A Survey on Cyber Security for Smart Grid Communications

Ye Yan, Yi Qian, Hamid Sharif and David Tipper

***Abstract*—A smart grid is a new form of electricity network with high fidelity power-flow control, self-healing, and energy reliability and energy security using digital communications and control technology. To upgrade an existing power grid into a smart grid, it requires significant dependence on intelligent and secure communication infrastructures. It requires security frameworks for distributed communications, pervasive computing and sensing technologies in smart grid. However, as many of the communication technologies currently recommended to use by a smart grid is vulnerable in cyber security, it could lead to unreliable system operations, causing unnecessary expenditure, even consequential disaster to both utilities and consumers. In this paper, we summarize the cyber security requirements and the possible vulnerabilities in smart grid communications and survey the current solutions on cyber security for smart grid communications.**

***Index Terms*—Smart grid communication, cyber security, vulnerability, reliability.**

I. Introduction

POWER industry is integrating the electrical distribution system with communication networks to form a two-directional power and information flow infrastructure, which is called a smart grid [1]. The integration not only moves power automation systems from outdated, proprietary technology to the advanced communication technologies, but also changes the closed power control systems to the public data networks [2]. By adding significant new functionality, distributed intelligence, and state-of-the-art communication capabilities to the power grid, the smart grid infrastructure can be more efficient, more resilient, and more affordable to manage and operate [3], [4].

However, it brings not only great performance benefit to the power industry, but also tremendous risks as well as arduous challenges in protecting the smart grid systems from cyber security threats [5]. Considering the vast scale of a smart grid, it is reasonable to expect that the cumulative vulnerability of the smart grid communication system might also be vast. Virtually all parties agree that the consequences of a smart grid cyber security breach can be enormous. New functions such as demand response introduce significant new cyber attack vectors such as a malware that initiates a massive coordinated and instantaneous drop in demand, potentially causing substantial damage to distribution, transmission, and even generation facilities [6].

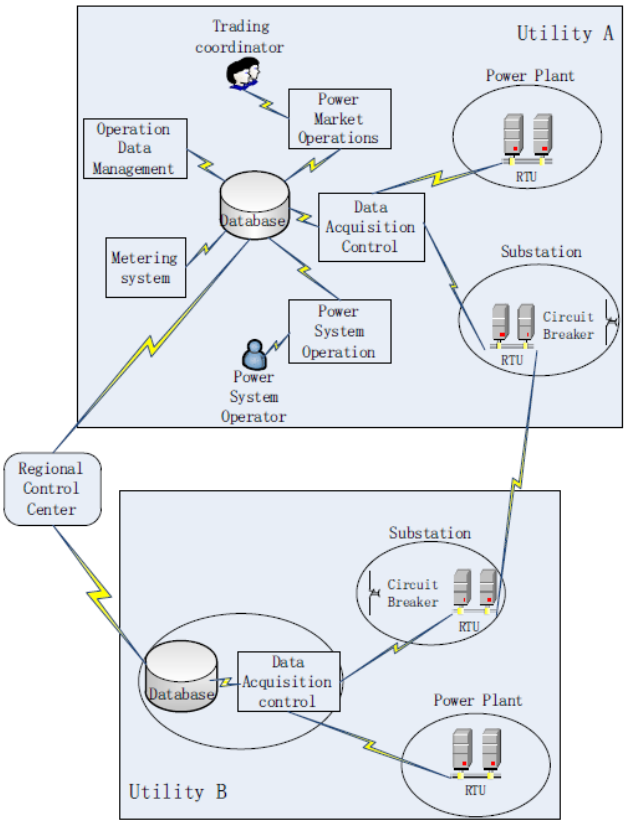

Fig. 1. A Smart Grid Communication System [7]

A typical smart grid communication system, as illustrated in Fig. 1, is a horizontal integration of one or more regional control centers, with each center supervising the operation of multiple power plants and substations. A smart grid communication system has a layered structure and performs data collection and control of electricity delivery. A regional control center typically support metering system, operation data management, power market operations, power system operation and data acquisition control. Substations contain Remote Terminal Units (RTUs), circuit breaker. Human Machine Interfaces (HMIs), communication devices (switches, hubs, and routers), log servers, data concentrators, and a protocol gateway. Intelligent Electronic Device (IEDs) are field devices, including an array of instrument transducers, tap changers, circuit re-closers, phase measuring units (PMUs), and protection relays [7].

Manuscript received 25 February 2011; revised 5 September 2011 and 22 November 2011.

Y. Yan, Y. Qian, and H. Sharif are with the Department of Computer and Electronics Engineering, University of Nebraska-Lincoln (e-mail: yqian@ieee.org).

D. Tipper is with the Graduate Telecommunications and Networking Program, University of Pittsburgh.

Digital Object Identifier 10.1109/SURV.2012.010912.00035.

The legacy cyber security techniques for enterprise networks can hardly fit well for the requirements of a smart grid communication system to operate securely in the public data communication networks such as internet. Compared with regular enterprise network systems, smart grid communication systems have different goals, objectives and assumptions concerning what need to be protected in cyber security. It is important to guarantee the real time performance and continuous operation features in a smart grid communication system. Those applications are not originally designed for the general enterprise network environment. Therefore, it is necessary to embrace the existing security solutions where they fit, such as communication networks within a control center and/or a substation, and develop unique solutions to fill the gaps where traditional enterprise network cyber security solutions do not work or apply [8].

Updating a system as complex as the smart grid communication infrastructure has the potential of introducing new security vulnerabilities into the system. In [9] the author presented a review of the work related to smart grid cyber security. The work reviewed is separated into five categories that make up different components of the smart grid: Process Control System (PCS) Security, Smart Meter Security, Power System State Estimation Security, Smart Grid Communication Protocol Security, and Smart Grid Simulation for Security Analysis. A smart grid is a large complex system, and it still requires a lot of cyber security design work.

In this paper we present a summary of vulnerabilities and potential cyber attacks on smart grid communication systems, and the major challenges of cyber security in smart grid communication systems. It also surveys the existing solutions for cyber security in smart grid communications.

The rest of this paper is organized as follows. In Section II, the background of smart grid communication security is described. Section III discusses the cyber security requirements for smart grid systems. Challenges and current solutions are discussed in Section IV and V respectively. Finally, Section VI draws the conclusion.

II. Background

A smart grid communication system is comprised of several subsystems. It is eventually a network of networks. SCADA is not only a controlling system but also a communication network in smart grid. The communication networks in smart grid systems could include dedicated or overlayed land mobile radios (LMR), cellular, microwaves, fiber optics, wirelines such as power line communications (PLC), RS-232/RS-485 serial links, wireless local area networks (WLANs) or a versatile data network combining these media [10]. In this section, we briefly discuss the background of a smart grid system in several aspects: SCADA system, communication networks and deployments of secure smart grid communications.

A. SCADA

Core to the monitoring and control of a substation is the SCADA system. It is utilized for Distribution Automation (DA) and computerized remote control of Medium Voltage (MV) substations and power grids, and it helps electric utilities to achieve higher reliability of supply and reduce operating and maintenance costs. In the past, Sectionalizer Switchgears, Ring Main Units, Reclosers and Capacitor Banks were designed for local operations with limited remote control. Today, using SCADA over reliable wireless communication links, RTUs provide powerful integrated solutions when upgrading remotely installed electric equipment. In a Distribution Management System (DMS), RTUs seamlessly interface via SCADA with a wide range of high performance control centers supplied by leading vendors worldwide. Connection to these Enterprise Management Systems (EMS) and DA/DMS control centers is typically provided via a high performance IP Gateway or a similar node [11].

B. Communication Networks

The operational and commercial demands of electric utilities require a high-performance data communication network that supports both existing functionalities and future operational requirements. Such a communication network constitutes the core of the electric system automation applications. The design of a cost-effective and reliable network architecture is crucial. In [12], the opportunities and challenges of a hybrid network architecture are discussed for electric system automation. Internet based Virtual Private Networks (VPNs), power line communications, satellite communications and wireless communications (wireless sensor networks, WiMAX and wireless mesh networks) are discussed. It provides a brief survey on the hybrid network architecture that can support the heterogeneous electric system automation application requirements. A smart grid communication network as a structured framework for electric utilities is planned to utilize new communication technologies for automation, and hence, to make the decision-making process more effective and direct.

Different scale and structure of the smart grid systems adopt different communication networking solutions. Advanced metering infrastructure (AMI) solutions can be meshed or point-to-point, with short local coverage or long range communications [13], [14]. Options for backhaul solutions might be fiber, wireless broadband, or broadband over power-line. The possible solutions include WiMax, WLAN, WSN, cellular and LMR, depending on the reliability, throughput, and coverage desired by the utility. The wireless communication solutions can be either licensed or unlicensed, again depending on the needs of the utility. For the highest reliability, licensed should be chosen. Each of the above options has their advantages and disadvantages, but what is consistently true of any and all of the solutions is the need to have a scalable security solution [15].

C. Deployments

Smart grid deployments must meet stringent security requirements. Strong authentication will be required for all users and devices which may affect the operation of the grid. With the large number of users and devices affected, scalable key and trust management systems, customized to the specific needs of the Energy Service Provider, will be essential. What has been learned from years of deploying and operating large secure network communication systems is that

the effort required to provision symmetric keys into thousands of devices can be too expensive or insecure. The development of key and trust management systems for large networks is required; these systems can be leveraged from other industries, such as land mobile radio systems and Association of Public-Safety Communications Officials (APCO) radio systems. Several APCO deployed systems provide state-wide wireless coverage, with tens of thousands of secure devices. Trust management systems, based on public key infrastructure (PKI) technology, could be customized specifically for smart grid operators, easing the burden of providing security which adheres to the standards and guidelines that are known to be secure [16]. Within three years there are expected to be over 1000 PMUs installed. There will be many more installed in distribution networks to help accommodate intermittent power from rooftop solar and electric vehicles. Additionally, PMUs will begin appearing at the terminals of generation equipment, transformers, and large motors. They will be used in large commercial and residential facilities. One of the key reasons for redundancy in PMU systems in smart grid is to support the requirements to be able to make security patches to the software without lost data. These software patches must be made with no loss of data. The energy company experience during the Hurricane Gustav power island event is a clear example of the value of PMUs for real time operations of the grid [17].

III. Requirements

The reliability of a smart grid depends on the reliability of the control and communication systems. In the development of smart grids, communication systems are becoming more and more sophisticated, allowing for better control and higher reliability. Smart grid will require higher degrees of network connectivity to support the new features. Meanwhile, the higher degree of connectivity should have corresponding sophisticated security protocols to deal with the cyber security vulnerabilities and breaches. Table I lists some security protocols adopted by different layers in communication networks with the specific security requirements, more details are summarized in [18]. In this section, we discuss the high level security requirements in general and the major security requirements and vulnerabilities in privacy, availability, integrity, authentication, authorization, auditability, nonrepudiability, third-party protection, and trust components for smart grid communications.

A. High Level Security Requirements

According to the Electric Power Research Institute (EPRI), one of the biggest challenges facing the smart grid deployment is related to cyber security of the systems [19]. According to the EPRI Report, cyber security is a critical issue due to the increasing potential of cyber attacks and incidents against this critical sector as it becomes more and more interconnected. Cyber security must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, or terrorists, but inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways. The high level requirements for smart grid communication security are conducted in various organizations and the corresponding standards in details.

There are many organizations working on the development of smart grid security requirements including North American Electrical Reliability Corporation-Critical Infrastructure Protection (NERC-CIP [20]), International Society of Automation (ISA [21]), IEEE 1402 [22], National Infrastructure Protection Plan (NIPP [23]), and National Institute of Standards and Technology (NIST), which has a number of smart grid cyber security programs on proceeding.

One prominent source of requirements is the Smart Grid Interoperability Panel (SGiP) Cyber Security Working Group, previously the NIST Cyber Security Coordination Task Group (CSCTG) [24]. The NIST CSCTG was established to ensure consistency in the cyber security requirements across all the smart grid domains and components. The latest draft document from the Cyber Security Working Group, NIST Interagency Report (NIST-IR7628) [25], entitled Smart Grid Cyber Security Strategy and Requirements, continues to evolve at the time of this writing. NIST and the DoE GridWise Architecture Council (GWAC) [26] have established Domain Expert Working Groups (DEWGs): Home-to-Grid (H2G), Building-to-Grid (B2G), Industrial-to-Grid (I2G), Transmission and Distribution (T&D) and Business and Policy (B&P).

Working with standards bodies, such as NIST and others, will be extremely important to ensure a highly secure, scalable, consistently deployed smart grid system, as these standards bodies will drive the security requirements of the system [27].

One thing is consistent among the various standards bodies, the security of the grid will strongly depend on authentication, authorization, and privacy technologies. Privacy technologies are well matured. Federal Information Processing Standard (FIPS) approved Advanced Encryption Standard (AES) [28] and Triple Data Encryption Standard (3DES) [29] solutions, offering strong security and high performance, are readily available. The specific privacy solution required will depend on the type of communication resource being protected. As a specific example, NIST has determined that 3DES solution will likely become insecure by the year 2030. Considering that utility components are expected to have long lifetimes, AES would be the preferred solution for new components. However, it is reasonable to expect that under certain circumstances where legacy functionality must be supported and the risk of compromise is acceptable, 3DES could be used.

Wireless links will be secured with technologies from well-known standards such as IEEE 802.11i [30] and IEEE 802.16e [31]. Different wireless protocols have varying degrees of security mechanisms. Wired links will be secured with firewalls, virtual private networks (VPNs) and IPSec technologies. Higher layer security mechanisms such as Secure Shell (SSH) and SSL/TLS should also be used [32].

System architects and designers often identify the need for and specify the use of secure protocols, such as SSH and IPSec, but then skip the implementation details associated with establishing security associations between end points of communications. Such an approach is likely to result

TABLE I
LAYERED SECURITY PROTOCOLS

Layer	Security Protocol	Application	Confidentiality	Integrity	Authentication
Application	WS-Security	Document	Yes	Yes	Data
	PGP/GnuPG	Email	Yes	Yes	Message
	S/MIME		Yes	Yes	
	HTTP Digest Authentication	Client-to-Server	No	No	User
Transport	SSH		Yes	Yes	Server
	SSL/TLS		Yes	Yes	
Network	IPSec	Host-to-Host	Yes	Yes	Host
Link	CHAP/PAP	Point-to-Point	No	No	Client
	WEP/WAP/802.1X	Wireless Access	Yes	Yes	Device

in a smart grid communication system where the necessary procedures for secure key management can quickly become extremely huge and complicated an operational nightmare. This is due to the fact that, when system architects do not develop an integrated and comprehensive key management scheme, customers may be provided with few key management options, and often resort to manually pre-configuring symmetric keys. This approach is simple for the system designers, but it can be very expensive for the system owners/operators.

B. Privacy

Privacy issues have to be covered with the derived customer consumption data as they are created in metering devices. Consumption data contains detailed information that can be used to gain insights on a customer's behavior.

Smart grid communications have unintended consequences for customer privacy. Electricity usage information stored at the smart meter and distributed thereafter acts as an information-rich side channel, exposing customers' habits and behaviors. Certain activities, such as watching television, have detectable power consumption signatures. History has shown that where financial or political incentives align, the techniques for mining behavioral data will evolve quickly to match the desires of those who would exploit that information [33].

Utility companies are not the only sources of potential privacy abuse. The recently announced Google PowerMeter service [34], for instance, receives real-time usage statistics from installed smart meters. Customers subscribing to the service receive a customized web page that visualizes local usage. Although Google has yet to announce the final privacy policy for this service, early versions leave the door open to the company using this information for commercial purposes, such as marketing individual or aggregate usage statistics to third parties. Although services such as Google PowerMeter are optional, the customers have less control over the use of power information delivered to utility companies. Existing privacy laws in the US are in general a patchwork of regulations and guidelines. It is unclear how these or any laws apply to customer energy usage yet.

C. Availability

Availability refers to ensuring that unauthorized persons or systems cannot deny access or use to authorized users. For smart grid systems, this refers to all the IT elements of the plant, like control systems, safety systems, operator workstations, engineering workstations, manufacturing execution systems, as well as the communication systems between these elements and to the outside world.

Malicious attacks targeting availability can be considered as denial-of-service (DoS) attacks, which attempt to delay, block or even corrupt information transmission in order to make network resources unavailable to communicating nodes that need information exchange in the smart grid. Since it is widely expected that at least, if not all, part of the smart grid will use IP-based protocols (e.g., IEC 61580 [35] has already adopted TCP/IP as a part of its protocol stacks) and TCP/IP is vulnerable to DoS attacks. DoS attacks against TCP/IP have been well studied in the literature regarding attacking types, prevention and response [36]–[38].

However, a major difference between a smart grid communication network and the Internet is that the smart grid is more concerned with the message delay than the data throughput due to the timing constraint of messages transmitted over the power networks. Indeed, network traffic in smart grid communication networks is in general time-critical. For instance, the delay constraint of generic object oriented substation events (GOOSE) messages is 4 ms in IEC 61850.

Intruders only need to connect to communication channels rather than authenticated networks in the smart grid, it is very easy for them to launch DoS attacks against the smart grid communication networks, especially for the wireless-based communication networks that are susceptible to jamming attacks [39]–[41]. Hence, it is of critical importance to evaluate the impact of DoS attacks on the smart grid and to design effective countermeasures to such attacks.

D. Integrity

Integrity refers to preventing undetected modification of information by unauthorized persons or systems. For smart grid communication systems, this applies to information such as product recipes, sensor values, or control commands. This objective includes defense against information modification via message injection, message replay, and message delay on the network. Violation of integrity may cause safety issues, that is, equipment or people may be harmed.

Different from attacks targeting availability, attacks targeting data integrity can be regarded as less brute-force yet more sophisticated attacks. The target of the integrity attacks is either customer's information (e.g., pricing information and customer account balance) or network operation information (e.g., voltage readings, device running status). In other words, such attacks attempt to deliberately modify the original infor-

mation in the smart grid communication system in order to corrupt critical data exchange in the smart grid.

The risk of attacks targeting data integrity in the power networks is indeed real. A notable example is the recent work [42], which proposed a new type of attacks, called false data injection attacks, against the state estimation in the power grid. It assumed that an attacker has already compromised one or several meters and pointed out that the attacker can take advantage of the configuration of a power system to launch attacks by injecting false data to the monitoring center, which can legitimately pass the data integrity check used in current power systems.

E. Authentication

Authentication is concerned with determination of the true identity of a communication system participator and mapping of this identity to a system-internal principal (e.g., valid user account) by which this user is known to the system. Most other security objectives, most notably authorization, distinguish between legitimate and illegitimate users based on authentication.

F. Authorization

Authorization, also known as access control, is concerned with preventing access to the system by persons or systems without permission to do so. In the wider sense, authorization refers to the mechanism that distinguishes between legitimate and illegitimate users for all other security objectives, e.g., confidentiality, integrity, etc. In the narrower sense of access control, it refers to restricting the ability to issue commands to the plant control system. Violation of authorization may cause safety issues.

G. Auditability

Auditability is concerned with being able to reconstruct the complete history of the system behavior from historical records of all (relevant) actions executed on it. This security objective is mostly relevant to discover and find reasons for malfunctions in the system after the fact, and to establish the scope of the malfunction or the consequences of a security incident. Note that auditability without authentication may serve diagnostic purposes, but does not provide accountability.

H. Nonrepudiability

Nonrepudiability refers to being able to provide irrefutable proof to a third party of who initiated a certain action in the system, even if this actor is not cooperating. This security objective is relevant to establish accountability and liability. In the context of smart grid systems, this is most important regarding to regulatory requirements, violation of this security requirement has typically legal/commercial consequences.

I. Third-party Protection

Third-party protection refers to averting damage done to third parties via the communication systems, that is, damage that does not involve safety hazards of the controlled plant itself. The successfully attacked and subverted automation system could be used for various attacks on the communication systems or data or users of external third parties, e.g., via Distributed DoS (DDoS) or worm attacks. Consequences could reach from a damaged reputation of a smart grid system owner up to legal liability for the damages of the third party. The risk to third parties through possible safety-relevant failures of the plant arising out of attacks against the plant automation system is covered by other security objectives, most notably authorization/access control.

J. Trust

The new designs of future smart grid communication systems form a multi-layered architecture. The growth of smart grid systems resulted in a plentifulness of power system related software applications, developed in many different programming languages and platforms. Extending old applications or developing new ones usually involves integrating legacy systems. Therefore approaching the security of future smart grid communication networks cannot be done with a complete new start.

In parallel to the development of smart grid communication systems, the complete and monolithic cyber security infrastructure is not a viable option. Instead, multi-layer architecture, advanced control methodologies and dependable software infrastructure as well as device protection mechanisms and hardware monitoring anchors have to be specified at the same time. Advanced control approaches have to include predictive and self-adaptive intelligence at higher level and cross-layer mapping to the different technical layers. The dependable software infrastructures have to be designed to identify and isolate higher-layer independent applications as well as to secure cross-layer communications. With such architecture, it should have the flexibility of incorporating parts of existing infrastructure with the frontiers and interfaces to adjacent systems. Furthermore, the architecture needs the flexibility to interchange or update the part of the system in a secure way at a later stage due to new laws and regulations or new developments in the energy market [43].

IV. CHALLENGES

Smart grid is a conglomeration of different legacy systems paired with new technologies and architectural approaches, based on different standards and regulations that all need to be amalgamated into a communication network to support the challenges of the future electricity network. To support this objective, the cyber security architecture for smart grid communications are being presented on the basis of cyber security and architecture requirements, dependency on legacy installations, and the regulations and industry standards. This section provides an overview of classifying functions and systems in a future smart grid communication network. Furthermore, it introduces methods for defining security controls and thus enabling the further development of a compliance process with regard to trusted connectivity in smart grid communications. The major challenges in building and operating a secure smart grid communication system include internetworking, security policy and operations, security services, efficiency and

scalability, and the differences between enterprise network and smart grid network security.

A. Internetworking

The interconnected smart grid communication systems are riddled with vulnerabilities that vary across the networks due to the lack of built-in security in many applications and devices. This should not be the model for a network as important as the smart grid. Layers of cyber security defense of smart grid should be built into the solution to minimize the threats from interruption, interception, modification, and fabrication.

Keeping the network private, i.e. where all transport facilities are wholly owned by a utility, would greatly minimize the threats from intruders, as there would be no potential for access from intruders over the Internet. But having a completely separate network is not feasible in today's highly connected world. It makes good business sense to reuse communication facilities, such as the Internet. A minimally secured smart grid connected with Internet as commonly found with commercial networks, opens the grid to threats from multiple types of attacks. These include cyber attacks from hostile groups looking to cause an interruption to the power supply [33], [44].

One of these cyber attacks is worm infestations which have proven to negatively impact critical network infrastructures. Such threats have largely been the result of leaving a network vulnerable to threats from the Internet. For example, there have been DoS attacks on a single network that disrupted all directory name servers, thus prohibiting users from connecting to any of the resources. It demonstrates the fragility of an interconnected smart grid communication infrastructure [45].

All connections to the Internet from a smart grid network need to be highly secure. Intrusion detection is needed not only at the points where a smart grid network connects to the Internet, but also critical points within the network as well as vulnerable wireless interfaces [46].

The components, systems, networks, and architecture are all important to the security design and reliability of the smart grid communication solutions. But its inevitable that an incident will occur at some point and one must be prepared with the proper incident response plan. This can vary between commercial providers and private utility networks. A private utility network is likely to provide better consistency of the incident response plan in the event of a security incident, assuming the private network is built upon a standardized framework of hardware and software. The speed of the response decreases exponentially as the number of parties involved increases. Conversely, a private network would ideally depend on fewer parties, therefore a more efficient incident response process would provide for more rapid response and resolution. The rapidity of the response is critical during situations that involve a blackout [47].

Criticalness of a device or a system also determines how prone it will be to attacks. History has shown that private networks by their inherent nature are less prone to attacks. As a result, it is recommended as the best approach in situations where security is paramount [48].

B. Security Policy and Operations

The reliability of a smart grid depends on the proper operations of many components and the proper connectivity between them [49]. To disrupt a smart grid system, an attacker might attempt to gain electronic access to a component and configure it to impersonate as another component and/or report a false condition or alarm. One of the simplest types of attacks that an adversary might attempt is the DoS attack, where the adversary prevents authorized devices from communicating by consuming excessive resources on one device. For example, it is a well-known issue that if a node, such as a server or an access control device, uses an authentication protocol which is prior to authentication and authorization, then the node may be subject to DoS attacks. Smart grid protocol designers must ensure that proper care and attention is given to this threat during protocol development.

Many organizations will be involved in the operations of a smart grid. As more distributed intelligence entities are added to the smart grid communication network, it will be essential that those entities (people or devices) can authenticate and determine the authorization status of other entities from a remote organization. This issue is commonly referred to as federated identity management. There are many possible technical solutions to this issue based on different security policies, such as those offered by Security Assertion Markup Language (SAML) [50], Web Services Trust (WS-Trust) [51], and PKI [52]. Not only will vendors need to offer consistent technical solutions, but organizations will further need consistent security policies. Great care must be taken by organizations to ensure their security policies and practices are not in conflict with those of other organizations with which they will need interoperability. At least a minimum set of operational security policies for the organizations operating a smart grid is formally adopted and documented in industry standards [53].

C. Security Services

Managing and maintaining a secure smart grid will be as equally vital as developing, deploying and integrating a secure smart grid solution. Security services will help network operators to identify, control and manage security risks in smart grid communications.

According to EPRI, every aspect of a smart grid must be secure [19]. Cyber security technologies are not enough to achieve secure operations without policies, on-going risk assessment, and training. The development of these human focused procedures takes time and needs to take time to ensure that they are done correctly.

A smart grid requires access to cost-effective, high-performance security services, including expertise in mobility, security, and system integration. These security services can be tailored per utility to best fit their needs and help them achieve their organizational objectives. Fig. 2 illustrates a typical set of security services in smart grid communications [54]. It describes a framework that operationalizes cyber security across the people, process, policy and technology foundations of each organization.

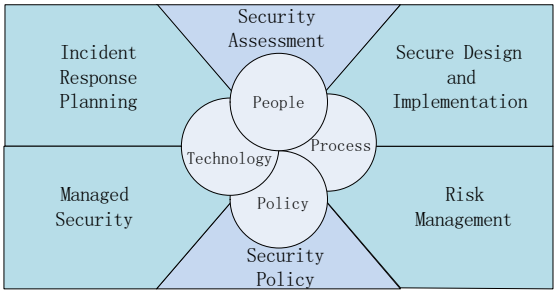

Fig. 2. Smart Grid Security Services [54]

D. Efficiency and Scalability

Ensuring system availability is a high priority in critical systems like the smart grid which requires that several key issues be addressed. First, the system must be efficient in its use of computation and communication resources so that resources do not get overwhelmed and all requests can be handled. Second, the system must have good error management built in to ensure proper handling of failures (e.g., those resulting from bad messages). Furthermore, the error management functions must be fail-safe in nature so they do not lead to resource exhaustion even in the face of adversarial action. Third, the system must have adequate redundancy built into it so that, if sub-systems fail or are compromised, then the entire system does not collapse. Fourth, the system should support auxiliary security functions that may be deployed in the smart grid communication system to detect to and respond to cyber attacks [49].

Since many existing cyber security scheme such as key management schemes are not suitable for deployment in smart grid, in [55] the authors proposed a novel key management scheme which combines symmetric key technique and elliptic curve public key technique. The symmetric key scheme is based on the Needham-Schroeder authentication protocol. The known threats including the man-in-the-middle attack and the replay attack can be effectively eliminated under the proposed scheme. The advantages of the key management scheme for smart grid communication include strong security, scalability, fault-tolerance and efficiency.

E. Differences between Enterprise Network and Smart Grid Network Security

During the last decade, the IT industry has witnessed the development of many cyber security solutions to protect enterprise networks and to reduce the vulnerabilities to cyber attacks. From firewalls to intrusion detection systems (IDS) and Virtual Private Networks (VPN), these solutions have been quite effective in securing the IT infrastructure at business and office automation levels. However, the enterprise network based cyber security solutions come short of providing the same level of security at the control and automation levels. There are three major differences between enterprise network and smart grid network security.

1) Different Security Objectives: In enterprise networks, the main security objective is to protect data. The following major concerns exist: 1) data integrity; 2) data confidentiality; and 3) data availability. Preserving data integrity refers to protecting data against modification by unauthorized persons or entities. Data confidentiality refers to the prevention of data access by unauthorized persons or entities. Maintaining data availability involves ensuring that no person or entity could deny access to those authorized users and systems. In smart grid, the first priority is always human safety. The second priority is to ensure the system reliability. For instance, a cyber attack could create a blackout (system outage), a brownout (degraded power quality) or shift the power grid system from its economically optimal running condition. The third priority is the protection of equipment and power lines [53].

2) Different Security Architecture: In enterprise networks, the data server resides at the center of the network and requires more protection than the edge nodes, which are used as access points by end users. In smart grid networks, EMS sits at the center (in the control center) whereas RTU/PLCs sit at the edge. Usually, only devices (such as re-closer, circuit breaker), which are controlled directly by RTU/PLCs, can do harm to human life, operation, or damage equipment and power lines. EMS/SCADA and data log servers cannot do any damage directly. Therefore, in smart grid communication systems, edge nodes need the same level of protection as central devices [56].

3) Different Technology Base: In enterprise networks, Windows, Unix and Linux are widely used as operating systems, whereas Ethernet is used to connect all devices with IP-based protocols. Therefore, common security solutions are designed based on these common architectures. However, in current smart grid communication systems, besides the common operating systems above, many utilities use proprietary operating systems and networks facilities, and many different communication protocols (IEC61850, DNP 3.0, ICCP, etc.) are in use rather than ordinary TCP/IP suits. Thus, it is very difficult to develop common host-based or network-based security solutions for smart grid applications [57].

V. Current Solutions

In this section, we survey several existing solutions on cyber security for smart grid communications. We focus on the technologies being deployed, the key smart grid communication applications being implemented and the outlines of power industry trials that have recently been announced in privacy, integrity, authentication and trusted computing.

A. Privacy

Privacy of smart grid communication systems is important to the eventual acceptance by the public. Smart grid communications must assure that the communication data preserves privacy anywhere at anytime.

In [44], the authors proposed a method for compressed meter reading for smart metering in smart grid communications. The distinguishing feature of the compressed meter reading is that the active smart meters are allowed to transmit simultaneously and the access point (AP) is able to distinguish the reports from different smart meters. The simultaneous access results in uniform delays, in contrast to the possible large delay in carrier sensing multiple access (CSMA) technique. The

random sequence used in the compressed sensing enhances the privacy of the meter reading.

In [58], the authors described a method for securely anonymizing frequent (for example, every few minutes) electrical metering data sent by a smart meter. Although such frequent metering data may be required by a utility or electrical energy distribution network for operational reasons, the data may not necessarily be attributable to a specific smart meter or consumer. However, it needs to be securely attributable to a specific location (e.g. a group of houses or apartments) within the electricity distribution network. The proposed method provides a 3rd party escrow mechanism for authenticated anonymous meter readings which are difficult to associate with a particular smart meter or customer. This method does not preclude the provision of attributable metering data that is required for other purposes such as billing, account management or marketing research purposes.

In [59], the authors presented a home electrical power routing scheme that can be used to moderate the home's load signature in order to hide appliance usage information. A power management model using a rechargeable battery with a power mixing algorithm is proposed. Then, the protection level is evaluated by proposing three different privacy metrics: an information theoretic (relative entropy), a clustering classification, and a correlation/regression one. This paper sets the ground for further research on the subject of optimizing home energy management hiding load signatures.

In smart grid communication systems, any stored data should be encrypted using storage keys shielded similar to the mechanisms proposed in [60]–[62]. While a Storage Root Key (SRK) can be used to develop a key chain by encrypting individual storage keys whose private part will not be exposed to the host system. The storage keys then may seal potentially unlimited data on any medium [63].

B. Integrity

Several integrity policy models (e.g., Biba [64], LOMAC [65], and Clark-Wilson [66]) have been developed to govern integrity levels of a system. The Biba model ensures that processes can not corrupt data in higher levels and are not corrupted by data from lower level processes [64]. The LOMAC model dynamically sets the integrity level of a process to the minimum integrity level of data it interacts with [65]. Similarly, the Clark-Wilson model allows a process to discard or upgrade the integrity level of data thus allowing it to interact with lower integrity level data [66]. In smart grid communications, however, it might leave the policy decisions to a user but focus on mechanisms to provide security services. In the following, system integrity, process integrity, and data integrity are discussed:

1) System integrity: System integrity is a binary property that indicates whether the system has a trustworthy execution environment. Using trusted computing functionalities, it performs binary attestation to verify the integrity of a system and its enforcement capabilities. Particularly, all parties in blind processing will challenge peers to ensure that the remote system conforms to Trusted Computing Group (TCG) specifications with (1) a Trusted Platform Module (TPM) providing root of trust, (2) a security kernel providing an isolated execution environment for trusted processes whose computations and memory are safe from tampering, (3) a cryptographically protected storage for sensitive data decipherable only by the dedicated process, and (4) shielded communication channels with remote processes.

2) Process integrity: The integrity of a process essentially depends on the genuineness of its code. It is important not only to detect changes in software but also to ensure that newly developed code is trustworthy. A modified code may yield malicious behavior that would compromise the data. We can ensure the integrity of a process using fingerprints, i.e., cryptographic digest or hash functions of its code. When communicating with an ally or competitor process both parties will assure the integrity of each other by comparing stored fingerprints with reported Platform Configuration Registers (PCR) values before transmitting any data. To enforce process integrity, it applies software engineering techniques that enhance software security, including safe software architecture and compilation techniques for intrusion prevention [67], security specification and management [68], software quality assurance throughout software lifecycle, and security testing [69].

3) Data integrity: Verifying the genuineness of data depends on whether the data is collected or generated. Collected data is primitive data given to a process and its integrity is application specific. Some techniques to ensure integrity of collected data are semantic check (i.e., integration of logic into the process to verify data semantics), certificate (i.e., signatures from trusted central authorities), and trusted path (i.e., ensuring that the data come from an authenticated user or sensing device) [70].

Generated data integrity depends on genuineness of the process and collected data. Overall, data integrity requires a chain of trust. Ensuring the integrity of generated data requires ensuring the integrity of the generating process as well as the integrity of input data to the process. Ensuring the integrity of input data requires ensuring the genuineness of the communicating process or the input device.

Integrity evaluation involves verifying the source, its integrity, and freshness of the measurements and requires knowledge of fingerprints (i.e., SHA-1 hashes) of the code involved in blind processing. Secure root processes of the TPM are utilized to develop authenticators that ensure integrity of processes using the Core Root of Trust for Measurement (CRTM) [71]–[73]. Moreover, as CRTM performs integrity measurement at load-time, run-time vulnerabilities will be detected using run-time attestation [70] and verifiable code execution [74].

Integrity measurement of a complete interactive system is a challenging task, as thousands of measurements and knowledge of their fingerprints may be required for various software [75], [76]. In [77] the authors investigated the integrity of a known set of processes loaded in a deterministic order and running in an isolated environment from the rest of the processes. Using a security kernel, a system needs to ensure integrity of the TPM, the BIOS, the security kernel and a well-known set of processes providing blind processing.

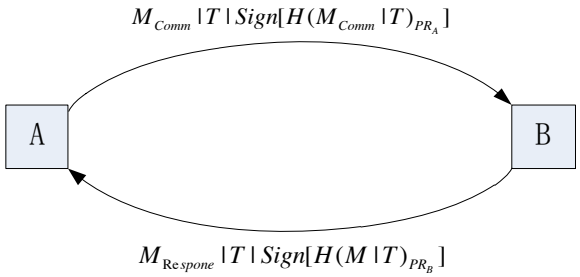

Fig. 3. Digital signature approach for authentication and integrity [81].

C. Authentication

Smart grid communications must be authenticated by adding to the information flow transmission to verify whether a communication entity is the one that is claimed and the transmitted data has integrity [78]. The mechanisms that provide authentication usually also provide integrity, the ability to verify that a message has arrived unaltered from its original state. Authentication and integrity can help smart grid system to protect against the most common cyber attacks, including man-in-the-middle, forgery, impersonation, and message modification. Numerous tools exist for providing authentication and integrity, including hashes and keyed hashes such as SHA-1 or HMAC-SHA-1 and digital signatures such as RSA or ECC signatures [79].

One of the sophisticated attacks that authentication protocols must address is the replay attack, in which an adversary captures messages and replays them to the devices later. A message may have dramatically different effects depending upon when it is received. For example, a message to increase reactive power output by 10 MVAr is appropriate to deal with a low voltage situation. However, if the same message is delayed and resent during a time when the system is experiencing high voltages, the result of the same message will be the opposite of what was intended. There are two popular ways for helping ensure that a message is fresh and not a replay. If the system can support the notion of time and at least loose clock synchronization, then timestamps can provide freshness. Therefore, timestamps have their own constraint on synchronization [80]. Other options include the use of nonces (random numbers) and sequence numbers. Nonces usually involve an extra message exchange while sequence numbers, which identify the order of individual TCP packets, need reliable communication channels to ensure synchronization. Any authentication effort must provide some way to ensure that a message is current and not the rebroadcast of a previously sent communication.

In [81], the authors proposed an authentication and integrity approach that used digital signatures and timestamps. Fig. 3 illustrates this approach. Parties A and B reside within the same communication realm. A transmits to B the message M_{Comm} and a timestamp T in plaintext, along with the digital signature of the message and timestamp combination, $M_{Comm}|T$. It computes the digital signature by hashing $M_{Comm}|T$ and then encrypting it with its private key PR_A. The recipient B receives the plaintext message M_{Comm} and timestamp T, along with the digital signature. It decrypts the signature using A's public key to unwrap the hash $H(M_{Comm}|T)$ that was known to A before encrypted it, computes its own hash $H^{'}(M^{'}_{Comm}|T^{'})$, and compares $H^{'}$ with H. If they match, then B knows that $M_{Comm}|T$ and $M^{'}_{Comm}|T^{'}$ are identical. Therefore, B can conclude that the message must have been sent by A, since A's public key can faithfully decrypt something encrypted by A's private key only; and that the combination of message and timestamp were not altered in transit. To guard against replay, when B confirms that the timestamp it received matches what A tried to send, it will record the timestamp in its own log. If it receives another message with the same timestamp later, it knows that the later message must be a replay, and can discard that.

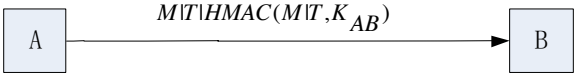

Fig. 4. HMAC approach for authentication and integrity [81].

The digital signature approach might introduce more computational overhead than is necessary. Since confidentiality does not merit as much concern as authentication and integrity for real-time control in smart grid, an approach that does not require an encryption step, HMAC [82], might be more appropriate. Fig. 4 shows A sends a message M to B at time T using HMAC to provide authentication and integrity. A and B share some secret, K_{AB}. Along with M and T, A computes and sends to B the HMAC of the combination $M|T$. When this message arrives at B, B computes its own HMAC of the combination $M|T$ it received. If the HMAC B computes matches the HMAC value received from A, then B can conclude, assuming no other entities have knowledge of the secret key K_{AB} it shares with A, that A must have sent the message and that no third party altered the combination $M|T$ in transit. Therefore, B has authenticated the sender of the message and verified the integrity of the contents. Verification of message freshness works as that B will maintain a log of received timestamps and reject later messages that have an identical timestamp to one that appears in the log already. The reduced computational expense of HMAC makes it the preferred authentication and integrity approach for situations where confidentiality is not a primary concern.

D. Trusted Computing

Considering the incredible size of the cyber security threat and severe consequences from cyber attacks, the smart grid cyber security protection must be extremely tight to the cyber security requirements. Smart grid communication requires a comprehensive security plan that encompasses virtually all aspects of smart grid operations. One component of such a plan includes trusted computing. Fig. 5 shows a basic trusted computing model [83]. Such platforms and associated mechanisms are used to ensure that malware is not introduced into software processing devices. The main design goal is the realization of a minimal and therefore manageable, stable and evaluable security kernel for conventional hardware platforms, servers, embedded systems, and mobile devices like PDAs and smartphones. All requirements are fulfilled by extracting only security-critical operations and data to the security kernel.

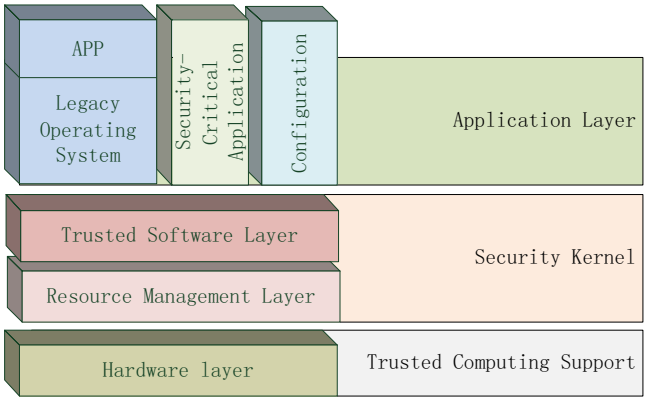

Fig. 5. Trusted Computing model [83]

There are two categories of devices for which the malware protection problems should be considered: embedded computer systems and general purpose computer systems. Embedded systems are computer systems that are designed to perform a specific task or set of tasks. They are intended to run only software that is supplied by the manufacture. By contrast, general purpose systems are intended to support third party software purchased by the specific consumer who purchased the system. A PC is an excellent example of a general purpose system. A microwave oven, or cable television set-top box, are examples of embedded systems. The problem of malware protection should be considered separately for each category.

For embedded systems the problem of protecting the system against the installation of malware can be solved with high degrees of assurance. First and foremost the manufacturer must implement secure software development processes. Many standard models for such processes are defined [84]. Second, if the device is intended to be field upgradable, the manufacturer must provide a secure software upgrade solution. The predominant method of doing this is to manufacture the embedded system hardware with secure storage containing keying material for a software validation. Typically the hardware is configured with the public key of a secure signing server operated by the manufacturer. With this key, the device can validate any newly downloaded software prior to running it. Such a proactive approach can provide higher levels of assurance than can be obtained with a reactive approach such as a virus checker.

For devices which are intended to run for long periods of time (e.g., years) without booting, it is useful to have a method of performing secure software validation on running code. It is possible to have background tasks that can periodically perform such functions without disrupting the operations of the device. It is further possible to couple such background validation steps with other operational aspects of the device, such that if the device is found to be compromised, secure hardware on the device (needed to bring up and maintain security associations with remote entities) will prevent the local device from establishing and maintaining security associations with the remote entities. In [85], the authors described some methods to provide remote device attestation.

To make matters worse, the rapid adoption of cloud computing and sophisticated Internet based applications has resulted in the widespread deployment of a number of mobile code technologies. Mobile code is the code which is downloaded and run on your PC, typically by your browser, without the users' knowledge. Examples of mobile code include ActiveX, Flash animation, Java, JavaScript, PDF, Postscript, and Shockwave. The Department of Homeland Security (DHS) Control System Security Program recommends tight controls on mobile code in critical control systems for the nation's critical infrastructure and key resources (CIKR) [86].

To address this concern, the adoption of, and adherence to, strict code signing standards by smart grid suppliers and operators are proposed. Mechanisms for enforcing such standards on general purpose computers, such as PCs, have been put forth by the Trusted Computing Group and are well documented [87]. Such standards should cover all critical devices including field deployed units, such as RTU and IED, network devices, such as routers, switches, and firewalls, and control center equipment, such as servers and user consoles. The standards should cover embedded systems, as well as general purpose computers, their operating systems, drivers, and applications, as well as all mobile codes. That is, no mobile code should be allowed to run on a critical PC or server that has not been signed by an authority that is able to determine the trustworthiness of the code. Considering that it is certain that hardware and software elements for critical components of the grid will come from many different providers, it is likely that a trust management framework will have to be established for smart grid. This framework will likely require the establishment of a set of criteria that are to be met by vendors who wish to sell critical components to smart grid operators. Additionally it is likely that one or more accreditation organizations will need to be established to audit suppliers to determine that they are meeting the specified criteria [87].

VI. Conclusion

As a critical infrastructure, smart grid requires comprehensive solutions for cyber security. A comprehensive communication architecture with security built in from the very beginning is necessary. A smart grid communication security solution requires a holistic approach including traditional schemes such as PKI technology, trusted computing elements, authentication mechanisms based on industry standards. Clearly, securing the smart grid communication infrastructure will require the use of standards-based state-of-the-art security protocols. To achieve the vision put forth, there are many steps which need to be taken. Primary among them is the need for a cohesive set of requirements and standards for smart grid security. Industry and other participants should continue the work that has begun under the direction of NIST to accomplish these foundational steps quickly. However, the proper attention must be paid to creating the requirements and standards, as they will be utilized for many years, given the lifecycle of utility components. In this paper, we present the background and requirements for smart grid communication security. After discussing the challenge of smart grid communication security, the current research and solutions are surveyed. This paper gives an insight to smart grid communication security in

architecture features, system designs as well as technical development.

REFERENCES

[1] C. W. Gellings, M. Samotyj, B. Howe, "The future's smart delivery system (electric power supply)," IEEE Power and Energy Mag., vol.2, no.5, pp. 40-48, Sept.-Oct. 2004.

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

[3] S. M. Amin, B. F. Wollenberg, "Toward a smart grid: power delivery for the 21st century," IEEE Power and Energy Mag., vol.3, no.5, pp. 34-41, Sept.-Oct. 2005.

[4] Litos Strategic Communication "The Smart Grid: An Introduction ," 31 May 2009 [Online]. Available: http://www.oe.energy.gov /DocumentsandMedia/DOE_SG_Book_Single_Pages.pdf

[5] H. Khurana, M. Hadley, L. Ning, and D. A. Frincke, "Smart-grid security issues," IEEE Security and Privacy, vol. 8, pp. 81-85, 2010.

[6] S. Clements, H. Kirkham, "Cyber-security considerations for the smart grid," in IEEE Power and Energy Society General Meeting 2010, pp. 1-5, 2010.

[7] C. H. Hauser, D. E. Bakken, A. Bose, "A Failure to Communicate," IEEE Power and Energy Mag., pp. 47-55, Mar- Apr, 2005.

[8] J. Fan, S. Borlase, "The evolution of distribution," IEEE Power and Energy Mag., vol. 7, pp. 63-68, 2009.

[9] T. Baumeister, "Literature Review on Smart Grid Cyber Security," Tech Report, 2010.

[10] C. Lo and N. Ansari, "The Progressive Smart Grid System from Both Power and Communications Aspects," IEEE Commun. Surveys & Tutorials, pp. 1-23, 2011.

[11] S. Hong, and M. Lee, "Challenges and Direction toward Secure Communication in the SCADA System," in Eighth Annual Communication Networks and Services Research Conference (CNSR 2010), pp.381-386, 2010.

[12] V. C. Gungor and F. C. Lambert, "A survey on communication networks for electric system automation," Computer Networks, vol. 50, pp. 877-897, 2006.

[13] L. Wenpeng, D. Sharp, and S. Lancashire, "Smart grid communication network capacity planning for power utilities," in IEEE Transmission and Distribution Conference and Exposition, pp.1-4, 2010.

[14] E. Liu, M. L. Chan, C. W. Huang, N. C. Wang, and C. N. Lu, "Electricity grid operation and planning related benefits of advanced metering infrastructure," in 5th International Conference on Critical Infrastructure (CRIS2010), pp. 1-5, 2010.

[15] P. P. Parikh, M. G. Kanabar, and T. S. Sidhu, "Opportunities and challenges of wireless communication technologies for smart grid applications," in IEEE Power and Energy Society General Meeting,pp. 1-7, 2010.

[16] A. R. Metke; R. L. Ekl, "Security Technology for Smart Grid Networks," IEEE Trans. Smart Grid, vol. 1, pp. 99-107, 2010.

[17] C. H. Wells, A. Moore, K. Tjader, and W. Isaacs, "Cyber secure synchrophasor platform," in IEEE/PES Power Systems Conference and Exposition (PSCE 2011), pp. 1-4, 2011.

[18] D. Dzung, M. Naedele, T. P. Von Hoff, and M. Crevatin, "Security for Industrial Communication Systems," Proc. IEEE, vol. 93, pp. 1152-1177, 2005.

[19] Report to NIST on Smart Grid Interoperability Standards Roadmap EPRI, Jun. 17, 2009 [Online]. Available: http://www.nist.gov/smartgrid/ InterimSmartGridRoadmapNISTRestructure.pdf

[20] M. Zafirovic-Vukotic, R. Moore, M. Leslie, R. Midence, and M. Pozzuoli, "Secure SCADA network supporting NERC CIP," in Power & Energy Society General Meeting, 2009. PES '09. IEEE, 2009, pp. 1-8.

[21] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. de Vicuna, and M. Castilla, "Hierarchical Control of Droop-Controlled AC and DC Microgrids: A General Approach Toward Standardization," Industrial Electronics, IEEE Transactions on, vol. 58, pp. 158-172, 2011.

[22] IEEE Guide for Electric Power Substation Physical and Electronic Security, IEEE Std 1402-2000, 2000.

[23] D. Dumont, "Cyber security concerns of Supervisory Control and Data Acquisition (SCADA) systems," in IEEE International Conference on Technologies for Homeland Security (HST 2010), pp. 473-475, 2010.

[24] T. Zhang, W. M. Lin, Y. F. Wang, S. Deng, C. C. Shi, and L. Chen, "The design of information security protection framework to support Smart Grid," in International Conference on Power System Technology (POWERCON 2010), pp. 1-5, 2010.

[25] Draft smart grid cyber security strategy and requirements, NIST IR 7628, Sep. 2009 [Online]. Available: http://csrc.nist.gov/publications/ drafts/nistir-7628/draft-nistir-7628.pdf

[26] S. Widergren, A. Levinson, J. Mater, and R. Drummond, "Smart grid interoperability maturity model," in 2010 IEEE Power and Energy Society General Meeting, , 2010, pp. 1-6.

[27] S. Rohjans, M. Uslar, R. Bleiker, J. Gonzalez, M. Specht, T. Suding, and T. Weidelt, "Survey of Smart Grid Standardization Studies and Recommendations," in First IEEE International Conference on Smart Grid Communications (SmartGridComm 2010), pp. 583-588, 2010.

[28] National Institute of Standards and Technology, "Announcing the Advanced Encryption Standard (AES)," in Federal Information Processing Standards Publication, Nov. 26, 2001.

[29] National institute of Standards and Technology, "Data Encryption Standard," Federal Information Processing Standards (FIPS) Publication 46-7, USA, 1999.

[30] IEEE Std 802.11i, "IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements," pp. 1-175, 2004.

[31] IEEE Std 802.16e, "IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1," pp. 1-822, 2006.

[32] A. Bendahmane, M. Essaaidi, A. El Moussaoui, and A. Younes, "Grid computing security mechanisms: State-of-the-art," in International Conference on Multimedia Computing and Systems (ICMCS '09), pp. 535-540, 2009.

[33] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," IEEE Security & Privacy, vol. 7, pp. 75-77, 2009.

[34] K. Allan, "Power to the people [power energy saving]," Engineering & Technology, vol. 4, pp. 46-49, 2009.

[35] T. S. Sidhu and Y. Yin, "Modelling and simulation for performance evaluation of IEC61850-based substation communication systems," IEEE Trans. Power Del., vol. 22, no. 3, pp. 1482C1489, July 2007.

[36] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni, "Analysis of a denial of service attack on tcp," in Proc. IEEE Symposium on Security and Privacy (S&P 1997), May 1997.

[37] A. Yaar, A. Perrig, and D. Song, "Pi: A path identification mechanism to defend against DDoS attacks," in Proc. IEEE Symposium on Security and Privacy (S&P 2003), 2003.

[38] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, pp. 39C53, 2004.

[39] M. Strasser, S. Capkun, C. Popper, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in Proc. IEEE Symposium on Security and Privacy (S&P 2008), May 2008, pp. 64C78.

[40] C. Popper, M. Strasser, and S. Capkun, "Jamming-resistant broadcast communication without shared keys," in Proc. 18th USENIX Security Symposium (Security 09), Aug. 2009.

[41] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication," in Proc. 29th IEEE Conference on Computer Communications (INFOCOM 10), Mar. 2010.

[42] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," in Proc. ACM Conference on Computer and Communications Security (CCS 09), Sept. 2009.

[43] N. Kuntze, C. Rudolph, M. Cupelli, J. Liu, and A. Monti, "Trust infrastructures for future energy networks," in IEEE Power and Energy Society General Meeting 2010, pp. 1-7, 2010.

[44] L. Husheng, M. Rukun, L. Lifeng, and R. C. Qiu, "Compressed Meter Reading for Delay-Sensitive and Secure Load Report in Smart Grid," in First IEEE International Conference on Smart Grid Communications (SmartGridComm2010), pp. 114-119, 2010.

[45] G. Carl, G. Kesidis, R. R. Brooks, and R. Suresh, "Denial-of-service attack-detection techniques," IEEE Internet Computing, vol. 10, pp. 82-89, 2006.

[46] S. Kent, "On the trail of intrusions into information systems," IEEE Spectrum, vol. 37, pp. 52-56, 2000.

[47] C. W. Ten, G. Manimaran, and C. C. Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling," IEEE Trans. Systems, Man and Cybernetics, Part A: Systems and Humans, vol.40, no.4, pp.853-865, July 2010.

[48] W. Dong, L. Yan, 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), pp. 1-7, 2010.
[49] M. Jensen, C. Sel, U. Franke, H. Holm, and L. Nordstrom, "Availability of a SCADA/OMS/DMS system - A case study," in IEEE Innovative Smart Grid Technologies Conference Europe (ISGT Europe 2010), pp.1-8, 2010.
[50] T. Komura, Y. Nagai, S. Hashimoto, M. Aoyagi, and K. Takahashi, "Proposal of Delegation Using Electronic Certificates on Single Sign-On System with SAML-Protocol," in Ninth Annual International Symposium on Applications and the Internet (SAINT '09), pp. 235-238, 2009.
[51] C. Yongkai and T. Shaohua, "Security Scheme for Cross-Domain Grid: Integrating WS-Trust and Grid Security Mechanism," in International Conference on Computational Intelligence and Security(CIS '08), pp.453-457, 2008.
[52] R. Perlman, "An overview of PKI trust models," IEEE Network, vol. 13, pp. 38-43, 1999.
[53] R. J. Thomas, "Putting an action plan in place," IEEE Power and Energy Mag., vol. 7, pp. 26-31, 2009.
[54] A. R. Metke and R. L. Ekl, "Smart Grid Security Technology," in Innovative Smart Grid Technologies (ISGT2010), pp. 1-7, 2010.
[55] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," IEEE Trans. Smart Grid, vol. 2, pp. 375-381, 2011.
[56] T. M. Overman, R. W. Sackman, "High assurance smart grid: smart grid control systems communications architecture," in First IEEE International Smart Grid Communications (SmartGridComm 2010), Conference, pp.19-24, 2010.
[57] E. Santacana, G. Rackliffe, L. Tang, X.M. Feng, "Getting smart," IEEE Power and Energy Mag., vol. 8, pp. 41-48, 2010.
[58] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," in First IEEE International Conference on Smart Grid Communications (SmartGridComm 2010), pp. 238-243, 2010.
[59] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures," in First IEEE International Conference on Smart Grid Communications (SmartGridComm 2010), pp. 232-237, 2010.
[60] E. Cesena, G. Ramunno, and D. Vernizzi, "Secure storage using a sealing proxy," In Proc. 1st European Workshop on System Security, pages 27-34, New York, NY, USA, 2008.
[61] U. Kühn, M. Selhorst, and C. Stüble, "Realizing property-based attestation and sealing with commonly available hard and software," In Proc. 2007 ACM workshop on Scalable trusted computing, pp. 50-57, New York, NY, USA, 2007.
[62] U. Kühn and C. Stüble, "User-friendly and secure tpm-based hard disk key management," In Proc. First International Conference Future of Trust in Computing, pp. 171-177, Berlin, Germany, 2009.
[63] H. S. Fhom, N. Kuntze, C. Rudolph, M. Cupelli, J. Liu, and A. Monti, "A user-centric privacy manager for future energy systems," in International Conference on Power System Technology (POWERCON2010), pp. 1-7, 2010.
[64] K. J. Biba, "Integrity considerations for secure computer systems," Technical report, MITRE Corp., Apr, 1977.
[65] T. Fraser, "Lomac: Low water-mark integrity protection for cots environments," In IEEE Symposium on Security and Privacy, pp. 230C245, 2000.
[66] D. D. Clark and D. R. Wilson, "A Comparison of Commercial and Military Computer Security Policies," In IEEE Symposium on Security and Privacy, pp. 184-194, 1987.
[67] D. Kirovski, M. Drinic, and M. Potkonjak, "Enabling trusted software integrity," In proceedings of the 10th international conference on Architectural support for programming languages and operating systems(ASPLOS-X), pp. 108-120, New York, NY, USA, 2002.
[68] I. Sommerville, "Software Engineering," Addison-Wesley, 8th edition, 2007.
[69] R. S. Pressman, "Software Engineering: A Practitioners Approach," McGraw Hill, 7th edition, 20010.
[70] E. Shi and A. Perrig, "Bind: A fine-grained attestation service for secure distributed systems," In IEEE Symposium on Security and Privacy, pp. 154-168, 2005.
[71] M. Alam, X. Zhang, M. Nauman, T. Ali, and J.-P. Seifert, "Model-based behavioral attestation," In Proc. 13th ACM symposium on Access control models and technologies (SACMAT 08), pp. 175-184, New York, NY, USA, 2008.
[72] R. Sailer, T. Jaeger, X. Zhang, and L. V. Doorn, "Attestation-based policy enforcement for remote access," In 11th ACM conference on Computer and Communications Security, pp. 308-317, 2004.
[73] F. C. Schweppe and J. Wildes, "Power system static-state estimation," IEEE Trans. Power App. Syst., pp. 120-125, Jan, 1970.
[74] A. Seshadri, M. Luk, E. Shi, A. Perrig, L. van Doorn, and P. Khosla, "Pioneer: Verifying integrity and guaranteeing execution of code on legacy platforms," In ACM Symposium on Operating Systems Principles, pp. 1-15, Oct. 2005.
[75] J. M. McCune, A. Perrig, A. Seshadri, and L. van Doorn, "Turtles all the way down: research challenges in user-based attestation," In proceedings of the 2nd USENIX workshop on Hot topics in security (HOTSEC07), pp. 1-5, Berkeley, CA, USA, 2007.
[76] F. Stumpf, A. Fuchs, S. Katzenbeisser, and C. Eckert, "Improving the scalability of platform attestation," In Proc. 3rd ACM workshop on Scalable trusted computing (STC 08), pp. 1-10, New York, NY, USA, 2008.
[77] M. H. Gunes and C. Y. Evrenosoglu, "Blind processing: Securing data against system administrators," in IEEE/IFIP Network Operations and Management Symposium Workshops (NOMS Wksps 2010), pp. 304-311, 2010.
[78] International Standards Organization and International Electrotechnical Commission, ISO/IEC 9798-1:1997 Information Technology-Security Techniques- Entity Authentication Parts.
[79] W. Stallings, "Network security essentials : applications and standards." Boston: Prentice Hall, 2011.
[80] R. J. Anderson, R. M. Needham, "Robustness principles for public key protocols," in Proc. 15th Annu. Int. Cryptology Conf. Advances in Cryptology (CRYPTO95), pp. 236-247,1995.
[81] K. M. Rogers, R. Klump, H. Khurana, A. A. Aquino-Lugo, and T. J. Overbye, "An Authenticated Control Framework for Distributed Voltage Support on the Smart Grid," IEEE Trans. Smart Grid, vol. 1, pp. 40-47, 2010.
[82] Q. Dang, "Recommendation for Applications Using Approved Hash Algorithms" National Institute of Standards and Technology Special Publication, 2009.
[83] European Multilaterally Secure Computing Base, "Towards trustworthy systems with open standards and trusted computing," 2005 [Online] Available: http://www.emscb.com/content/pages/49373.htm
[84] N. Davis, "Secure software development life cycle processes," Software Eng. Inst., Carnegie Mellon Univ., 2009.
[85] M. Shaneck, K. Mahadevan, V. Kher, and Y. Kim, "Remote software based attestation for wireless sensors," Comput. Sci. Eng., Univ. Minnesotał Twin Cities, 2005
[86] U. S. Department of Homeland Security "Catalog of Control Systems Security: Recommendations for Standards Developers," Sep. 2009.
[87] D. Challener, K. Yoder, R. Catherman, D. Safford, and L. V. Doorn , "A Practical Guide to Trusted Computing", Upper Saddle River, NJ: IBM Press.

Ye Yan is the Ph.D. student in the Department of Computer and Electronics Engineering at University of Nebraska-Lincoln. He has published several research articles in international journals and conferences. He has been serving as TPC members on IEEE conferences and reviewers for many international journals and conferences. He is a student member of IEEE.

Yi Qian is an Assistant Professor in the Department of Computer and Electronics Engineering, University of Nebraska-Lincoln (UNL). His research interests include information assurance and network security, network design, network modeling, simulation and performance analysis for next generation wireless networks, wireless ad-hoc and sensor networks, vehicular networks, broadband satellite networks, optical networks, high-speed networks and the Internet. Prior to joining UNL, he worked in the telecommunications industry, academia, and the U.S. government. Some of his previous professional positions include serving as a senior member of scientific staff and a technical advisor at Nortel Networks, a senior systems engineer and a technical advisor at several start-up companies, an Assistant Professor at University of Puerto Rico at Mayaguez, and a senior researcher at National Institute of Standards and Technology. He has a successful track record to lead research teams and to publish research results in leading scientific journals and conferences. Several of his recent journal articles on wireless network design and wireless network security are among the most accessed papers in the IEEE Digital Library. Dr. Yi Qian is a member of ACM and a senior member of IEEE. He is currently serving as the Vice Chair for Conferences - Communications and Information Security Technical Committee (CISTC) for IEEE Communications Society. He is also serving as the IEEE Communications Society CISTC Representative to the Ad Hoc Committee on Smart-Grid Communications.

Hamid Sharif is the Charles J. Vranek Professor of the College of Engineering at the University of Nebraska-Lincoln. He is also the Director of the Advanced Telecommunications Engineering Laboratory (TEL) at University of Nebraska. Professor Sharif has published a large number of research articles in international journals and conferences and has been the recipient of a number of best paper awards. Dr. Sharif has been serving on many IEEE and other international journal editorial boards and currently is the co-editor-in-chief for the Wiley Journal of Security and Communication Networks. He has contributed to the IEEE in many roles including the elected Chair of the Nebraska Section, elected Chair of the Nebraska Computer Chapter, elected Chair of the Nebraska Communications Chapter, and the Chapter Coordinator for the IEEE Region 4 in US.

David Tipper is an Associate Professor and Director of the Graduate Telecommunications and Networking Program at the University of Pittsburgh. He is a graduate of the University of Arizona (Ph.D. EE, M.S.S.I.E.) and Virginia Tech (B.S.E.E.). His current research focuses on network design, energy efficiency, information assurance techniques, time varying network performance analysis and control.