SSH, SSL/TLS [17], [40], [67]. • Intrusion detection and firewalls 17,30.
	Wireless Network	• In wireless networks, layer 2/3 can be easily attacked by traffic injection and modification. Without routing security, traffic on these layers is not reliable [3], [17].	• Protect routing protocols in layer 2/3 networks [3]. • Security capabilities in 802.11i, 802.16e, and 3GPP LTE [27].
	Sensor Network	• Sensor data is critical for the grid. Intercepting, tampering, misrepresenting, or forging these data will damage the grid [3], [30].	• AES (Advanced Encryption Standard) encryption [31], [61].
Dispatching & Management	SCADA/ EMS/ DMS	• Distribution control commands and access logs are critical for SCADA systems. Intercepting, tampering, or forging these data damages the grid [3], [30], [39], [54]–[59]. • Synchronizing time-tagged data in wide areas is essential; without it the safety and reliability of the SCADA system cannot be achieved [3], [20]. • Every decision of SCADA comes from the analysis of the raw data based on a reasonable model. Improper models may mislead operator actions [3]. In addition, different vendors using distinct SCADA models will disrupt the consistency of the grid [3], [17]. • Load management of EMS provides both active and passive control by the service provider and customer. Inconsistent agreement on load control may cause unwarranted outages [3]. • The management of DER plants includes load forecasts. False forecast could misguide the decision of the DMS [3].	• Ensure all commands and log files are accurate and secure [3]. • Use a common time reference (GPS time-stamped) for time synchronization [3], [32]. • Customers may sign a contract with their utility company that allows their DER to be used for load support [3]. • Use multi-layer intrusion detection [30].
	Asset Management	• When assets need to be replaced, unplanned outages and the equipment damage could result [3]. • Compatibility problems could emerge while integrating legacy devices into the grid, which may cause the system to fail or malfunction [1], [3].	• Maximize the life-cyle of assets through cooperation among relevant operators [3]. • Back-up data mart [3]. • Enabling backwards compatibility [3].
	Cipher Key Management	• Data encryption and digital signatures are required in sensors to secure communications. Most of existing cryptographic scheme lack of efficiency under limited space and computation [3]. • Access and communication may occur across different domains [43]. To manage their own credential keys in different areas is difficult, especially in a national wide scenario [3]. • Device or system may be "locked out" when an emergency occurs [3].	• PKI (Public Key Infrastructure) [17], [27]. • IBE(Identity-Based Encryption) [43]. • Hierarchical, decentralized, and delegated schemes and their hybridization [3]. • Design a bypass or "cold boot" means for emergency while remaining secure in daily operations [3].
	Real-time Operation	• Some applications (e.g., real-time process) must meet limited time constraints. Increasing interoperability may cause unbounded and uncontrollable delays of the power system [3], [30].	• Minimize and make predictable timing impacts of security protections [3].

TABLE III
CYBER SECURITY ISSUES ON SMART GRID - PART II

Topics	Cyber Security Issues		
	Key Words	***Potential Problems***	***Possible Solutions***
Anomaly Detection	Temporal Information	• Unsecured time information may be used for replay attacks and revoked access, which has a significant impact on many security protocols [3], [36]. • Timestamps in event logs may be tampered by malicious people. [3].	• Use phasor measurement units (PMUs) to ensure accurate time information [3]. • Adopt existing forensic technologies to ensure temporal logs are accurate [3].
	Data & Service	• RTUs may be damaged in various ways. The accuracy of transmitted data and the quality of services therefore can not be guaranteed [33].	• Utilize fraud detection algorithms and models used in credit card transaction monitoring [3].
Others	Demand Response	• Tampering with information of real time pricing (RTP) may cause financial and legal problems [3], [25], [30], [59]. • Malware may infect the grid, indicating false trend of supply and demand. This causes substantial damage to the power delivery system [27], [32], [48].	• Deploying trusted computing platforms [27].
	Protocols & Standards	• Existing protocols may have some inherent security flaws [30], [32].	• More secure standards for automation and communication must be developed [29].

Fig. 4, a tree-based EPON will broadcast messages to every ONU (Optical Network Unit), all of which share one common channel over which to deliver data to an OLT (Optical Line Termination). In this case, every ONU is able to capture all downstream traffic from the OLT and will vie with other ONUs for limited upload bandwidth. Therefore, EPON can be easily attacked by methods such as spoofing, DoS, and eavesdropping. By using identity-based cryptography (IBC) and challenge-response technology, the authors then proposed a secure communication protocol for the EPON. Unlike traditional asymmetric cryptographic approaches (e.g., PKI), the IBC generates a public key by using an arbitrary data string, and the corresponding private key binds this information, which is signed by a trusted key distribution center (KDC) [28]. In their scheme, the OLT and ONUs will periodically perform mutual authentication. First, the OLT challenges an ONU, i, with a message, n, encrypted with i's public key. After verifying this message, i will respond with n and a random number m encrypted with OLT's public key. Upon getting this response message, the OLT can verify the identity of i. Finally, the OLT will send m back to i. Thus, i is able to verify the authority of the OLT. This mechanism establishes a secure channel between two devices. In fact, it is also adopted by the DNP standard for secure communication (e.g., challenge-response mode and aggressive mode) [39]. However, the authors did not give a simulation or an experiment to evaluate its performance in terms of time delay, package overhead, scalability, etc. Moreover, they had not discussed how to setup a KDC but rather assumed one existed.

For wireless networks, airborne radio waves would be potential vulnerabilities to adversaries. In particular, such an unprotected physical medium may disclose neighboring energy consumption data and thus cause a privacy invasion. The NIST report [3] claimed that schemes like 802.11i would help to secure smart grid wireless deployment. Moreover,

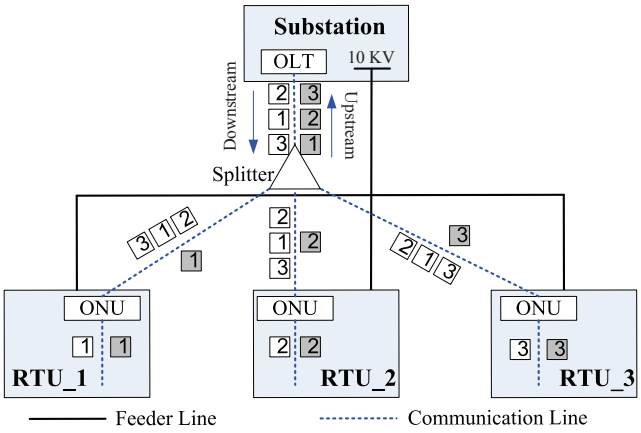


Fig. 4. Typical tree-based EPON system for the power grid [28]

Metke and Ekl [27] argued that wireless smart grids could be further secured with existing standards like 802.16e (Mobile WiMax) and 3GPP LTE. Possible technologies for wireless security include, but are not limited to: mutual or server EAP (Extensible Authentication Protocol), 4-way handshake, AES-CCMP (AES-Counter Mode CBC-MAC Protocol), CBC-MAC (Cipher Block Chaining Message Authentication Code), 128 group encryption key, 3DES (Triple Data Encryption Standard), PKMv2 (Privacy and Key Management version 2) RSA acknowledgement message, and mutual authentication between UE (User Equipment) and MME (Mobility Management Entity) [27]. But, the authors did not give analysis of their feasibility in the smart grid.

For sensor networks, to date, researchers [3], [27], [36] have reached the unanimous consensus that wireless mesh networks should be deployed in the AMI. A primary reason for this is that mesh networks can overcome bad links by using redundant communication paths [21]. Nevertheless, the

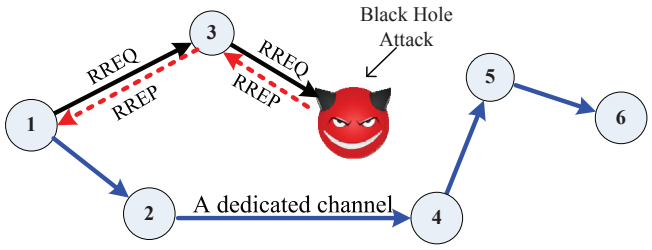


Fig. 5. Black hole attack against AODV routing protocol

IT industry has witnessed a series of attacks against wireless mesh technologies such as cross-layer traffic injection, node impersonation, route injection, message modification, etc. [3]. Most existing routing protocols lack specific strategies to secure the paths and the data mainly because of their inherent distribution features [3]. Without routing security, traffic in the AMI is not reliable. Hence, Zigbee Alliance released a standard to address this problem based on Zigbee Pro and 802.15.4 standards [36]. Bennett and Wicker [36], however, argued that the conventional Zigbee protocol would suffer from severe delays due to the multi-tier feature of the cluster-tree based routing strategy. Specifically, if a meter polled 11,250 bytes of data (88 packets) every 15 minutes under 802.15.4 context with a maximum data rate of 250 kbps, then the meter only had 4 milliseconds to deliver a packet, which would become even shorter when sending additional control messages or retransmission. To speed up the transfer rate, the authors suggested adding a new layer between layers 2 and 3 of Zigbee networks. This layer would use a modified multi-protocol label switching (MPLS) layer 2.5 protocol to decrease end-to-end delays. In addition, they suggested that the routing protocol in Zigbee networks should be pure AODV (Ad Hoc On Demand Distance Vector), which could significantly shorten the time required to establish a path. Through an in-depth study of the AODV protocol, the authors also found that this routing mechanism would easily suffer from "black hole" attacks [36] that discard path establishing messages. To address this problem, they proposed the solution of establishing a dedicated path between the two communication principals (as shown in Fig. 5). Simulation results in [36] indicated that these recommendations could improve the network throughput enough to meet the meter reading requirements.

C. Dispatching and Management Issues

Smart grid can be regarded as a combination of several micro grids [11]. Each micro grid operates autonomously within its local SCADA system and interacts with others like "Island Functionality" or "Islanding." Meanwhile, all micro grids will be controlled by a central master SCADA system in which every local SCADA acts as a slave controller providing energy related information to the central controller. This framework ensures reliability of the smart grid and thus has been approved by the IEEE-1547 standard. Traditionally, those SCADA systems are isolated and controlled by authorized personnel. Most of them lack real-time control and monitoring capabilities [32]. Until recently, GPS time-stamped (in milliseconds) phasor measurement units (PMUs) offered a solution to this problem. To address the clock synchronization problem in the distributed context, the NTP (Network Time Protocol) and the IEEE 1588 standard are used in the current SCADA system [40]. This increased interoperability, however, makes them more accessible to public users, which inevitably increases the risk of the system being compromised as follows:

1) *Take down the server*: If the IP of the SCADA server and the network path are known to the attacker, the server can be easily taken down or shutdown by the traditional denial of service errors or by simply deleting the system files. Denial of service can be done if the TCP/IP can be flooded. Deleting the files can be done by hacking the user passwords or gaining access to the physical system. These attacks can cause a major danger to future services as well.
2) *Gaining control over the system*: This is achieved by planting a Trojan or by backdoor entry into the system registries. This is the highest scale of security threat, by which a false alarm and manipulated controls can be generated and sent to RTUs causing large scale collapses.
3) *Stealing corporate data*: These problems occur if the enterprise security level is poor and the software architecture used is not highly capable. The corporate data can be stolen from the database for the internal rivalry between the competing service providers.
4) *Fiddling with billing information*: The intruders might be able to access the billing and other financial information from the system to get the details, which can later be misused and can cause major problems to the consumers. There needs to be a powerful firewall to protect the servers from losing this information.
5) *Key logger software*: Attackers generally tend to use the logged key strokes of the system keyboard and gain access to the system passwords and usernames.
6) *Gain competitive advantage*: Attackers from one service provider generally tend to access the data of the others to get to know their strategies and thus orient their planning in a way that they would eventually benefit in a competitive environment.
7) Misuse the SCADA servers to attack the other servers in the system and gain access information to the valuable information from the utility companies.
8) Manipulate mathematical data points to off track the utility operators, who then tend to detect a false alarm and tend to shutdown or rescale the system causing unnecessary latencies.
9) Change user logged data in a distant and remote DBMS; this can affect the innocent users as well as the utility companies.

For example, an attacker can attack the power grid by attacking the energy management system (EMS) [58] via faking meter data and misleading EMS by the state estimator to make bad decisions. Papers [54]–[59] studied stealthy false-data attacks against state estimators located in control centers in power systems. The authors in [54] first studied the attack, and authors in [55]–[57] further extend their work. In [56], quantified security metrics are adopted to measure the

difficulty of conducting a stealth attack against measurements. In [55], encryption was used to protect a state estimator from attacks. In [57], a security index was presented based on [56] and a protection scheme was proposed to further encrypt measurements to achieve maximizing their utility in terms of increased system security. The authors in [58] adopted a graph theoretic approach to detect and localize attacks of state estimations. For those unobservable data attacks (i.e. meter access restriction), a polynomial-time complexity algorithm is presented to find a minimum size of compromised meters that is required. In [59], effects on the electricity market caused by the attack are discussed. From an economic view, the authors point out that such attack can manipulate the nodal price of Ex-Post market, which may bring financial profit to the attacker. However, no relevant countermeasure is presented.

The authors in [52] proposed a multilevel framework for a trust model for smart grids with distributive control systems, and the scheme migrates against widespread failures when control system components themselves are compromised. However, no kind of simulation, prototyping, and implementation was done yet.

In order to limit the access right only to authorized personnel, Cheung *et al.* [24] have proposed a smart grid role-based access control (SRAC) strategy. In this strategy, each micro grid is divided into several sub-domains according to its functionalities and energy resources. The local SCADA system acts as a gateway to authorize access privileges to both local and foreign domain users with predefined security policies and role constraints. In the SRAC model, a user may be assigned several roles with different authorities and functions across the grids. A role could share its responsibilities with other roles. The role hierarchy can be organized and stored as a tree structure, in which the "parent" role directly inherits all the privileges of its "children" roles. A corresponding XML (Extensible Markup Language)-based security policy has been developed to simplify SRAC security management. Nevertheless, the authors have not clarified the details of the SRAC administration and authentication procedures in [24]. To achieve this goal, Hamlyn *et al.* [26] proposed the following constructive suggestions for the SRAC implementation: 1) use state-of-the-art digital credential technologies to verify all access requests; 2) check the reliability and trustworthiness of each request before issuing any certificate to the user.

For the above two suggestions, a flexible, robust, and efficient key management strategy is required. Years of research on securing IT communication systems tell us that deploying symmetric keys into a large number of devices can be expensive and unreliable [27]. Contemporary trust management technologies should be customized specifically for the smart grid communication system [27]. Metke and Ekl [27] believe that PKI technology is the best key management solution for the smart grid. In the current power grid, four relevant technical factors are discussed for PKI implementation: 1) PKI standards, 2) automated trust anchor (TA) security, 3) certificate attributes, and 4) smart grid PKI tools [27]. First of all, establishing a set of smart grid PKI standards is critical for device manufacturers and power service providers. Those standards should specify the security policies, PKI practices, and certificate formats. Second, they should ensure that each smart grid device has correct TA information [27]. One possible approach is to use a factory preload certificate. Every time they install a new device, the smart grid operator will authenticate it with a root certificate by using the manufacturer's TA transfer tool. Then the device's TA information will be securely stored in a local policy database. Third, certificate attributes should not involve the participation of security severs because of their unreachable situation. Thus, local policy attributes and local certificate statuses are required. Finally, they must build relevant smart grid PKI tools to ease the management of PKI components [27]. This process can be accomplished by modifying existing PKI operation tools.

A good example to deploy PKI technology into the smart grid is proposed by Hayden *et al.* [43]. By using an identity-based cryptograph (IBC) method, they addressed the confidentiality and authenticity issues in an AMI communication network. Based on their implementation results, they argued that this design did not require a complex setup procedure and was scalable in terms of small packet overhead (128 bytes). However, this mechanism requires a central key-generating server to distribute a private key for a certain device or a user. Thus, key management is still an issue for regional and national wide deployment.

D. Anomaly Detection Issues

Reliable operations of the smart grid require accurate and timely detection for anomalous and outliers events [3]. Ways of detecting and coping with errors and faults in the power grid need to be reviewed and studied in a model that includes systematic malicious manipulation [3].

To meet the criteria for automated fault analysis in the smart grid, several studies were undertaken [34], [35], many of which are still on-going. These include 1) a concept for detecting, classifying, and mitigating cascading events based on local and system-wide monitoring data; 2) implementing an optimal fault location algorithm that uses data from substation IEDs, as well as data from the SCADA PI Historian and simulation data from short circuit programs; 3) developing a risk-based asset management methodology for maintenance scheduling that takes into account condition-based data captured by substation IEDs; 4) proposing an intelligent alarm processor approach to take advantage of enhanced protective relay data in explaining cause-effect relationships between alarms; 5) a neural network based protective relaying scheme that enables simultaneous enhancements in dependability and security of transmission line protection.

Pang *et al.* [33] proposed a multi-agent based fault location algorithm for the smart grid. In their model, every smart distribution unit is regarded as an agent, and all agents construct a multi-agent system. There are three types of agents: node agent, control agent, and database agent. The node agent is typically bounded with an IED that locates at a feeder node of a smart grid. It can collect transient zero voltage and current signals and calculate the transient reactive power in selected frequency bands (SFB). This calculation result will be shared among different neighboring node agents. According to the transient reactive power of this node and the transient reactive power of the neighbor node, the node agent can judge

whether the feeder section concluding this node is faulty or not. The control agent is located at the control centre of a smart grid. It can receive the fault information from node agents and send the control command to node agents and trigger the alarm device when a fault occurs. Meanwhile, it can manage fault data in database agent to print, display the fault data, and so on. The database agent is responsible for storing fault data and the control command [33]. When one feeder is fault, every agent obtains transient zero voltage and current and computes transient zero reactive power in special frequency bands. Through communication and collaboration among agents, all fault information is shared. According to comparing amplitude and direction of transient zero reactive power between neighbor nodes, the fault section is located.

In [63], the authors explored the threats model and constraints of the AMI and then analyzed the requirements for host intrusion detection design. They claimed that the best IDS choice for AMI is specification-based detection, which is defined as "identifying deviations from a correct behavior profile predefined using logical specifications." The paper only gives a guideline for architectural design. More intensive study is required to complete this work.

E. Other Issues

Virtually all modern data communication protocols adhere to a messaging protocol that is well documented and available in the public domain. The DNP protocol is widely used by electric utilities throughout North America. The DNP protocol specification can be attained for a nominal user fee. Using these documented protocols allows an intruder to do reverse engineering of the data acquisition protocol and exploit the protocol using a "Man-in-the-middle" attack. The adverse effects could include sending misleading data to the field device or control center operator resulting in 1) financial loss if the attack leads to excess generation output; 2) physical danger if a line is energized while linemen are in the field servicing the line; 3) equipment damage if control commands sent to the field result in overload conditions [30].

Another issue involves information communication standards. IEC 61850 is a popular standard that specifies interoperability technologies and data formats for communication in the domain of power automation [29]. Authors in [67] proposed a prototype multicast system SecureSCL (Secure Substation Configuration Language) to handle publish-subscribe relationships in IEC 61850 power substation networks. It is a cross-layer design that secures the inter-substation communications by using IPsec multicast. Besides, the authors also developed a tool to detect multicast configuration anomalies. Preliminary experiment results show that their work can meet the latency requirement of power substations.

IEC 62351 is a support standard for IEC 61850 that particularly focuses on security and technical requirements of vendors. Fries *et al.* [29] gave an overview of both documents and pointed out that IEC 62351 should be updated due to some new use cases in the smart grid. Those use cases are mainly derived from customer participation and demand response in the grid. According to the results of the IEC 62351, the authors argued that the MMS and XML should be further improved to ensure the integrity of the application layer. As depicted in Fig. 6, when a central command is forwarded by an intermediate substation, the current MMS version in IEC 62351 is unable to ensure its integrity in the application layer. To address this problem, the authors proposed a possible solution by adding a "cryptotoken" to the command packet. First, it establishes a TLS connection on every hop with corresponding session keys on the transport level. Second, it establishes an end-to-end communication channel on the application level and negotiates the session key during the handshake phase. Third, it uses this session key to secure all subsequent traffic. Through these steps, integrity in the application layer is achieved.

IV. Privacy Issues on Smart Grid

Intelligent control and economic management of energy consumption require more interoperability between consumers and service providers. Unprotected energy-related data will cause invasions of privacy in the smart grid. In particular, radio waves in AMI may disclose information about where people were and when and what they were doing [23]. Failure to address privacy issues in the smart grid will not be accepted by regulators and customers. In this section, we will give a brief overview of current studies on privacy issues in the smart grid.

A. Personal Information

Personal information is any recorded information that can identify an individual directly or indirectly [3], [12]. Besides one's name, biographical, and contact information, it may also involve personal choices, social activities, health problem, or any economic, physical, or mental information derived from the above, and information about other relatives [12]. Considering in the smart grid context, any type of energy use data that links to personal information should be secured and monitored in a proper way. NIST guidelines [3] have provided a list of personal information that may be available through the smart grid as follows:

1) *Name*: responsible for the account.
2) *Address*: location to which service is being taken.
3) *Account Number*: unique identifier for the account.
4) *Meter Reading*: kW, kWh consumption recorded at 15-60 minute intervals during the current billing cycle.
5) *Current Bill*: current amount due on the account.
6) *Billing History*: past meter readings and bills, including history of late payments/failure to pay, if any.
7) *HAN*: in-home electrical appliances.
8) *Lifestyle*: when the home is occupied and it is unoccupied, when occupants are awake and when they are asleep, how many various appliances are used, etc.
9) *DER*: the presence of on-site generation and/or storage devices, operational status, net supply to or consumption from the grid, usage patterns.
10) *Meter IP*: the IP address for the meter, if applicable.
11) *Service Provider*: identity of the party supplying this account, relevant only in retail access markets.

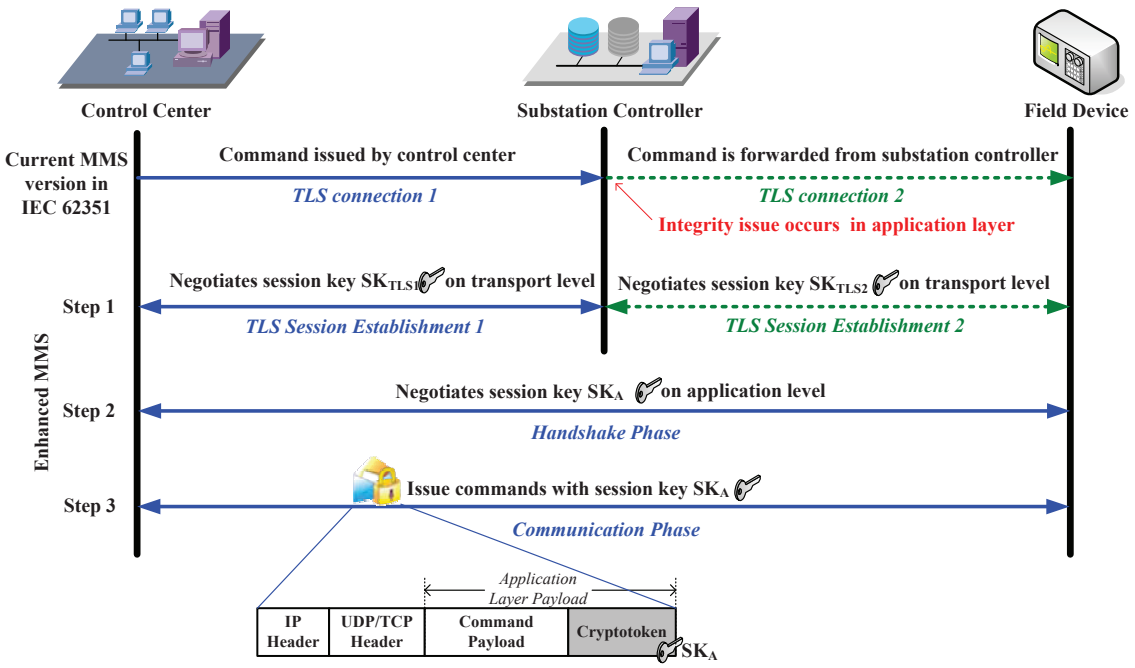


Fig. 6. Enhanced MMS protocol in IEC 62351 [29]

B. Privacy Concerns

In the context of the smart grid, energy consumption data obtained by a third party may disclose personal information without one's permission. Besides establishing corresponding laws and regulations to protect personal information in the smart grid, we also require a secure mechanism to prevent privacy violation from breaching local data and remote copies. According to the study of NIST [3], four typical areas of privacy concern in the smart grid are presented as follows:

First of all, fraud should be considered, especially when energy consumption is attributed to a different location (e.g., in PHEVs' case) [3]. The metering system (either physical recording or electronically and remotely metering systems) should not allow any personnel abuse or modify the collected data [3]. In particular, NIST's report [3] has analyzed two relevant privacy use cases in detail. One case is about a landlord with tenants who have PHEVs that require being charged separately. For the purpose of preserving the privacy of the tenants, utility is involved to authenticate communications between the smart meter and PHEVs through a secure line and energy services communication interface (ESCI) provided by the utility and/or vehicle manufacturer. Another case is regarding PHEV general registration and enrollment process. In order to complete initial setup for PHEVs, NIST believes that utilities should offer the following services to customers: 1) enrollment, 2) registration, 3) initial connection, 4) ability to repeatedly re-establish connection between a utility and PHEV, 5) ability to provide a PHEV tariff or charging status information to customer interfaces, and 6) correct bill.

Second, data in the smart meter and HAN could reveal certain activities of home smart appliances [3]. In addition, it is can be used for tracking specific times and locations of energy consumption in specific areas of the home, which may further indicate the appliances used and/or types of activities. For example, appliance vendors may want this kind of data to know both how and why individuals used their products in certain ways. Such information therefore could impact appliance warranties. Meanwhile, other entities may need this data to conduct target marketing. Georgios *et al.* [44] designed a system that utilized a power router and a rechargeable battery to hide or obscure load signatures in a home area. In this system, they assume that the home will have several energy storage and generation devices in the future. Through a power router, appliance load signature or usage pattern will be moderated and thus cannot be recognized and tracked by a malicious intruder. They have further improved this model in [65] and named it as ElecPrivacy. Besides, a number of privacy measurement approaches are provided for this model in [65].

Third, obtaining near-real-time data regarding energy consumption may infer whether a residence or facility is occupied, where people are in the structure, what they are doing, and so on [3]. Authors in [60] proposed a data aggregation approach for all level meters based on spanning tree topology. By using homomorphic encryption method, data is secured all the way from home meters to the data center. It can well protect the privacy of the individual power usage according to their analysis and evaluation in [66]. In [62], researchers pointed out that customers would possibly deploy a separate measurement device at home to better monitor their power usage. The redundant meter data, if transmitted in an unsecured wireless line, could leak customer's information to an eavesdropper. By compressing the data to a rate below its entropy, the authors in [62] proposed a coding method that well addressed this problem.

Fourth, personal lifestyle information derived from energy use data could be valuable to some vendors or parties [3]. For instance, vendors may use this information for targeted

marketing, which could not be welcomed by those targets. The beneficial information may be revealed by new technologies like smart meters, time of use and demand rates, and direct load control of equipment. They could be further sold and used for energy management analysis and peer comparisons. Costas *et al.* [45] proposed an escrow-based anonymization scheme to prevent personal information from being tracked by unauthorized third parties. They categorized metering data into two parts: "high-frequency" and "low-frequency." Then corresponding setup and communication procedures were designed for each type of data. Those procedures are both regular PKI authentication approaches. Since the anonymity degree of the system depends on the size of the "anonymity set," to widely deploy such a scheme requires a further investigation.

In addition, two aspects of the Smart Grid data need to be considered in the review of existing laws and regulatory policies to ensure that new types of data are addressed [3]: 1) granular and available data on use of individual appliances by time and location; 2) public awareness of contractual agreements about data ownership and what may be revealed about people's daily activities.

C. Recommendations

NIST has delivered a report [3] on the consumer-to-utility privacy impact assessment (PIA) of the smart grid. Ten potential design principles are proposed to address privacy issues in the smart grid:

1) An organization should ensure that information security and privacy policies and practices exist and are documented and followed. Audit functions should be present to monitor all data accesses and modifications.
2) Before collecting and sharing personal information and energy use data, a clearly-specified notice should be announced.
3) Available choices should be presented to all users. Organizations need to obtain users' consent or implied consent if it is not feasible, with respect to the collection, use, and disclosure of their personal information.
4) Only personal information that is required to fulfill the stated purpose should be collected from individuals. Treatment of the information should conform to these privacy principles.
5) Information should only be used or disclosed for the purpose for which it was collected and should only be divulged to those parties authorized to receive it. Personal information should be aggregated or anonymized wherever possible to limit the potential for computer matching of records. Personal information should only be kept as long as is necessary to fulfill the purposes for which it was collected.
6) The organization should allow individuals to check their corresponding personal information and to request the correction of perceived inaccuracies. Personal information data subjects should be notified about parties with whom personal information has been shared.
7) Personal information should be used only for the purposes for which it was collected. Personal information should not be disclosed to any other parties except for those identified in the notice, or with the explicit consent of the service recipient.
8) Personal information in all forms, should be protected from unauthorized modification, copying, disclosure, access, use, loss, or theft.
9) Organizations should ensure the data usage information is complete, accurate, and relevant for the purposes identified in the notice.
10) Privacy policies should be made available to service recipients. These service recipients should be given the ability and process to challenge an organization's compliance with their state privacy regulations and organizational privacy policies as well as their actual privacy practices.

Cavoukian *et al.* [12] presented the conceptual model "SmartPrivacy" to prevent potential invasions of privacy while ensuring full functionality of the smart grid. Specifically, in the case of utilities providing personal information to a third party with the express consent of an individual, the following are examples of SmartPrivacy defaults that offer greater protection of privacy:

- The information provided to third parties should be minimized such that it only fulfills the purpose of relevant services. For example, partial location data (e.g., the first few digits of a zip code) may be sufficient for services that allow for comparison of neighborhood averages and other features such as weather statistics.
- When data is transmitted, the risk of interception arises. Appropriate and secure channels of transmission between different communication protocols are required to ensure strong privacy protection in the smart grid.
- Anonymize identity if possible. When sharing data with a third party, consider using a pseudonym such as a unique number that the individual would be permitted to reset at any time.
- Third parties should not request information from the utility about consumers, or consumers must be able to maintain control over the type of information that is disclosed to third parties by the utility.
- Third parties should agree not to correlate data with data obtained from other sources or the individual, without the consent of the individual.

V. Future Research Directions

Generally speaking, three areas should be further studied to enhance the security level of the grid: 1) integrity and confidentiality of the transmitted data, 2) building a robust and efficient dispatching and management model for SCADA system, and 3) establishing a universal policy and standard for secure communication technology. We also have examined privacy concerns in the smart grid. To eliminate personal information leakage problems, we believe that state-of-the-art techniques like anonymity, access control, and accountability might provide their solutions. Possible future research directions may include following subsections.

A. Control System Security

Industrial control normally does not do too much about security. In recent years, people pay some attention to control

systems security to protect power generation, transmission and distribution. Co-designs of control and security in smart grids will be interesting topics in the future.

B. Power System Security

Besides cyber security, vulnerabilities in physical power grid should also be further explored and studied. Since new devices will be largely deployed, no one can guarantee the power line itself is 100% secure. Standards and regulations for those new components and their compatibilities need to be modified accordingly. Authors in [64] give us a good example. They proposed a graph-based model that combined both cyber and electrical grid. It can be used for analyzing the cause-effect relations on cyber attacks. Before it applies to a large-scale power grid, more work is still required.

C. Accountability

As we know, advanced cyber security technologies may well protect every level of the current network infrastructure. However, new vulnerabilities and risks continue to emerge under the particular framework of the smart grid. As a complement, accountability is required to further secure the smart grid in terms of privacy, integrity, and confidentiality. Even if a security issue presents itself, the built-in accountability mechanism will determine who is responsible for it. Once detected, some problems can be fixed automatically through the predefined program, while others may provide valuable information to experts for evaluation.

Generally speaking, accountability means that the system is recordable and traceable; this makes the system liable to those communication principles for their actions. Every single change in a local host or network traffic, which may be the most important or most desirable information, can be used as evidence in future judgment. Under such a circumstance, no one can deny their actions, not even the administrators or other users with high privileges. Together with some suitable punishments or laws in the real world, this will prevent many attacks.

One case study for the accountability is the monthly electricity bill of every homeowner. Albeit the real-time, or day-to-day, cost of electricity could be determined by the smart meter, we still doubt its reliability. The utility or the smart meter itself may alter transmitted data to suit someone's interests or for some other reasons (e.g., because they are under attack). As a consequence, homeowners could have two different electric bills: one from the utility and one from the smart meter. We have proposed an approach to address this issue in [49]. With accountability, the false party can be detected by provable evidences. To extend the accountability concept to the whole gird, area, regional and nationwide power management systems should be involved.

D. Integrity and Confidentiality

Integrity and confidentiality are two main aspects for computer and network security design. Naturally, they are still essential for securing the smart grids. For example, integrating with huge numbers of DERs may incorporate with distributed database management system and cloud computing technologies. Whether or not we could adopt current solutions to provide integrity and confidentiality for smart grid is indeed a future research direction.

E. Privacy

Privacy issues in cyber security may be addressed by adopting newly anonymous communication technologies. Current approaches to anonymize traffic in general networks will cause overhead problems or delay issues. For some time-critical operations, limited bandwidth and less connectivity features in the smart grid may hinder the implementation of anonymity. Some pilot works are presented in [44] and [45]. In addition, network traffic camouflage technique could be considered to hide critical entity (e.g., database or control center) in the grid.

VI. Conclusion

This paper mainly gives an overview of cyber security and privacy issues in the smart grid. According to existing research, we may conclude that almost every aspect related to IT technology in the smart grid has potential vulnerabilities due to inherent security risks in the general IT environment. The paper also provides future research directions.

Cyber security and privacy issues in the smart grid are new areas in the fields of power industry, electrical engineering, and computer science. More in-depth research is required to develop such a promising power grid in the near future.

Acknowledgment

This work was also supported in part by the National Science Foundation (NSF) under grants CCF-0829827, CNS-0716211, CNS-0737325, and CNS-1059265.

Prof. Liang's work is supported in part by the National High Technology Research and Development Program of China (863 plan) under 2011AA040101, the National Fundamental Research 973 Program of China under 2010CB334705, the Natural Science Foundation of China under 61174026, 60725312 and the Knowledge Innovative Program of The Chinese Academy of Sciences under KGCX2-EW-104-2.

Prof. Chen's work is supported in part by The National Fundamental Research 973 Program of China under Grant 2011CB302801 and Macau Science and Technology Development Fund grant number 008/2010/A1.

References

[1] Cisco Systems, Inc., "Internet protocol architecture for the smart grid," White Paper, Jul. 2009, available at: http://www.cisco.com/web/strategy/docs/energy/CISCO_IP_INTEROP_STDS_PPR_TO_NIST_WP.pdf.

[2] U.S. DOE, "Smart grid system report," White Paper, Jul. 2009, available at: http://www.oe.energy.gov/SGSRMain_090707_lowres.pdf.

[3] U.S. NIST, "Guidelines for smart grid cyber security (vol. 1 to 3)," NIST IR-7628, Aug. 2010, available at: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

[4] U.S. NIST, "NIST framework and roadmap for smart grid interoperability standards, release 1.0," NIST Special Publication 1108, Jan. 2010, available at: http://www.smartgrid.gov/standards/roadmap.

[5] U.S. NETL, "Advanced metering infrastructure," White Paper, Feb. 2008, available at: http://www.smartgrid.gov/white_papers.

[6] U.S. NETL, "A systems view of the modern grid," White Paper, Jan. 2007, available at: http://www.smartgrid.gov/white_papers.

[7] A. Clark and C.J. Pavlovski, "Wireless networks for the smart energy grid: application aware networks," in: Proc. International MultiConference of Engineers and Computer Scientists 2010 Vol II (IMECS 2010), Hong Kong, Mar. 2010.

[8] J. Gadze, "Control-aware wireless sensor network platform for the smart electric grid," IJCSNS International Journal of Computer Science and Network Security, vol. 9, no. 1, Jan. 2009, pp. 16-26.

[9] D. Dvian and H. Johal, "A smart grid for improving system reliability and asset utilization," CES/IEEE 5th International Power Electronics and Motion Control Conference, Shanghai, China, Aug. 2006, pp. 1-7.

[10] G.N. Srinivasa Prasanna, A. Lakshmi, S. Sumanth, V. Simha, J. Bapat, and G. Koomullil, "Data communication over the smart grid," in: IEEE International Symposium on Power Line Communications and Its Applications (ISPLC 2009), Dresden, 2009, pp. 273-279.

[11] H. A. Khan, Z. Xu, H. Iu, and V. Sreeram, "Review of technologies and implementation strategies in the area of smart grid," in: The 10th Postgraduate Electrical Engineering and Computing Symposium, IEEE WA Section, Perth, Australia, Oct. 2009.

[12] A. Cavoukian, J. Polonetsky, and C. Wolf, "SmartPrivacy for the smart grid: embedding privacy into the design of electricity conservation," Identity in the Information Society, Springer Netherlands, ISSN: 1876-0678, Apr. 2010.

[13] S. Spoonamore and R.L. Krutz, "Smart grid and cyber challenges - national security risks and concerns," March 2009, avaliable online: http://www.whitehouse.gov/files/documents/cyber/.

[14] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," IEEE Security and Privacy, vol. 7, no. 3, May/Jun. 2009, pp. 75-77.

[15] 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), Nov. 2008, available at: http://www.inl.gov/scada/publications.

[16] C. Wei, "A conceptual framework for smart grid," in: Power and Energy Engineering Conference (APPEEC 2010), Chengdu, China, Mar. 2010, pp. 1-4.

[17] A.R. Metke and R.L. Ekl, "Smart grid security technology," in: Innovative Smart Grid Technologies (ISGT 2010), Gaihersburg, MD, Jan. 2010, pp. 1-7.

[18] W.Y. Chu and Dennis J.H. Lin, "Communication strategies in enabling smart grid development," in: The 8th International Conference on Advances in Power System Control, Operation and Management (APSCOM 2009), Hong Kong, China, Nov. 2009, pp. 1-6.

[19] W. Shireen and S. Patel, "Plug-in hybrid electric vehicles in the smart grid environment," in: 2010 IEEE PES Transmission and Distribution Conference and Expositoin, New Orleans, LA, Apr. 2010, pp. 1-4.

[20] K. Moslehi and R. Kumar, "A reliability perspective of the smart grid," IEEE Trans. Smart Grid, vol. 1, no. 1, Jun. 2010, pp. 57-64.

[21] W.F. Boyer and S.A. McBride, "Study of security attributes of smart grid systems - current cyber security issues," Idaho National Laboratory Technical Report (INL/EXT-09-15500), Apr. 2009, available at: http://www.inl.gov/scada/publications.

[22] G.N. Ericsson, "Cyber security and power system communication - essential parts of a smart grid infrastructure," IEEE Trans. Power Delivery, vol. 25, no. 3, Jul. 2010, pp. 1501-1507.

[23] 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: Proc. 1st International Conference on Energy-Efficient Computing and Networking, Passau, Germany, Apr. 2010, pp. 115-118.

[24] H. Cheung, A. Hamlyn, T. Mander, C. Yang, and R. Cheung, "Strategy and role-based model of security access control for smart grids computer networks," 2007 IEEE Canada Electrical Power Conference (EPC 2007), Montreal, Canada, Oct. 2007, pp. 423-428.

[25] P. Vytelingum, S.D. Ramchurn, T.D. Voice, A. Rogers, and N.R. Jennings, "Trading agents for the smart electricity grid," in: The Ninth International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2010), Toronto, Canada, May 2010, pp. 897-904.

[26] A. Hamlyn, H. Cheung, T. Mander, L. Wang, C. Yang, and R. Cheung, "Computer network security management and authentication of smart grids operations," 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, Jul. 2008, pp.1-7.

[27] A.R. Metke and R.L. Ekl, "Security technology for smart grid networks," IEEE Trans. Smart Grid, vol. 1, no. 1, Jun. 2010, pp. 99-107.

[28] Z. Sun, S. Huo, Y. Ma, and F. Sun, "Security mechanism for smart distribution grid using ethernet passive optical network," in: The 2nd International Conference on Advanced Computer Control (ICACC 2010), vol. 3, Shenyang, China, Mar. 2010, pp. 246-250.

[29] S. Fries, H.J. Hof, and M. Seewald, "Enhancing IEC 62351 to improve security for energy automation in smart grid environments," in: The 5th International Conference on Internet and Web Applications and Services (ICIW 2010), Barcelona, Spain, May 2010, pp. 135-142.

[30] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An integrated security system of protecting smart grid against cyber attacks," in: Innovative Smart Grid Technologies (ISGT 2010), Gaithersburg, MD, Jan. 2010, pp. 1-7.

[31] P. Zhang, O. Elkeelany, L. McDaniel, "An implementation of secured smart grid ethernet communications using AES," in: Proceedings of the IEEE SoutheastCon (SoutheastCon 2010), Concord, NC, Mar. 2010, pp. 394-397.

[32] V. Li, F.F. Wu, and J. Zhong, "Communication requirements for risk-limiting dispatch in smart grid," in: IEEE International Conference on Communications Workshops (ICC 2010), Capetown, May 2010, pp. 1-5.

[33] Q. Pang, H. Gao, and M. Xiang, "Multi-agent based fault location algorithm for smart distribution grid," in: The 10th IET International Conference on Development in Power System Protection (DPSP 2010), Manchester, Apr. 2010, pp. 1-5.

[34] Y. Cai and M. Chow, "Exploratory analysis of massive data for distribution fault diagnosis in smart grids," in: IEEE Power & Energy Society General Meeting (PES '09), Calgary, AB, Jul. 2009, pp. 1-6.

[35] M. Kezunovic, "Automated fault analysis in a smart grid," in: IEEE Asia and Pacific Transmission & Distribution Conference & Exposition, Seoul, Oct. 2009, pp. 1-3.

[36] C. Bennett and S.B. Wicker, "Decreased time delay and security enhancement recommendations for AMI smart meter networks," in: Innovative Smart Grid Technologies (ISGT 2010), Gaithersburg, MD, Jan. 2010, pp. 1-6.

[37] National Communications System, "Supervisory control and data acquisition (SCADA) systems," Technical Report, Oct. 2004, available at: http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf.

[38] S. Ward, J. O'Brien, B. Beresh, G. Benmouyal, D. Holstein, J.T. Tengdin, K. Fodero, M. Simon, M. Carden, M.V.V.S. Yalla, T. Tibbals, V. Skendzic, S. Mix, R. Young, T. Sidhu, S. Klein, J. Weiss, A. Apostolov, D.-P, Bui, S. Sciacca, C. Preuss, S. Hodder, and G. Seifert, "Cyber security issues for protective relays," in: IEEE Power Enginnering Society General Meeting, Tampa, FL, Jun. 2007, pp. 1-27.

[39] S. Hong and M. Lee, "Challenges and direction toward secure communication in the SCADA system," in: Proc. 8th Annual Communication Networks and Services Research Conference, Montreal, Canada, May 2010, pp. 381-386.

[40] F. Alsiherov and T. Kim, "Secure SCADA network technology and methods," in: Proc. 12th WSEAS International Conference on Automatic Control, Modelling & Simulation, Catania, Italy, May 2010, pp. 434-438.

[41] IEC TC57, "Power system control & associated communications - data & communication security," IEC 62351 Part 1 to 8, Technical Specification and Draft, 2010.

[42] A. Faruqui, R. Hledik, and S. Sergici, "Piloting the smart grid," The Electricity Journal, vol. 22, issue 7, 2009, pp. 55-69.

[43] H.K.-H. So, S.H.M. Kwok, E.Y. Lam, and King-Shan Lui, "Zero-configuration identity-based signcryption scheme for smart grid," in: The First IEEE Internation Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, Oct. 2010, pp. 321-326.

[44] G. Kalogridis, C. Efthymiou, S.Z. Denic, T.A. Lewis, and R. Cepeda, "Privacy for smart meters: towards undetectable appliance load signatures," in: The First IEEE Internation Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, Oct. 2010, pp. 232-237.

[45] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in: The First IEEE Internation Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, Oct. 2010, pp. 238-243.

[46] NaturalGas.org, "Natural gas and the environment," 2010, available at: http://www.naturalgas.org/environment/naturalgas.asp.

[47] A. Creery and E.J. Byres, "Industrial cybersecurity for power system and SCADA networks," in: Industry Applications Society 52nd Annual Petroleum and Chemical Industry Conference, Denver, Colorado, Sept. 2005, pp. 303-309.

[48] North American Electric Reliability Council, "SQL slammer worm lessons learned for consideration by the electricity sector," Jun. 2003, available at: http://www.esisac.com/publicdocs/SQL_Slammer_2003.pdf.

[49] J.Liu, Y. Xiao, and J. Gao, "Accountability in smart grids," in: IEEE Consumer Communications and Networking Conference 2011 (IEEE

CCNC 2011), Smart Grid Special Session, Las Vegas, Nevada, Jan. 2011.

[50] ModBus, "Modbus specifications and implimentation gudes," ModBus Protocol Specification v1.1b.

[51] ProfiBus, "Profibus standard," Profibus Specifications & Standards, available at: http://www.profibus.com/downloads/specifications-standards/.

[52] T. M. Overman and R. W. Sackman, "High assurance smart grid: smart grid control systems communications architecture," in: Proc. 1st IEEE SmartGridComm 2010, Gaithersburg, MD, Oct. 2010, pp. 19-24.

[53] R. Anderson and S. Fuloria, "Who controls the off switch?" in: Proc. 1st IEEE SmartGridComm 2010, Gaithersburg, MD, Oct. 2010, pp. 96-101.

[54] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," in: Proc. 16th ACM conference on Computer and Communications Security, Chicago, Illinois, 2009, pp. 21-32.

[55] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in: Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010, 2010.

[56] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in: Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010, 2010.

[57] G. Dan and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in: Proc. 1st IEEE SmartGridComm 2010, Gaithersburg, MD, Oct. 2010, pp. 214-219.

[58] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: attack strategies and countermeasures," in: Proc. 1st IEEE SmartGridComm 2010, Gaithersburg, MD, Oct. 2010, pp. 220-225.

[59] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in: Proc. 1st IEEE SmartGridComm 2010, Gaithersburg, MD, Oct. 2010, pp. 226-231.

[60] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in: Proc. 1st IEEE SmartGridComm 2010, Gaithersburg, MD, Oct. 2010, pp. 327-332.

[61] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Secure lossless aggregation for smart grid M2M networks," in: Proc. 1st IEEE SmartGridComm 2010, Gaithersburg, MD, Oct. 2010, pp. 333-338.

[62] D. P. Varodayan and G. X. Gao, "Redundant metering for integrity with information-theoretic confidentiality," in: Proc. 1st IEEE SmartGridComm 2010, Gaithersburg, MD, Oct. 2010, pp. 345-349.

[63] R. Berthier, W. H. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: requirements and architectural directions," in: Proc. 1st IEEE SmartGridComm 2010, Gaithersburg, MD, Oct. 2010, pp. 350-355.

[64] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K.L. Butler-Purry, "Towards modeling the impact of cyber attack on a smart grid," International Journal of Security and Networks (IJSN), special issue on security and privacy in smart grids, Vo. 6, No. 1, 2011 , pp. 2-13.

[65] G. Kalogridis, S. Z. Denic, T. Lewis, and R. Cepeda, "Privacy protection system and metrics for hiding electrical events," International Journal of Security and Networks (IJSN), special issue on security and privacy in smart grids, Vo. 6, No. 1, 2011, pp. 14-27.

[66] F. Li, B. Luo, and P. Liu, "Secure and privacy-preserving information aggregation for smart grids," International Journal of Security and Networks (IJSN), special issue on security and privacy in smart grids, Vo. 6, No. 1, 2011, pp. 28-39.

[67] J. Zhang and C. A. Gunter, "Application-aware secure multicast for power grid communications," International Journal of Security and Networks (IJSN), special issue on security and privacy in smart grids, Vo. 6, No. 1, 2011, pp. 40-52.

[68] Y. Xiao, "Editorial," International Journal of Security and Networks, Vol. 6, No.1, pp. 1 - 1, 2011.

[69] Y. Xiao, V. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A Survey of Key Management Schemes in Wireless Sensor Networks," Computer communications Journal, Special issue on Security on Wireless Ad Hoc and Sensor Networks, Vol. 30 No. 11-12, Sep. 2007. pp. 2314-2341.

[70] Y. Guo and S. Perreau, "Detect DDoS flooding attacks in mobile ad hoc networks," International Journal of Security and Networks, Vol. 5, No.4 pp. 259 - 269, 2010.

[71] Y. Xiao, H. Chen, B. Sun, R. Wang, and S. Sethi, "MAC Security and Security Overhead Analysis in the IEEE 802.15.4 Wireless Sensor Networks," EURASIP Journal on Wireless Communications and Networking, vol. 2006, Article ID 93830, 12 pages, 2006.

[72] S. Tang and W. Li, "An Epidemic Model with Adaptive Virus Spread Control for Wireless Sensor Networks," International Journal of Security and Networks, Vol. 6 No. 4, 2011.

[73] Y. Dong, S. Hsu, S. Rajput, and B. Wu, "Experimental analysis of application-level intrusion detection algorithms," International Journal of Security and Networks, Vol. 5, No.2/3 pp. 198-205, 2010.

[74] W. Chang, J. Wu, C. C. Tan, "Friendship-based Location Privacy in Mobile Social Networks," International Journal of Security and Networks, Vol. 6 No. 4, 2011.

[75] A. Olteanu, Y. Xiao, F. Hu, B. Sun, and H. Deng, "A Lightweight Block Cipher Based on a Multiple Recursive Generator for Wireless Sensor Networks and RFID," Wireless Communications and Mobile Computing (WCMC) Journal, John Wiley & Sons, Vol. 11, No. 2, pp. 254-266, Feb. 2011.

[76] Z. Zhuang, Y. Li, and Z. Chen, "Enhancing Intrusion Detection System with proximity information," International Journal of Security and Networks, Vol. 5, No.4 pp. 207-219, 2010.

[77] A. Desoky, "Edustega: An Education-Centric Steganography Methodology," International Journal of Security and Networks, Vol. 6 Nos. 2-3, 2011, pp. 153-173.

[78] H. Guo, Y. Mu, X.Y. Zhang, and Z.J. Li, "Enhanced McCullagh-Barreto identity-based key exchange protocols with master key forward security," International Journal of Security and Networks, Vol. 5, No.2/3 pp. 173 - 187, 2010.

[79] N. Jaggi, U. M. Reddy, and R. Bagai, "A Three Dimensional Sender Anonymity Metric," International Journal of Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 77-89.

[80] S. S.M. Chow and S. Yiu, "Exclusion-Intersection Encryption," International Journal of Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 136-146.

[81] A. Olteanu, Y. Xiao, and Y. Zhang, "Optimization between AES Security and Performance for IEEE 802.15.3 WPAN," IEEE Trans. Wireless Communications, Vol. 8, Nov. 12, Dec. 2009, pp. 6030-6037.

[82] N. Cheng, K. Govindan, and P. Mohapatra, "Rendezvous Based Trust Propagation to Enhance Distributed Network Security," International Journal of Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 101-111.

[83] J. Liu, Y. Xiao, H. Chen, S. Ozdemir, S. Dodle, and V. Singh, "A Survey of Payment Card Industry (PCI) Data Security Standard," IEEE Communications Surveys & Tutorials, Vol. 12, No. 3, pp. 287-303, Third Quarter 2010, DOI: 10.1109/SURV.2010.031810.00083

[84] A. Olteanu and Y. Xiao, "Security Overhead and Performance for Aggregation with Fragment Retransmission (AFR) in Very High-Speed Wireless 802.11 LANs," IEEE Trans. Wireless Communications, Vol. 9, No. 1, Jan. 2010, pp. 218-226.

[85] A. Fathy, T. ElBatt, and M. Youssef, "A Source Authentication Scheme Using Network Coding," International Journal of Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 112-122.

[86] D. Chopra, H. Schulzrinne, E. Marocco, and E. Ivov, "Peer-to-peer overlays for real-time communication: security issues and solutions," IEEE Communications Surveys & Tutorials, Vol. 11, No. 1, pp. 4-12. First Quarter 2009.

[87] G. Luo and K. P. Subbalakshmi, "KL-Sense Secure Image Steganography," International Journal of Security and Networks, Vol. 6 No. 4, 2011.

[88] B. W. Ramsey, B. E. Mullins, R. W. Thomas, T. R. Andel, "Subjective audio quality over a secure IEEE 802.11n network," International Journal of Security and Networks, Vol. 6, No.1, pp. 53-63, 2011.

[89] Y. Xiao, "Accountability for Wireless LANs, Ad Hoc Networks, and Wireless Mesh Networks," IEEE Commun. Mag., special issue on Security in Mobile Ad Hoc and Sensor Networks, Vol. 46, No. 4, Apr. 2008, pp. 116-126.

[90] Z. Chen, C. Chen, and Q. Wang, "On the scalability of Delay-Tolerant Botnets," International Journal of Security and Networks, Vol. 5, No.4 pp. 248-258, 2010.

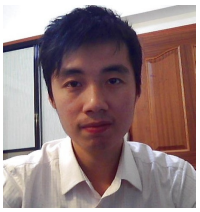
[91] D. Takahashi and Y Xiao, "Retrieving Knowledge from Auditing Log Files for Computer and Network Forensics and Accountability," (Wiley Journal) Security and Communication Networks, Vol. 1, No. 2, pp. 147-160, March/April 2008.

[92] D. Walker and S. Latifi, "Partial Iris Recognition as a Viable Biometric Scheme," International Journal of Security and Networks, Vol. 6 Nos. 2-3, 2011 , pp. 147-152.

[93] T. Abbes, A. Bouhoula, and M. Rusinowitch, "Efficient decision tree for protocol analysis in intrusion detection," International Journal of Security and Networks, Vol. 5, No.4 pp. 220-235, 2010.

[94] M. Peng and Y. Xiao, "A Survey of Reference Structure for Sensor Systems," IEEE Commun. Surveys & Tutorials, DOI: 10.1109/SURV.2011.081511.00070, accepted.

[95] K. R. Schrader, B. E. Mullins, G. L. Peterson, and R. F. Mills, "An FPGA-based system for tracking digital information transmitted via Peer-to-Peer protocols," International Journal of Security and Networks, Vol. 5, No.4 pp. 236 - 247, 2010.
[96] J. Liu, Y. Xiao, K. Ghaboosi, H. Deng, and, J. Zhang, "Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures," EURASIP Journal on Wireless Communications and Networking, Volume 2009, Article ID 692654, 11 pages, doi:10.1155/2009/692654
[97] Q. Chai and G. Gong, "On the (In)security of Two Joint Encryption and Error Correction Schemes," International Journal of Security and Networks, Vol. 6 No. 4, 2011
[98] T. Choi, and H. B. Acharya, "Is That You? Authentication in a Network without Identities," International Journal of Security and Networks, Vol. 6 No. 4, 2011
[99] H. Chen, Y. Chen, and D. H. Summerville, "A Survey on the Application of FPGAs for Network Infrastructure Security," IEEE Commun. Surveys & Tutorials, Vol. 13, No. 4, pp. 541-561, Fourth Quarter 2011.
[100] A. O. Richard, A. Ahmad, and K. Kiseon, "Security assessments of IEEE 802.15.4 standard based on X.805 framework," International Journal of Security and Networks, Vol. 5, No.2/3 pp. 188-197, 2010.
[101] M. Lei, Y. Xiao, S. V. Vrbsky, and C.-C. Li, "Virtual Password Using Random Linear Functions for On-line Services, ATMs, and Pervasive Computing," Computer Communications Journal, Elsevier, Vol. 31, No. 18, Dec. 2008, pp. 4367-4375.
[102] L. Liu, Y. Xiao, J. Zhang, A. Faulkner, and K. Weber, "Hidden Information in Microsoft Word," International Journal of Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 123-135.
[103] M. Barua, X. Liang, R. Lu, X. Shen, "ESPAC: Enabling Security and Patient-centric Access Control for eHealth in Cloud Computing," International Journal of Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 67-76.
[104] Y. Xiao, S. Yu, K. Wu, Q. Ni, C. Janecek, and J. Nordstad, "Radio Frequency Identification: Technologies, Applications, and Research Issues," Wireless Communications and Mobile Computing (WCMC) Journal, John Wiley & Sons, Vol. 7, No. 4, May 2007, pp.457-472.
[105] M. J. Sharma and V. C. M. Leung, "Improved IP Multimedia Subsystem Authentication Mechanism for 3G-WLAN Networks," International Journal of Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 90-100.
[106] Y. Xiao, H. Chen, X. Du, and M. Guizani, "Stream-based Cipher Feedback Mode in Wireless Error Channels," IEEE Trans. Wireless Commun., Vol.8, No.2, Feb. 2009, pp. 622-626.
[107] X. Zhao, L. Li, and G. Xue, "Authenticating Strangers in Online Social Networks," International Journal of Security and Networks, Vol. 6 No. 4, 2011.
[108] Y. Xiao, "Flow-Net Methodology for Accountability in Wireless Networks," IEEE Network, Vol. 23, No. 5, Sept./Oct. 2009, pp. 30-37.
[109] N. Ampah, C. Akujuobi, S. Alam, and M. Sadiku, "An intrusion detection technique based on continuous binary communication channels," International Journal of Security and Networks, Vol. 6 Nos. 2-3, 2011, pp. 174-180.
[110] Y. Xiao, X. Shen, B. Sun, and L. Cai, "Security and Privacy in RFID and Applications in Telemedicine," IEEE Commun. Mag., Special issue on Quality Assurance and Devices in Telemedicine, Vol. 44. No. 4, Apr. 2006, pp. 64-72.
[111] H. Chen and B. Sun, "Editorial," International Journal of Security and Networks, Vol. 6 Nos. 2/3, 2011 , pp. 65-66.
[112] M. Nicholes and Mukherjee, "A survey of security techniques for the border gateway protocol (BGP)," IEEE Commun. Surveys & Tutorials, Vol. 11, No. 1, pp. 52 - 65 . First Quarter 2009.
[113] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. L. P. Chen, "A Survey of Communication/Networking in Smart Grids," (Elsevier) Future Generation Computer Systems, Vol. 28, No. 2, Feb. 2012, pp. 391-404. DOI:10.1016/j.future.2011.04.014
[114] Z. Xiao, Y. Xiao, and D. Du, "Building Accountable Smart Grids in Neighborhood Area Networks," Proc. The IEEE Global Telecommunications Conference 2011 (IEEE GLOBECOM 2011).
[115] J. Liu, Y. Xiao, and J. Gao, "Accountability in Smart Grids," IEEE Consumer Communications and Networking Conference 2011 (IEEE CCNC 2011), Smart Grids Special Session.
[116] Y. Xiao, eds., "Communication and Networking in Smart Grids," Auerbach Publications, Taylor & Francis Group, CRC, ISBN-10: 1439878730, ISBN-13: 978-1439878736, 2012.



Jing Liu is a Ph.D. student in the Department of Computer Science at The University of Alabama. He is an active researcher in the area of network security, smart grid, bio-inspired network and telemedicine, including botnet issues, visual attention, anonymous communication and accountability in telemedicine. Jing Liu received his BSc and MSc degrees from the Hunan University (China) in 2005 and 2008, respectively.

Dr. Yang Xiao (SM'04) worked in industry as a MAC (Medium Access Control) architect involving the IEEE 802.11 standard enhancement work before he joined Dept. of Computer Science at The Univ. of Memphis in 2002. He is currently with Department of Computer Science at The University of Alabama. He was a voting member of IEEE 802.11 Working Group from 2001 to 2004. He is an IEEE Senior Member. He serves as a panelist for the US National Science Foundation (NSF), Canada Foundation for Innovation (CFI)'s Telecommunications expert committee, and the American Institute of Biological Sciences (AIBS), as well as a referee/reviewer for many national and international funding agencies. His research areas are security and communications/networks. He has published more than 180 refereed journal papers (including 50 IEEE/ACM transactions papers) and over 200 refereed conference papers and book chapters related to these research areas. Dr. Xiao's research has been supported by the US National Science Foundation (NSF), U.S. Army Research, The Global Environment for Network Innovations (GENI), Fleet Industrial Supply Center-San Diego (FISCSD), FIATECH, and The University of Alabama's Research Grants Committee. He currently serves as Editor-in-Chief for *International Journal of Security and Networks (IJSN)* and *International Journal of Sensor Networks (IJSNet)*. He was the founding Editor-in-Chief for *International Journal of Telemedicine and Applications (IJTA)* (2007-2009).

Shuhui Li received his B.S. and M.S. degrees in Electrical Engineering from Southwest Jiaotong University in Chengdu, China, in 1983 and 1988, respectively and Ph.D. degree in Electrical Engineering in 1999, from Texas Tech University. From 1988 to 1995, he was with the School of Electrical Engineering at Southwest Jiaotong University, where his fields of research interest include modeling and simulation of large dynamic systems, dynamic process simulation of electrified railways, power electronics, power systems, and power system harmonics. From 1995 to 1999, he was engaged in research on wind power, artificial neural networks, and applications of massive parallel processing. He joined Texas A&M University - Kingsville as an Assistant Professor in 1999 and then as an Associate Professor in 2003. He worked with Oak Ridge National Laboratory for simulation system development on supercomputers in 2004 and 2006. He joined the University of Alabama as an Associate Professor in 2006. His current fields of interest include renewable energy systems, power electronics, power systems, electric machines & drives, FACTS, intelligent control, microgrid, smart grid, and distributed generation.

Wei Liang received the Ph.D. degree in Mechatronic Engineering from Shenyang Institute of Automation, Chinese Academy of Sciences, in 2002. She is currently serving as an associate professor of Shenyang Institute of Automation. Her research interests are in the areas of wireless sensor network, dynamic scheduling theory and system simulation.

C. L. Philip Chen (S'88-M'88-SM'94-F'07) Dr. Chen is currently Dean and Chair Professor of the Faculty of Science and Technology, University of Macau. He has been a Professor and the Chair of the Department of Electrical and Computer Engineering, Associate Dean for Research and Graduate Studies of the College of Engineering, University of Texas at San Antonio, Texas. His current research interests include theoretic development in computational intelligence, intelligent systems, cyber-physical systems, robotics and manufacturing automation, networking, diagnosis and prognosis, and life prediction and life-extending control. He is an elected Fellow of IEEE and AAAS. He is the President of the IEEE Systems, Man and Cybernetics Society (SMCS), 2012-2013, where he has been the Vice President on Conferences and Meetings and the Vice President of the Technical Activities on Systems Science and Engineering. Dr. Chen is a member of Tau Beta Pi and Eta Kappa Nu honor societies and has been the faculty advisor for Tau Beta Pi Engineering honor society. In addition, he is an ABET (Accreditation Board of Engineering and Technology Education) Program Evaluator for Computer Engineering, Electrical Engineering, and Software Engineering programs.