

Cyber Security in the Smart Grid: Survey and Challenges[☆]

Wenye Wang^{a,*}, Zhuo Lu^a

^aDepartment of Electrical and Computer Engineering, North Carolina State University, Raleigh NC 27606, US.

Abstract

The Smart Grid, generally referred to as the next-generation power system, is considered as a revolutionary and evolutionary regime of existing power grids. More importantly, with the integration of advanced computing and communication technologies, the Smart Grid is expected to greatly enhance efficiency and reliability of future power systems with renewable energy resources, as well as distributed intelligence and demand response. Along with the silent features of the Smart Grid, cyber security emerges to be a critical issue because millions of electronic devices are inter-connected via communication networks throughout critical power facilities, which has an immediate impact on reliability of such a widespread infrastructure. In this paper, we present a comprehensive survey of cyber security issues for the Smart Grid. Specifically, we focus on reviewing and discussing security requirements, network vulnerabilities, attack countermeasures, secure communication protocols and architectures in the Smart Grid. We aim to provide a deep understanding of security vulnerabilities and solutions in the Smart Grid and shed light on future research directions for Smart Grid security.

Keywords: Smart Grid, Cyber security, Attacks and countermeasures, Cryptography, Security protocols

1. Introduction

In past decades, the development of power grids has not been keeping pace with the industrial and social advancements that drastically increase the demand on power supply. For example, statistics [1] showed that from 1950 to 2008, energy production and consumption in the US increase approximately two and three times, respectively. In particular, the public/commercial services, industry and residential areas are the most demanding areas for electricity in the US in 2008. In order to cope with such a demand increase, one major challenge is to *efficiently manage* a variety of energy resources, including traditional fossil fuel sources (e.g., coal, petroleum, and natural gas), and renewable energy resources (e.g., solar and hydro) [2]. Therefore, the National Institute of Standards and Technology (NIST) rolled out national efforts to develop the next-generation electric power system, commonly referred to as the Smart Grid [3].

Compared with legacy power systems, the Smart Grid is envisioned to fully integrate high-speed and two-way communication technologies [4–8] into millions of power equipments to establish a dynamic and interactive infrastructure with new energy management capabilities, such as advanced metering infrastructure (AMI) [9] and demand response [10]. However, such a heavy dependence

on information networking inevitably surrenders the Smart Grid to potential vulnerabilities associated with communications and networking systems. This in fact increases the risk of compromising reliable and secure power system operation, which, nonetheless, is the ultimate objective of the Smart Grid. For example, it has been shown [11] that potential network intrusion by adversaries may lead to a variety of severe consequences in the Smart Grid, from customer information leakage to a cascade of failures, such as massive blackout and destruction of infrastructures.

As a result, we are motivated to investigate *cyber security* issues in the Smart Grid, which is of critical importance to the design of information networks and has been considered as one of the highest priorities for the Smart Grid design [12, 13]. Since the research on cyber security for the Smart Grid is still in its early stage, our objective is to provide an overview, analyze potential cyber security threats, review existing security solutions, and summarize research challenges in the Smart Grid. Specifically, the following issues are discussed in the paper:

- Objectives and requirements: We first describe the objectives and requirements of cyber security in the Smart Grid, with a focus on identifying fundamental differences between the Smart Grid and another large-scale network paradigm, the Internet.
- Potential cyber security threats: Since cyber attacks mainly come from malicious threats in communication networks, we review cyber attacks in electric power systems, and provide an extensive analysis of network vulnerabilities under important use cases in the Smart Grid.

[☆]This work is supported by ERC Program of the National Science Foundation under Award Number EEC-08212121 – FREEDM at North Carolina State University.

*Corresponding author. Phone: 919-513-2549. Fax : 919-515-5523.

Email addresses: wwang@eos.ncsu.edu (Wenye Wang), zlu3@ncsu.edu (Zhuo Lu)

- **Attack prevention and defense:** To efficiently counter-act cyber attacks, it is essential to widely deploy attack prevention and defense strategies throughout the Smart Grid. Therefore, we conduct an evaluation of the existing solutions, including network and cryptographic countermeasures, by considering case studies and applications in the Smart Grid.
- **Network protocols and architectures:** As attack countermeasures will be integrated into network protocols to achieve reliable information exchange, the effectiveness of security solutions needs to be evaluated in the course of message delivery for real-time monitoring, control and protection in the Smart Grid. Thus, we present discussions on existing cyber security solutions, as well as open research issues, in combination with communication architectures and protocols in the context of real-time and non-real time scenarios for the Smart Grid.

The remainder of this paper is organized as follows. In Section 2, we introduce the fundamental communication network architecture in the Smart Grid. In Section 3, we present the objectives and requirements of cyber security. In Section 4, we categorize and evaluate network threats with case studies in the Smart Grid. In Sections 5 and 6, we discuss network and cryptographic countermeasures against cyber attacks in the Smart Grid, respectively. In Section 7, we review and summarize secure communication protocols for message delivery. Finally, we discuss and conclude in Sections 8 and 9, respectively.

2. Communication Network Architecture in the Smart Grid

In this section, we present the fundamental architecture of communication networks in the Smart Grid, which is followed by widely-adopted communication protocols for power grids.

2.1. Fundamental Architecture

Electric power systems are very complex physical networks. For example, statistics [8] showed that there are over 2000 power distribution substations, about 5600 distributed energy facilities, and more than 130 million customers all over the US.

According to NIST's conceptual model [3], the Smart Grid consists of seven logical domains: Bulk Generation, Transmission, Distribution, Customer, Markets, Service Provider and Operations. The first four feature the two-way power and information flows. The last three feature information collection and power management in the Smart Grid. (A more detailed discussion on Smart Grid domains can be found in [14–16].) In order to interconnect all these domains, the communication network must be highly-distributed and hierarchical. As shown in Fig. 1, we represent the Smart Grid communication network onto

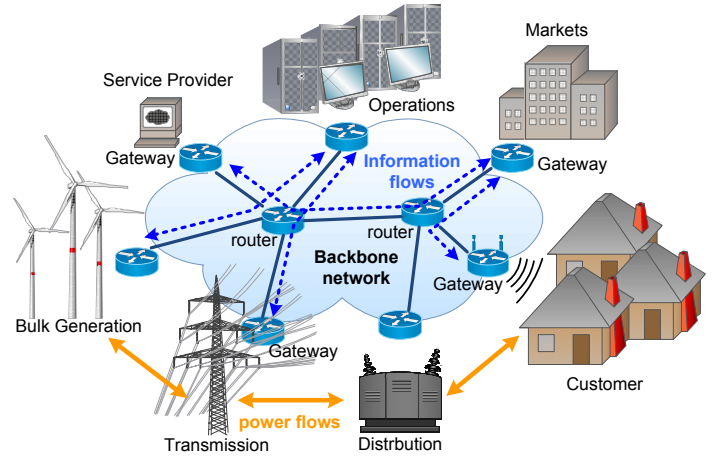


Figure 1: The network architecture in the Smart Grid: backbone and local-area networks.

a hybrid and hierarchical network, including the backbone network and millions of local-area networks.

The backbone network is established for inter-domain communication. It consists of infrastructure nodes, which can be either gateways for local-area networks or high-bandwidth routers to forward messages across a variety of domains in the Smart Grid. In the backbone network, conventional wireline communication technologies, such as fiber optical technologies, can be used to achieve high-speed data and bulk information delivery across domains. For example, the SCADA system is a power operation monitoring system across the Operations, Transmission, and Distribution domains. All power signal quality samples are delivered from local-area systems in Transmission and Distribution domains via the backbone network to the Operations domain for centralized management.

A local-area network is used for intra-domain communication. A local-area network consists of ad-hoc nodes, which are meters, sensors or intelligent electronic devices (IEDs) installed on the power infrastructure. They are usually equipped with limit bandwidth and computational ability for certain monitoring or protection purposes.

Ad-hoc nodes in a local-area network are not limited to use wireline communication. In fact, many of them are expected to use wireless technologies, such as wireless sensor networks [17, 18], cellular systems [5, 7], and even cognitive radio [19]. It has been shown that there are a number of advantages for using wireless communication technologies in the Smart Grid [5–7, 17, 18], including untethered access to utility information, mobility, reduced cost, low complexity, and off-the-shelf products such as WiFi and ZigBee. Besides research efforts, industry companies are also endeavoring to develop new wireless communication products for the Smart Grid. For example, ZigBee embedded products have been released recently to target the Smart Grid applications, such as smart meters, demand response, and home-area network devices for the AMI system in the Customer domain [20].

Therefore, comparing with legacy power systems, the Smart Grid will leverage both wireline and wireless network technologies to provide a revolutionary paradigm of large-scale, highly-distributed, and hierarchical communication infrastructures for energy delivery and management in the future. To ensure secure and reliable operation, such a complicated information system requires a comprehensive security treatment [21] based on the specific features in the Smart Grid communication network, which will be described in the following subsection.

2.2. Features of Smart Grid Communication Networks

It is evident that the Smart Grid communication network is similar to the Internet in terms of the complexity and hierarchical structure. However, there are fundamental differences between these two complex systems in many aspects.

1. Performance metric. The basic function of the Internet is to provide data services (e.g., web surfing and music downloading, etc.) for users. How to achieve high throughput and fairness among users is of great importance in the Internet design. Whereas, power communication networks are used *not* to provide high-throughput services, but to ensure reliable, secure, and real-time message delivery and non-real time monitoring and management. Hence, *latency* is much more important than the throughput in power systems, leading to delay-oriented design in power communication protocols. For example, in power substation communications, time-critical messages for protection purposes are passed from the application layer directly to the MAC layer to avoid redundant processing [22].
2. Traffic model. It is well known that many Internet traffic flows have the self-similarity property, such as the world wide web (WWW) traffic [23]. In power networks, however, a large amount of traffic flows are periodic [24, 25] for the purpose of consistent monitoring, such as raw data sampling in power substations and periodic meter reading in home-area networks [3]. Thus, it can be expected that the majority, if not all, of communication traffic in the Smart Grid differs from that in the Internet.
3. Timing requirement. Over the Internet, most IP traffic is best-effort traffic while the delay-sensitive traffic has delay requirements of 100–150 ms in order to support voice-over-IP and multimedia services [26]. However, the Smart Grid features a wider range of delay requirements from milliseconds to minutes [3]. For example, messages for trip protection in substations have the delay constraint of 3 ms [22, 27]. Therefore, the Smart Grid has much more stringent timing requirements for message delivery than the Internet.
4. Communication model. The end-to-end principle is the basis of the Internet such that it can support peer-to-peer communication between any node pair in the

world. In legacy power grids, the most commonly used communication model is one-way communication: electronic devices report their readings to the control center. In contrast, the Smart Grid enables a two-way communication model: *top-down* (center to device) and *bottom-up* (device to center). The Smart Grid also supports the peer-to-peer communication model, but usually restricts the model in local-area networks for security concerns [28, 29].

5. Protocol stack. The Internet is built upon the IP protocol and is moving forward to IPv6. It has been widely expected that the Smart Grid will use IPv6 [3] as the major network-layer protocol. However, the Smart Grid is not limited to IPv6 and can have heterogeneous protocol stacks, depending on network functionalities and requirements. For example, ATM switching has been proposed to guarantee quality-of-service (QoS) for time-critical message delivery in power transmission systems [30]. As a result, the Smart Grid will feature heterogeneous protocol stacks for a variety of applications.

Table 1 summarizes the fundamental differences between the Smart Grid communication network and the Internet. From Table 1, we can see that although the Internet offers a paradigm for the design of large-scale communication network infrastructures, the design of communication networks for the Smart Grid still needs to be revisited comprehensively to ensure efficient, robust and secure information delivery for energy management of a variety of power facilities.

2.3. Communication Protocols for Power Systems

Power system communication protocols have been evolving for decades, from various proprietary protocols to recently standardized protocols. In the following, we briefly introduce two widely-used protocols in power systems: the distributed networking protocol 3.0 (DNP3) that is currently the predominant standard used in North America power systems [31], and IEC 61850 that is recently standardized for modern power substation automation by the International Electrotechnical Commission (IEC) [22]. A more comprehensive summary of communication protocols for power systems can be found in [6].

2.3.1. DNP3

DNP3 is a power communication protocol originally developed by General Electric that made it public in 1993. DNP3 was first designed for supervisory control and data acquisition (SCADA) applications and is now widely used in electrical, water infrastructure, oil and gas, security and other industries in North America, South America, South Africa, Asia and Australia [6].

DNP3 was initially designed with four layers: physical, data link, transport, and application layers [6]. The original physical layer was based on serial communication

Table 1: Differences between the Internet and the Smart Grid communication network.

	The Internet	Smart Grid Communication Network
Performance metric	Throughput and fairness	Message delay
Major traffic	Power-law	Periodic
Timing requirement	Delay-sensitive (100ms) to best-effort	Time-critical (3ms) to best-effort
Communication model	End-to-end	Two-way, limited peer-to-peer
Protocol stack	IPv4, IPv6	Proprietary, heterogeneous, IPv6

protocols, such as Recommended Standard (RS)-232, RS-422, or RS-485. Today’s DNP3 has been ported over to the TCP/IP layer to support recent communication technologies, and thus can be regarded as a three-layer network protocol operating upon the TCP/IP layer [6] to support end-to-end communication.

2.3.2. IEC 61850

IEC 61850 is a recent standard recommended by IEC for Ethernet-based communications in substation automation systems [22]. Differing from DNP3 that is based on TCP/IP, IEC 61850 specifies a series of protocol stacks for a variety of services, including TCP/IP, UDP/IP, and an application-directly-to-MAC stack for time-critical messages. In addition, IEC 61850 explicitly defines timing requirements for information and data exchange in power substations. Table 2 shows a list of delay requirements for IEC 61850 messages, which reveals that the power substation communication features a number of time-critical messages with application-layer delay constraints varying from 3ms to 500ms.

Table 2: Messages for substation communication in IEC 61850.

Message Type	Delay Constraint
Type 1A/P1	3 ms
Type 1A/P2	10 ms
Type 1B/P1	100 ms
Type 1B/P2	20 ms
Type 2	100 ms
Type 3	500 ms

- Types 1A/P1 and 1A/P2 are used for fault isolation and protection purposes, thus having very strict delay constraints.
- Types 1B/P1 and 1B/P2 are used for routine communications between automation systems.
- Types 2 and 3 are used for less time-critical information exchange, such as monitoring and readings, in substations.

It is worth noting that IEC 61850 is intended to replace DNP3 in substation communications. However, current

IEC 61850 is only limited within a power substation, but it is generally believed that IEC 61850 can be potentially used for outside substation communication in future power systems [6].

As the initial design of DNP3 and IEC 61850 came without any security mechanisms, their messages can be easily intercepted or falsified in the Smart Grid network, which in turn results in either information leakage or incorrect operation of power devices. Hence, the power, network and security communities are working cooperatively to design secure and reliable protocols for Smart Grid applications. Before we provide a comprehensive coverage on security issues and design, it is vital to first present the high-level security objectives and requirements for the Smart Grid in the following section.

3. Objectives and Requirements of Cyber Security in the Smart Grid

The Smart Grid communication network is a mission-critical network for information exchange in power infrastructures. To ensure secure and reliable operation, it is essential to understand what are the security objectives and requirements before providing a comprehensive treatment of cyber security in the context of energy delivery and management. Here, we describe the objectives and security requirements for the Smart Grid.

3.1. Smart Grid Security Objectives

The cyber security working group in the NIST Smart Grid interoperability panel has recently released a comprehensive guideline for Smart Grid cyber security [29]. In the following, we cite three high-level Smart Grid security objectives, as shown in Fig. 2 [29].

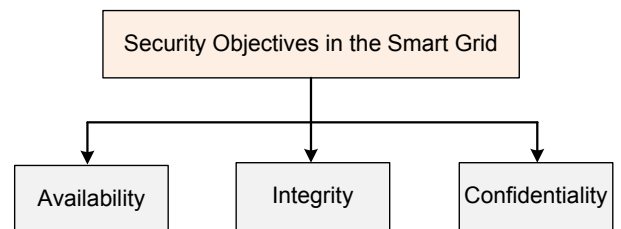


Figure 2: Three high-level security objectives for the Smart Grid.

- **Availability:** Ensuring timely and reliable access to and use of information is of the most importance in the Smart Grid. This is because a loss of availability is the disruption of access to or use of information, which may further undermine the power delivery.
- **Integrity:** Guarding against improper information modification or destruction is to ensure information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information and can further induce incorrect decision regarding power management.
- **Confidentiality:** Preserving authorized restrictions on information access and disclosure is mainly to protect personal privacy and proprietary information. This is in particular necessary to prevent unauthorized disclosure of information that is not open to the public and individuals.

From the perspective of system reliability, availability and integrity are the most important security objectives in the Smart Grid. Confidentiality is the least critical for system reliability; however, it is becoming more important, particularly in systems involving interactions with customers, such as demand response and AMI networks.

3.2. Cyber Security Requirements

Availability, integrity, and confidentiality are three high-level cyber security objectives for the Smart Grid. In addition to such high-level objectives, the NIST report [29] also recommends specific security requirements for the Smart Grid, including both cyber security and physical security. Specifically, the cyber security part specifies detailed security issues and requirements related to Smart Grid information and network systems; and the physical security part specifies requirements pertaining to physical equipment and environment protection as well as employee and staff security policies. As we are interested in security for information and network systems in this survey, we summarize in the following cyber security requirements for the Smart Grid [29].

- **Attack detection and resilience operations.** Compared with legacy power systems, the Smart Grid features a relatively open communication network over large geographical areas. Accordingly, it is almost impossible to ensure every part or node in the Smart Grid to be invulnerable to network attacks. Therefore, the communication network needs to consistently perform profiling, testing and comparison to monitor network traffic status such as to detect and identify abnormal incidents due to attacks. Moreover, the network must also have the self-healing ability to continue network operations in the presence of attacks. Due to the critical importance of power infrastructures, resilience operation in communication networks is essential to sustaining network availability in the Smart Grid.

- **Identification, authentication and access control.** The Smart Grid network infrastructure incorporates millions of electronic devices and users. Identification and authentication is the key process of verifying the identity of a device or user as a prerequisite for granting access to resources in the Smart Grid information system. The focus of access control is to ensure that resources are accessed only by the appropriate personnel that are correctly identified. Strict access control must be enforced to prevent unauthorized users from accessing sensitive information and controlling critical infrastructures. To meet these requirements, every node in the Smart Grid must have at least basic cryptographic functions, such as symmetric and asymmetric cryptographic primitives, to perform data encryption and authentication.
- **Secure and efficient communication protocols.** Differing from conventional networks, message delivery requires both time-criticality and security in the Smart Grid, in particular in distribution and transmission systems. The two objectives, however, usually contradict with each other. As networks (or sub-networks) in the Smart Grid cannot always use secure, physically-protected and high-bandwidth communication channels, optimal tradeoffs are required to balance *communication efficiency* and *information security* in the design of communications protocols and architectures for the Smart Grid.

Table 3 summarizes the cyber security requirements for the Smart Grid in comparison with those for the Internet. Note from Table 3 that the Smart Grid imposes much more strict security requirements than the Internet in order to fully achieve efficient and secure information delivery for critical power infrastructures. These security requirements for communication networks, together with those for system operation policies and physical infrastructures [29], will empower the Smart Grid with comprehensive security capabilities to fulfill the goal of “Energy Internet”.

4. Network Security Threats in the Smart Grid

As security challenges mainly come from malicious cyber attacks via communication networks, it is essential to understand potential vulnerabilities in the Smart Grid under network attacks. In this section, we provide an overview of network attacks towards the Smart Grid. We first classify network attacks into general classes, then analyze their potential threats in the Smart Grid via use case studies, and finally summarize research challenges.

4.1. Attack Classification

In communication networks, security attacks can be classified into two types: selfish misbehaving users and malicious users. Selfish misbehaving users are those attempting to obtain more network resources than legitimate users by violating communication protocols [32–34].

Table 3: Comparison of security requirements between the Smart Grid and the Internet

Security Functions	Smart Grid Communication Network	The Internet
Authentication and access control	Strictly enforced for all communication flows throughout the system	Mostly free end-to-end without access control
Attack detection and countermeasures	Essential and widely-deployed everywhere	Mainly for critical routers and servers
Every node	Basic cryptographic functions	No specification
Security for network protocols	From MAC-layer to application-layer security	From network-layer to application-layer security

In contrast, malicious users have no intent to benefit for their own; however, they aim to illegally acquire, modify or disrupt information in the network. Accordingly, both selfish and malicious users pose challenging security problems to communication networks.

In the Smart Grid, however, malicious behavior is a more concerned issue than selfish misbehavior, as millions of electronic computing devices are used for monitoring and control purposes instead of providing data services such as file downloading and sharing [29]. Thus, malicious attacks may induce catastrophic damage to power supplies and widespread power outage, which is a definitely forbidden case in the Smart Grid. As enumerating all possible attacks in the Smart Grid is not practical due to its large-scale and system complexity, we consider malicious attacks as three types based on the Smart Grid security objectives, that is, availability, integrity and confidentiality, as shown in Fig 2.

- Attacks targeting availability, also called denial-of-service (DoS) attacks, attempt to delay, block or corrupt the communication in the Smart Grid.
- Attacks targeting integrity aim at deliberately and illegally modifying or disrupting data exchange in the Smart Grid.
- Attacks targeting confidentiality intend to acquire unauthorized information from network resources in the Smart Grid.

Recently, research efforts have been focused on studying DoS attacks as well as attacks targeting integrity and confidentiality in power systems [35–43]. In what follows, we present a review of these attacks against communication networks in the Smart Grid.

4.1.1. Denial-of-Service Attacks

As a primary security goal of Smart Grid operations is *availability*, we first investigate network vulnerabilities in the Smart Grid under DoS attacks, which can severely degrade the communication performance and further impair the operation of electronic devices.

In general, existing DoS attacks can happen at a variety of communication layers in the Smart Grid, which are shown in Table 4.

Table 4: Denial-of-service attacks in power systems.

Communication layer	Attacks in power systems
Application layer	-
Network/ Transport layer	Traffic flooding [35] Buffer flooding [36]
MAC layer	ARP spoofing [37]
Physical layer	Jamming in substations [38]

- Physical layer. Channel jamming (e.g., [44–46]) is one of the most efficient ways to launch physical-layer DoS attacks, especially for wireless communications. Since intruders only need to connect to communication channels rather than authenticated networks, it is very easy for them to launch DoS attacks at the physical layer. In the Smart Grid, as wireless technologies will be widely used in local-area systems [5–7, 17, 18], wireless jamming becomes the primary physical-layer attack in such networks. A recent work [38] has showed that jamming attacks can lead to a wide range of damages to the network performance of power substation systems, from delayed delivery of time-critical messages to complete denial-of-service.
- MAC layer. MAC layer is responsible for reliable point-to-point communication as well as fairness. An attacker (e.g., a compromised device) may deliberately modify its MAC parameters (e.g., backoff parameters [32, 33]) to have better opportunities in accessing the network at the cost of performance degradation of others that are sharing the same communication channel. Therefore, MAC layer misbehavior can lead to a weak version of DoS attacks. In the Smart Grid, spoofing is a relatively harmful threat at the MAC layer because it targets both availability and integrity. A spoofing attacker, by taking advantage of the openness of the address fields in a MAC frame, can masquerade itself as another device to send fake information to other devices. For example, in a power substation network, a malicious node can broadcast forged address resolution protocol (ARP) packets to shut down connections of all IEDs to the substation gateway node [37].
- Network and transport layers. According to the

TCP/IP protocol model, these two layers need to provide reliability control for information delivery over multi-hop communication networks. DoS attacks at both layers can severely degrade the end-to-end communication performance, such as distributed traffic flooding and worm propagation attacks on the Internet [47–49]. Recently, few studies [35, 36] have evaluated the impact of network/transport-layer DoS attacks on the network performance of power systems. For example, a recent study investigated the impact of a buffer-flooding attack on the DNP3-based SCADA network with real SCADA system hardware and software, and showed that current SCADA system is quite vulnerable to the DoS attack [36].

- Application layer. Lower layer attacks focus mainly on transmission bandwidth in communication channels, computers or routers. Application-layer DoS attacks, however, intend to exhaust resources of a computer, such as CPU or I/O bandwidth. As shown in [50], application layer attacks can easily overwhelm a computer with limited computing resources by flooding computationally intensive requests. As millions of computing and communication devices in the Smart Grid are equipped with limited computational abilities, they can be potential victims of application-layer DoS attacks.

Note that compared with the Internet, the Smart Grid features a *delay-constrained* network because of stringent delay requirements of information or control messages to be delivered for the power systems (e.g., IEC 61850 messages in Table 2). In the Smart Grid, a DoS attacker does not need to completely shut down network access by using some extreme means (e.g., all-time jamming) but instead it may launch weaker versions of attacks to intentionally delay the transmission of a time-critical message to violate its timing requirement. This can also be catastrophic for power infrastructures. For instance, an attacker can cause severe damages to power equipments if it successfully delays the transmission of a protection message in the case of trip protection in substations [11]. Therefore, the goals of DoS attacks in the Smart Grid include not only disrupting the resource access but also violating the timing requirements of critical message exchange.

4.1.2. Attacks Targeting Integrity and Confidentiality

Different from DoS attacks that can be launched at various layers, attacks targeting integrity and confidentiality in general occur at the application layer, since they attempt to acquire or manipulate data information in the Smart Grid.

Attacks targeting data integrity can be considered less brute-force yet more sophisticated than DoS attacks. Such attacks attempt to stealthily modify data in order to corrupt critical information exchange in the Smart Grid. The target can be either customers’ information (e.g., pricing

Table 5: Classification of false data injection attacks against power systems.

Targeted Systems	Impact	References
DC SCADA	Invalid state estimation	[39–41, 43]
AC SCADA	Invalid state estimation	[42, 52, 59]
Electric market	Potential financial losses	[57, 58]

information and account balance) or status values of power systems (e.g., voltage readings and device running status). Because such information in power systems is valuable to both end users and utility companies, fault-tolerant and integrity-check methods are deployed in power systems to protect data integrity [51]. However, the risk of integrity attacks is indeed real. Recently, the false data injection attack against power grids, which was discovered and designed in [39], have drawn increasing attention in the research community. The false data injection attack was initially designed to impact the state estimation for the SCADA system. Based on the assumption that an attacker has already compromised one or several meters, the work in [39] pointed out that the attacker can successfully inject falsified data to the SCADA center, and at the same time pass the data integrity check used in current state estimation process. Since the introduction of false data injection attacks, considerable research efforts [40–43] have been conducted in providing analysis and countermeasures of such attacks for SCADA systems.

There are a line of continued works targeting constructing and counterattacking new classes of false data injection attacks [52–57]. For instance, false data injection attacks have been extended to the electric market [58] to deliberately manipulate the market price information. This could result in significant financial losses to the social welfare. The load redistribution attack [59] is another special type of false data injection attacks, in which only load bus injection measurements and line power flow measurements are attackable. The work in [59] shows that such attacks are realistic false data injection attacks with limited access to specific meters. To sum up, research on false data injection attacks has become an active and challenging field in Smart Grid security. Table 5 classifies existing false data injection attacks and their associated impacts on the Smart Grid domains.

Compared with attackers targeting integrity, attackers targeting confidentiality have no intent to modify information transmitted over power networks. They eavesdrop on communication channels in power networks to acquire desired information, such as a customer’s account number and electricity usage. Typical examples include wiretappers [60] and traffic analyzers [61]. Such attacks can be considered to have negligible effects on the functionality of communication networks in the Smart Grid. However, with the increasing awareness and importance of customer privacy, the social impacts due to confidentiality attacks have received more and more attentions in recent years,

especially the potential leakage of massive customer information.

There is also a new line of recent work on attacks targeting privacy: using information theory to model the dynamic communication and control process in the Smart Grid. The work in [62] theoretically studies from the information theory perspective the communication capacity in a dynamic power system under an eavesdropper targeting confidentiality. The work of [63] proposes the concept of competitive privacy and uses an information-theoretic approach to model the intriguing privacy issues in the Smart Grid information and communication infrastructures.

It is worthy of noting that the premise to launch attacks against integrity and confidentiality is that attackers can be authenticated to the communication networks or the grid, and have the access to sensitive information. Hence, authentication and access control are also essential to preventing the Smart Grid from such attacks.

4.2. Smart Grid Use Cases with Critical Security Requirements

In reviewing cyber security attacks in power grids, we observe that existing work focuses on either power substation systems [37, 38, 64] or SCADA systems [35, 36, 39–43]. However, communication scenarios in the Smart Grid are not limited in these two networks, such as PMU synchronization in the wide-area measurement network and meter reading in the AMI network. To facilitate research on the Smart Grid security, the NIST report [29] recommends a series of key use cases for security consideration. Based on these cases, in the following we provide a comprehensive analysis of network vulnerabilities in the Smart Grid.

First, we summarize the use cases with critical security requirements into two independent classes: 1) distribution and transmission operation in which communication is time-critical for monitoring, control, and protection; 2) AMI and home-area networks in which communication is primarily for interactions between customers and utilities. We then discuss potential network security threats in the two classes, respectively.

4.2.1. Distribution and Transmission Operation

Power distribution and transmission operation systems are vital components in power systems, since they are responsible for reliable power delivery between generators and customers. There are millions of critical power equipments used for monitoring and control purposes; these devices are inter-connected with the SCADA sever for centralized management [14]. According to [29], availability and integrity are crucial for such systems, whereas data confidentiality is less important because there is no customers' private information involved. Next, we consider three key use cases with critical requirements of availability and integrity, as shown in Fig. 3 and Table 6. Note that the three use cases also include major information flows in

power distribution and transmission systems. In the following, we describe several communication scenarios and analyze potential security vulnerabilities in each use case.

The first scenario is referred to as *Case 1*, which represents local management in a power substation. A power substation network is a single-hop network, consisting of a substation computer that serves as the gateway to outside networks, and tens of IEDs that consistently monitor all feeder equipments to ensure reliable operation in the substation. Local protection procedures will be triggered by IED-to-IED (peer-to-peer) communications once an abnormal status is detected [24]. For legacy power systems, serial-port (e.g., RS232) based DNP3 is widely used for communications between power devices. In contrast, for the Smart Grid, Ethernet based IEC 61850 [22] has been already adopted in substations for efficient information exchange. In addition, the use of wireless communications (e.g., WiFi) is also proposed for power substation communication [38, 65]. Thus, a power substation network in *Case 1* can be considered as (wireless) local area network (LAN) with critical timing requirements as defined in Table 2. The potential cyber attacks are defined as follows:

- DoS attacks: As IEC 61850 is based on Ethernet and TCP/IP [22], IEDs in a substation can become targets of DoS attacks, such as traffic-flooding and TCP SYN attacks. However, local DoS attacks launched by compromised IEDs are limited in scale and may not lead to significant impacts on the communication performance, since there are limited number (tens) of IEDs in a power substation [24]. Therefore, the threat of large-scale DoS attacks that overwhelm a substation network is mainly from the outside of a substation. In this regard, the substation computer (the network gateway of the substation) becomes the primary target of TCP/IP DoS attacks. In other words, substation gateways must enforce strong access control and filtering policies for incoming communication flows. Furthermore, when wireless technologies are adopted in a substation, jamming attacks may become a primary security threat. Therefore, anti-jamming technologies need to be used to protect wireless communication in substations.
- Attacks targeting integrity: In this single-hop network, spoofing attacks can lead to loss of both availability and integrity. In particular, spoofing attacks targeting the protection system should be a primary focus. For example, switches are used to protect power infrastructures in substations, when an IED detects an abnormal status (e.g. high current), it will send close/open messages to switches to balance the power load (or simply break the circuit for protection) [66]. If a spoofing attacker successfully masquerades itself as a monitoring IED, it could send false close/open messages to switches and lead the protection system to a mess-up status, resulting in potential loss of power supply for customers. Therefore, strong

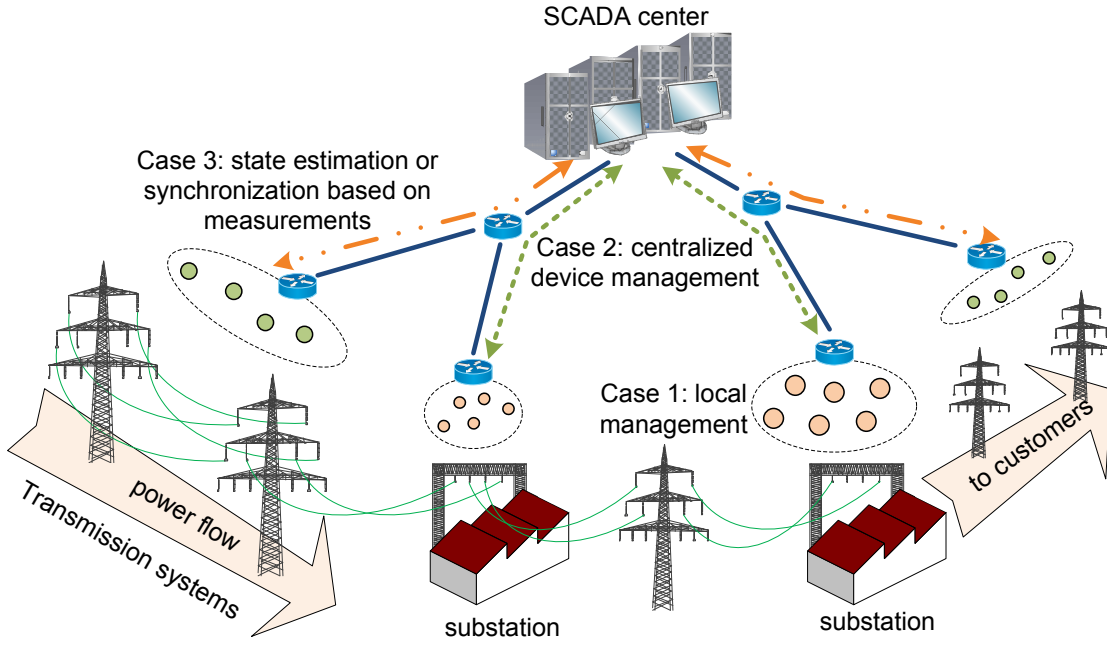


Figure 3: Key use cases in distribution and transmission systems in the Smart Grid.

Table 6: Key use cases with critical security requirements in distribution and transmission systems.

No.	Network	Information Delivery	Brief Description
1	Power substation networks	Single-hop, peer-to-peer	Local monitoring, control, and protection of power equipments and devices in substations.
2	SCADA and wide-area power systems	Multi-hop, hierarchical	Centralized monitoring and control of power equipments at the SCADA center.
3	SCADA and wide-area power systems	Multi-hop, hierarchical	State estimation or synchronization based on measurements from raw data samples (e.g., from PMUs).

point-to-point authentication schemes should be enforced to prevent such spoofing attacks in substations.

The second scenario, referred to as *Case 2*, is about monitoring, control and protection, which are not limited in local-area systems. In this process, electronic device status and readings in local-area systems can also be delivered to the SCADA center for centralized management. As shown in Fig. 3, *Case 2* features a conventional server-and-clients communication model in a multi-hop and hierarchical network, which is similar to the Internet and sensor networks. Therefore, network attacks are serious security threats to the Smart Grid in *Case 2* as they are in conventional communication networks:

- DoS attacks: As the SCADA center serves as the *sink node* to which data packets are delivered, it becomes a primary target of distributed DoS (DDoS) attacks that can be launched from various local-area systems. Accordingly, the SCADA center can leverage existing DDoS attack defense strategies to countermeasure potential DDoS attacks.
- Attacks targeting integrity: As *Case 2* features a conventional end-to-end communication model, the com-

munication between power devices at local-area networks and the SCADA center should be protected by end-to-end authentication schemes to prevent substations from integrity attacks, such as relay or man-in-the-middle attacks in which an attacker attempts to serve as an intermediate node between two nodes to inject falsified data during communication.

The last scenario is referred to as *Case 3* shown in Fig. 3, which represents a multi-hop and hierarchical communication network, where raw data samples of power signals are delivered from local-area systems to the SCADA center to perform state estimation. *Case 3* appears to be very similar to *Case 2* because they share the same network architecture. However, *Case 3* features collecting correlated data samples from local-area systems in order to construct a global snapshot of power signal quality at a particular time instant. The difference is that in *Case 3*, all correlated data samples from different areas must arrive within a specific time interval, which is not required in *Case 2*. For example, in a wide-area measurement network, a PMU is used to accurately sample the power signal at an instant known as the time tag, then transmit the sample

with the time tag to the SCADA center or the phasor data concentrator (PDC) [67]. All samples with the same time tag must be collected in a timely manner to estimate the power signal quality for a certain time instant, which is called synchronization. Depending on applications, the frequency of synchronization is usually 15–60 Hz [67], leading to delay requirements of tens of milliseconds for PMU data delivery. This means that all correlated samples with the same time tag must arrive within the interval of tens of milliseconds, which induces different security vulnerabilities from *Case 2*.

- DoS attacks: Similar to *Case 2*, data collection and aggregation in *Case 3* is also vulnerable to DDoS attacks. Furthermore, the SCADA center may not be the primary target in this case; attackers can target local-area networks and launch relatively small-scale DoS attacks to delay or block data delivery from those systems. Since state estimation can be performed only when all data is sufficiently collected from local-area systems [39, 43], such small-scale DoS attacks can result in partial unavailability of data samples for state estimation. Accordingly, the SCADA center cannot gather correct, global information of the power flow status from partial data samples. To prevent such attacks, countermeasures must be deployed in all local-area systems to ensure data delivery in a timely manner for reliable state estimation.
- Attack targeting integrity: The correlation between sampled raw data from different locations, in fact, increases the difficulty for attackers to falsify power status information to the SCADA center. Independent tamper of data or samples can easily be identified by the data-integrity detector at the SCADA center [39]. Thus, attackers may cooperate with each other in order to successfully launch attacks targeting data integrity. For example, with the knowledge of a power system topology, false data injection attackers (or further, unobservable attackers) against power state estimation have to compromise a number of sensors to inject falsified information to the SCADA center, while passing data integrity check at the same time [39, 41–43]. Therefore, it is challenging for attackers to work cooperatively to corrupt data integrity. However, once a coordinated attack is successfully launched, it can bypass conventional bad-data detectors and stealthily result in devastating impacts on power system operations. Thus, it is also challenging to design countermeasures to detect and counter-react such attacks.

4.2.2. Advanced Metering Infrastructure and Home-Area Networks

In the above, we have analyzed potential security threats of three key use cases in distribution and transmission systems. Here, we move on to the key use cases related to the

AMI and home-area networks, which are also integral parts of the Smart Grid.

The AMI system is an essential system in the Smart Grid because it deploys communication networks to connect each customer’s home-area network with utility companies, and consistently interacts with smart meters in home-area networks for scheduled energy management or demand/request response in customers’ homes. The NIST report [29] has recommended over ten use cases relating to the AMI system, from which we focus on two key use cases that demand for critical integrity and confidentiality, as shown in Fig. 4 and Table 7.

The information exchange between smart meters and the utility center, such as metering reading and maintenance is represented by *Case 4* in Fig. 4; while *Case 5* illustrates the interactions between smart meters and electric market, such as real-time pricing and demand response. Both cases feature a multi-hop and hierarchical communication network. Differing from stringent timing requirements in distribution and transmission networks, the message latency in both cases (e.g., metering reading and market price broadcasting) varies from minutes to hours [29]. As a result, although availability is important to provide network access for end users, data integrity and confidentiality are more critical in the AMI network than substation automation systems due to a large amount of sensitive information, including customer’s account number and balance.

Because of the highly-distributed nature of the AMI network, it is expected that wireless technologies are to be used for efficient and low-cost deployment. For example, Austin Energy has installed a wireless mesh network to enable the two-way communication between the utility center and smart meters [68]. The openness of the wireless communication medium can further expose information exchange to attackers targeting data integrity and confidentiality. In both *Case 4* and *Case 5*, potential security threats that can lead to significant impacts on the AMI infrastructure and system operation are detailed as follows:

- Eavesdroppers and traffic analyzers. By eavesdropping on wireless communication channels, an attacker at a home-area network could possibly gain private information even if the information was encrypted [29]. Therefore, strong data encryption and secret key management schemes must be enforced for any communication in the AMI network to prevent attacks from deducing the secret key out of a large amount of network data samples.
- Attacks targeting integrity. Since both *Case 4* and *Case 5* are dominated by non-time critical traffic, similar to the Internet and data collection in sensor networks, conventional relay or man-in-the-middle attacks can be possibly launched in the AMI network to inject falsified data during the communication pro-

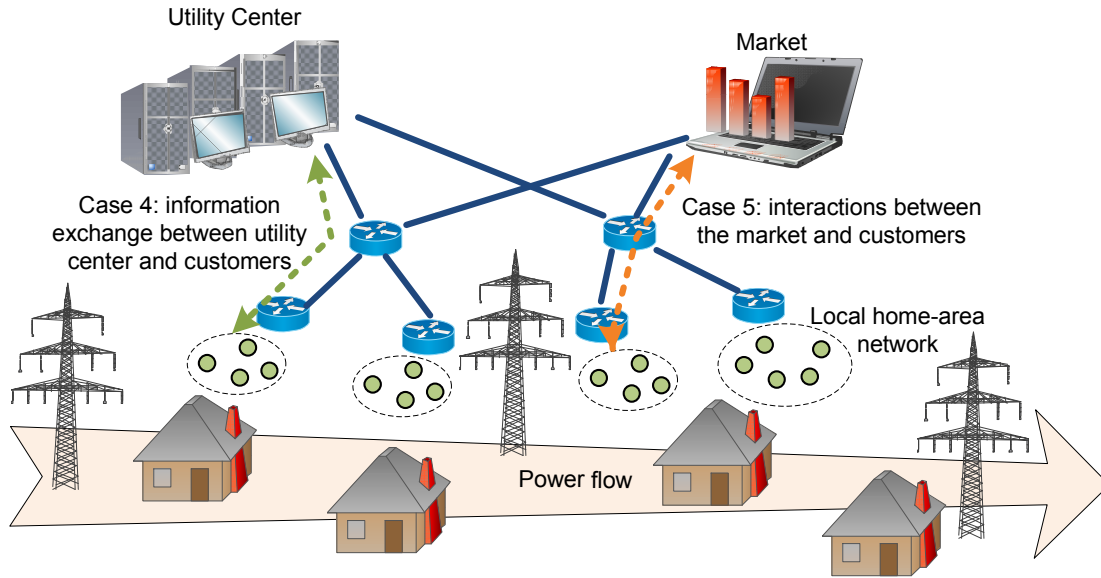


Figure 4: Key use cases in the AMI and home-area networks.

Table 7: Key use cases with critical security requirements in the AMI system.

No.	Network	Network Type	Brief Description
4	AMI and home-area networks	Multi-hop, hierarchical	Information exchange between customers and the utility center (e.g., meter reading service).
5	Demand response and home-area networks	Multi-hop, hierarchical	Interactions between customers and the market (e.g., customers respond to real-time electricity prices).

cess. To this end, end-to-end encryption and authentication schemes are required to eliminate such attacks in the AMI network. Moreover, protection of data integrity in these two cases must also include non-repudiation to prevent customers from denying their financial behaviors [29].

- DoS attacks. As shown in Fig. 4, *Case 4* features top-down and bottom-up communication models between the utility center and customers, which is exactly similar to conventional node-sink communication model in the sensor networks. Thus, conventional DoS attacks (e.g., [17, 69, 70]) in sensor networks can be also potential threats in *Case 4*. Moreover, for *Case 5*, there is more important real-time price information exchanged in the AMI network. Such information is vital to fulfill the demand response functionality in *Case 5*, thereby becoming the potential target of DoS attacks. In fact, a recent work in [71] has already pointed out that attackers can focus on jamming real-time price signals transmitted in wireless home-area networks to effectively result in denial-of-service and dysfunction of the entire demand respond system.

4.3. Summary and Research Challenges

Based on aforementioned description, we have identified two important use cases in the Smart Grid systems: 1)

the distribution and transmission system and 2) the AMI system. The main differences between the two systems with respect to communication and security requirements are summarized in Table 8.

- The distribution and transmission system in general features more time-critical yet less confidential communications. There are three important scenarios (as shown in Table 6) in substation and SCADA systems with distinct communication requirements and security vulnerabilities. In addition, critical timing requirements further limit the use of strong, but time-consuming security solutions (e.g., public key based communication) in such a system.
- The AMI network is used to connect customers' homes, the utility center and the electricity market. In the AMI network, message delivery becomes non-time critical, and availability is less important than integrity and confidentiality. Thus, network security solutions for the AMI network should focus primarily on providing integrity and confidentiality, and can also leverage existing solutions for the Internet and sensor networks.

Based on the discussion of vulnerabilities in the Smart Grid, we in the following summarize research challenges regarding the analysis and evaluation of cyber security

Table 8: Comparison between the distribution and transmission system and the AMI networks.

System	Communication Methods	Timing Requirements	Security Objectives
Power distribution and transmission	Single-/multi-hop communications, peer-to-peer	Milliseconds to seconds	Critical availability and integrity
Advanced metering infrastructure	Multi-hop, hierarchical networking	Minutes to hours	Critical integrity and confidentiality

threats. In particular, we focus on the DoS attacks because they have an immediate impact on the availability, which is arguably the most important security requirement of power distribution and transmission [3].

4.3.1. Modeling the Impact of Denial-of-Service Attacks in Distribution and Transmission Systems

For conventional communication networks, because of the packet-switched network architecture for TCP/IP, the literature in general modeled the impact of DoS attacks at the packet level (e.g., packet loss [72] and the number of corrupted packets [69]) or at the network level (e.g., network throughput [73]).

In power distribution and transmission networks, however, data messages are time-critical with application-layer delay constraints in a wide range, from milliseconds (e.g., in Cases 1 and 3) to seconds. Conventional packet-level or network-level metrics do not directly reveal the performance measurements at the application-layer, especially the delay constraints of such time-critical messages. Even though end-to-end delay was studied extensively in communication networks, the majority of results are on asymptotic bounds for large-scale networks at the network layer for non-real-time or non-time-sensitive applications. For example, if a DoS attacker can induce 5 ms delay for most traffic in a power substation, it will be considered devastating for Type-1A/P1 messages (3 ms limit) but benign for Type-1A/P2 messages (10 ms limit) as shown in Table 2. Consequently, for power distribution and transmission systems, *message-oriented* metrics, which not only characterize the end-to-end message delay but also reflect the delay constraint, should be properly defined to model the impact of DoS attacks on the network performance.

4.3.2. Risk Assessment of Large-Scale DoS Attacks

According to our case studies in the previous section, it is evident that DoS attacks are crucial security threats to communication networks in the Smart Grid. Historic events have also showed that large-scale DoS attacks, including DDoS attacks [74, 75] and worm attacks [76], can significantly deteriorate the Internet performance. For example, the Morris worm, disrupted about 10% of the computers on the Internet in 1988 [76].

Thus, large-scale DoS attacks, if successfully launched, will lead to severe network performance degradation in the Smart Grid. On the other hand, the Smart Grid is a complex cyber-physical system, including not only communication networks but also power infrastructures. Hence,

it is also important to understand what is the impact of large-scale DoS attacks on power facilities in the Smart Grid because a series of actions on power devices may be triggered by following up control and monitoring messages. Accomplishing such an ambitious objective requires a joint risk assessment on communication and power infrastructures. Toward this challenge, there have been several risk assessment methods proposed for power systems, including probabilistic, graph based, and security metric based methods. To name a few, we have

- Probabilistic risk assessment. Vulnerability assessment methods based on the probabilistic risk assessment (PRA) for power control systems are proposed in [77–79]. In PRA, The security levels are calculated by the probabilities of occurrence of cyber security events, the probabilities of incidents caused by the events, and the related power loss. These probabilities are obtained by statistical samples and history events. Thus, PRA can provide a quantitative impact evaluation of power systems under malicious attacks.
- Graph based assessment. One of the drawbacks of PRA is the difficulty to identify the probabilities for potential security incidents that do not exist in history database. Therefore, graph-based assessment is proposed to model attack impact on power networks [80–82]. This solution defines general relations between attack goals, consequences, and defense strategies into a graph and uses decision-making mechanisms to assess the impact and possibility of attacks against power networks. For example, the work in [80] introduces an attack graph that represents a collection of possible intrusion scenarios in a computer network and uses multiple criteria decision-making (MCDM) to provide a complete methodology of security assessment for communication networks of power control systems.
- Security metric based assessment. A recent work [83] proposes a scheme for auditing the security of a substation network based upon a security metric for IEDs. In this approach, a score is assigned to each IED based on prior identification of all known threats to the IED and the availability of their countermeasures. Then, the security metric for the substation can be computed based on the scores of all IEDs.

However, it is quite difficult for PRA to estimate the probability of potential large-scale DoS attacks against the

Smart Grid, as there is no historic data for profiling and it is also very likely that different DoS attacks may present different priorities across the system. On the other hand, graph-based and security-metric based methods currently both have scalability issues and are limited in small-scale power networks (e.g., a substation network). Further, the most challenging issue with these solutions is that none of them is able to demonstrate to what extent a DoS attack would undermine the power system with respect to time-critical messages. For example, even though we are able to decide what devices could be affected due to an attack by using graph-based measurements, it is impossible to find out whether such an attack would delay a fault detection or diagnosis message and hence it is unable to determine the subsequent effect. Therefore, existing analytical frameworks are incapable of providing an accurate risk assessment of large-scale DoS attacks against the Smart Grid. Our understanding of modeling and evaluation of security impact in the Smart Grid is quite limited, e.g., how likely large-scale DoS attacks can be launched against the Smart Grid and how can they affect power infrastructures. Accurate risk assessment of such attacks remains as a challenging issue.

5. Network Countermeasures for the Smart Grid

Due to the cyber-physical system nature of the Smart Grid and the great impact of energy systems, a primary security objective for Smart Grid operation is *availability* [3], DoS attacks which have an immediate impact on the availability of communication systems and control systems become the primary network security threats in the Smart Grid. Detection and defense of DoS attacks depend highly on network countermeasures, such as network traffic monitoring and filtering. Thus, it is essential to providing effective network approaches against DoS attacks. In this section, we first examine the status of applying existing countermeasures against DoS attacks to the Smart Grid, and then discuss potential issues that may not be solved in current solutions.

5.1. Attack Detection for Power Networks

Because of the interaction of information networks and electric devices in energy systems, the Smart Grid must be able detect and counteract DoS attacks that may be launched anywhere in communication networks. Attack detection is the first step towards providing countermeasures against these attacks. To summarize, existing DoS attack detection can be categorized into several schemes, as shown in Fig. 5.

- Signal-based detection. At the physical or MAC layer, a DoS attack detector can measure the received signal strength information (RSSI) to detect the presence of an attack (e.g. wireless jamming [72, 84–86]): if the RSSI of many packets is larger than a threshold (which means the receiver should correctly receive

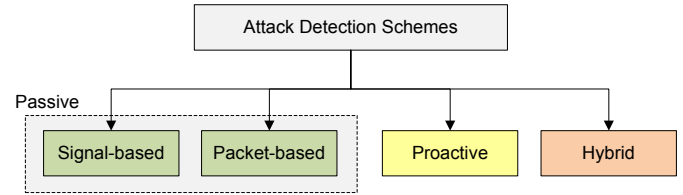


Figure 5: Classification of DoS attack detection schemes.

them) but the packet decoder outputs errors, the attack detector can raise an alarm of the presence of an attacker.

- Packet-based detection. The solutions falling into this category (e.g., [69, 87, 88]) can be implemented at every layer to measure the transmission result of each packet and discover potential attacks by identifying a significant increase of packet transmission failures. The packet-based detection is a general and effective detection scheme since DoS attacks can always lead to network performance degradation in terms of packet loss or delay.
- Proactive method. The main idea is to design algorithms that (e.g., [89, 90]) attempt to identify DoS attacks at the early stage by proactively sending probing packets to test or measure the status of potential attackers.
- Hybrid method. It is also likely to design one scheme that combines different ideas to improve attack detection accuracy. For example, the work in [72] proposed to use both signal-based and packet-based detection to effectively identify jamming attacks in wireless networks.

Most DoS attack detection methods belong to passive detection that keeps monitoring the network status, such as traffic load and packet transmission ratio, and raises an attack alarm once there is an evident mismatch between new samples and historical data. As such, existing methodology for DoS attack detection can be directly applied to communication networks in the Smart Grid. For example, signal-based detectors can be easily deployed in wireless Smart Grid applications (e.g., wireless monitoring for transformers [91]); and packet-based methods are suitable for general DoS attack detection in AMI networks and substations [37].

Table 9: Potential uses and applications of existing attack detection methods for the Smart Grid.

Scheme	Potential Use	Existing Application
Packet-based	wide applications	substation [37]
Signal-based	wireless applications	-
Proactive	limited	-

Table 9 summarizes the potential uses and existing applications of DoS attack detection methods for the Smart

Grid. As the packet-based method measures the packet delivery/loss ratios to detect the presence of attacks, it can be regarded as a general network approach with wide applications to the Smart Grid. For instance, a packet-based attack detection system is proposed recently in [37] to discover security threats in an IEC61850-based power substation network. Signal-based methods are applicable to wireless networks in the Smart Grid. Note that proactive methods may be limited in non-time critical networks, since they unavoidably introduce communication overhead by transmitting probing packets.

5.2. Applications of Attack Mitigation Mechanisms to Power Networks

Along with the detection schemes for DoS attacks, attack mitigation mechanisms can be deployed to prevent network nodes from DoS attacks. In the literature, DoS attack mitigation schemes mainly include two lines of work: 1) network-layer mitigation for DDoS attacks with intent to exhaust a target's resources, and 2) physical-layer mitigation for jamming attacks with intent to disrupt any wireless communications. In the following, we will discuss their applications to the Smart Grid one by one.

5.2.1. Network-Layer Mitigation

The most widely used approaches for mitigating DoS attacks are designed for the network layer and many of them have been demonstrated to be effective for the Internet. For example, the following mechanisms are discussed extensively [49]:

- **Rate-limiting.** The basic idea of rate-limiting mechanisms is to impose a rate limit on a set of packets that have been characterized as possibly malicious by the detection mechanism. It is usually deployed when the detection mechanism has many false positives or cannot precisely characterize the attack stream.
- **Filtering.** Corroborating with attack detection methods, filtering mechanisms can compare the source addresses of packets with the blacklist provided by attack detectors to filter out all suspicious flows. As such, packets from attackers will not be further forwarded or routed to victims.
- **Reconfiguration.** In order to mitigate the impact of DoS attacks, one solution is to reconfigure network architecture, such as changing the topology of the victim or the intermediate network to either add more resources to the victim or to isolate the attack machines.

Compared with the Internet that allows arbitrary end-to-end communication flows, the Smart Grid features two major predictable directional information flows: bottom-up and top-down (e.g., Cases 2-5 in Section 4). This in fact makes it easy for gateway and router softwares to perform rate-limiting and filtering mechanisms to block undesired

or suspicious traffic flows. For example, Table 10 shows the typical data transmission frequencies and directions for different power applications. From Table 10, it is easy for network operators to predefine the rate-limiting and filtering policies for communication flows of power applications to prevent DoS attacks in the Smart Grid.

Table 10: Typical data transmission frequencies for power applications.

Typical data in power applications	Transmission frequency	Information direction
Raw data samples in substation IEDs	960, 1920, 4800 Hz[24]	Peer-to-peer (IED-to-IED)
PMU samples in wide-area systems	12 - 60 Hz [67]	Bottom-up (data collection)
Samples for SCADA state estimation	0.25 - 0.5 Hz [41]	Bottom-up (data collection)
Metering reporting in AMI	Smaller than 1 Hz [29]	Bottom-up (data collection)
Real-time pricing in demand response	Smaller than 1 Hz [29]	Top-down (broadcasting)

However, it may not be easy to use reconfiguration mechanisms, since parts of the Smart Grid network are static due to the fixed topology of power distribution and transmission equipments.

5.2.2. Physical-Layer Mitigation

As wireless networks will be widely deployed in local-area systems in the Smart Grid, wireless jamming becomes the primary DoS attack in wireless based power networks, especially in some scenarios in distribution and transmission systems [25, 38, 65, 92]. Thus, jamming-resilient wireless communication becomes critical for Smart Grid applications to survive jamming attacks and maintain continuity of information delivery.

Recently, great progress has been made on the development of jamming-resilient schemes [44–46, 70, 93–95] for wireless networks. Such schemes can be designed in either coordinated or uncoordinated manner.

- **Coordinated protocols** are conventional anti-jamming transmission schemes that have already been explored in the area of wireless communications. They can be categorized as frequency hopping spread spectrum (FHSS), direct sequence spread spectrum (DSSS), and chirp spread spectrum (CSS) [96, 97]. However, the issue associated with coordinated protocols is that the secret, such as direct sequence in DSSS and hopping pattern in FHSS, is assumed confidential to others (e.g., attackers). Such an assumption is not valid for open communication standards, such as WiFi and cellular networks. Thus, coordinated protocols are vulnerable to intentional attacks with the knowledge of protocol information.
- **Uncoordinated protocols** [44, 46, 98] are promising for secure wireless communications in a distributed environment. Uncoordinated protocols do not need the

transmitter and the receiver to share a pre-known secret with each other. They randomly generate a secret (e.g., hopping pattern in FHSS) for each transmission and prevent attacks from acquiring sufficient knowledge to disrupt the communication. Conventional FHSS and DSSS have their uncoordinated counterparts UFHSS and UDSSS, respectively.

Both coordinated and uncoordinated protocols can be used in the Smart Grid to achieve anti-jamming wireless communications. Compared with coordinated protocols, uncoordinated protocols are more secure and resilient to intentional attacks as they do not share a pre-known secret between the transmitter and the receiver. However, the cost of uncoordinated protocols, on the other hand, is the delay performance since they need to negotiate a secret before initiating data communication.

Table 11: Delay performance of implementations of DoS attack resistant protocols. The delay performance is represented by the typical delay to transmit a 1000-bit message for each scheme.

Anti-Jamming Scheme	Hardware Platform	Bandwidth (Mbps)	Delay (Second)
UFHSS	USRP	1	1-2
UDSSS	USRP	1	10-32
UFH-UDSS	USRP	1	1-1000
DEEJAM	MICAz	0.25	0.434-1.002
TC	MICA2	0.012	117.4-186.6

Table 11 shows the delay performance of recently proposed jamming-resistant protocols based on different hardware platforms, including UFHSS [98], UDSSS [98], UFH-UDSS [98], DEEJAM [93] and Timing-channel (TC) [99]. We can see from Table 11 that existing implementations lead to second-level message delay to transmit a single 1000-bit message, which is indeed delay-inefficient. Table 11 implies that current schemes can be readily applied to wireless-based AMI and home-area networks whose communication traffic is non-time critical. Nevertheless, it is still unclear whether they can be efficiently used in distribution and transmission systems where millisecond-level communication performance is necessary.

5.3. Research Challenges and Open Questions

We have so far summarized the applications of network countermeasures against DoS attacks to the Smart Grid. We find that, in the Smart Grid context, packet-based detection schemes can be used to a broad range of applications in the Smart Grid; rate-limiting and filtering are very effective attack mitigation methods; and current anti-jamming communication schemes can be applied to the AMI and home-area networks. Besides the wide applications of existing approaches to the Smart Grid, there are still open issues summarized as follows.

5.3.1. Denial-of-Service Attack Detection for Distribution and Transmission Systems

As we have discussed, DoS attack detection for the Smart Grid may still be based on existing frameworks (e.g., packet-based, signal-based), which means security functions and algorithms would be equivalent to the information networks. Therefore, the research challenge mainly lies in the differences between packet transmission in data networks and message delivery in the Smart Grid. Through the careful examination of use cases in the Smart Grid, it is evident that the design of attack detection must be effective to time-critical distribution and transmission networks. Due to their importance, a DoS attack detector should yield a reliable output within a very short decision time to notify network operators of potential threats.

Existing methods usually adopt a “profile-then-detect” strategy: first profiling parameters [69, 72] or inferring statistical models [87, 88] from measured data, then detecting attacks based on the profiled knowledge. For example, a sequential jamming attack detector proposed in [69] needs to estimate the transmission failure probabilities in both non-jamming and jamming cases before performing jamming detection. However, such methods face several practical issues for distribution and transmission systems: (i) the first-profiling then-detecting process inevitably increases the detection time; (ii) it is unclear in practice how much reliability the profiling phase can provide for attack detection within different timing constraints.

Given the fact that traffic is predictable and has timing requirements in distribution and transmission systems, it is possible to combine the profiling and detection in one setup, i.e., using the “the profile-and-detect” strategy. In particular, profiling the data while applying traffic pattern and timing analysis could directly uncover suspicious traffic induced by attackers, making fast and effective attack detection feasible in distribution and transmission systems.

5.3.2. Jamming-Resilient and Delay-Efficient Wireless Communications

It is well-known that spread spectrum technologies combat interference and jamming attacks by introducing a large amount of communication overhead in wireless communications [96]. The second-level delay performance in Table 11 indicates that it is still unclear whether current jamming-resilient schemes can be directly used in power distribution and transmission systems with millisecond-level delay constraints. The reason behind the delay performance shown in Table 11 is two-fold: 1) hardware platforms used in existing schemes are incapable of achieving low-delay transmissions because of low bandwidth and limited computational ability; 2) current schemes focus more on jamming robustness and are not optimized in terms of delay efficiency. Consequently, both jamming-resilient and delay-efficient transmission schemes have to be designed to achieve secure communication in wireless based distribution and transmission systems.

6. Cryptographic Countermeasures for the Smart Grid

Network approaches are primary countermeasures to detect, mitigate and eliminate DoS attacks that actively lead to network traffic dynamics. However, they are much less effective to deal with attacks targeting integrity and confidentiality that cause negligible effect on the network performance. Cryptographic primitive based approaches become major countermeasures against such attacks. In this section, we first review existing work on three key topics on cryptographic countermeasures: encryption, authentication, and key management for power systems. Then, we summarize and present research challenges.

6.1. Encryption

Encryption is an elementary cryptographic method to achieve secure communication and information protection for any information system. In the Smart Grid, most electronic devices are expected to have at least basic cryptographic capabilities, including the ability to support symmetric ciphers (or public-key cryptography supported by low-cost hardware with embedded cryptography functionality [29]).

The design of encryption schemes is the essential mechanism to protect data confidentiality and integrity in the Smart Grid. As the Smart Grid communication network consists of millions of embedded computing systems with limited computational ability (e.g., IEDs and smart meters), computational efficiency becomes an important factor for an encryption scheme to be adopted in the Smart Grid. Thus, in this subsection, we will evaluate the applications of widely-used encryption algorithms to the Smart Grid using an IED-based experimental study.

6.1.1. Background

Encryption schemes can be based on symmetric key cryptography (e.g., AES, DES) or asymmetric key cryptography (e.g., RSA). Symmetric key cryptography uses the same key for encryption and decryption. Asymmetric or public key cryptography uses private and public keys to encrypt and decrypt, respectively. There are a lot of works in the literature [100–103] that have provided comprehensive comparisons in/between symmetric and asymmetric schemes for network protocol design. Generally speaking,

- Asymmetric key cryptography requires more computation resources than symmetric key cryptography for long key size (strong security). Thus, the use of asymmetric key encryption may be limited in embedded computing systems.
- Symmetric key cryptography requires approximately constant computational resources regardless of the key size; however, it requires secure exchange and update of secret keys among network nodes, thereby complicating the process of key management.

To see how the two distinct encryption schemes perform in power equipments, we provide in the following an experimental case study to quantitatively evaluate their computational efficiency on a practical IED for power substations.

6.1.2. Experimental Case Study based on Intelligent Electronic Device

The IED in our experiments is a communication module, called TS7250, connected to a solid-state transformer in the FREEDM center¹. The device is used for sending the transformer status and receiving commands from the control center. It is equipped with 200-MHz ARM9 CPU and 32-MB SD-RAM. We also implement the same cryptographic schemes on a laptop named LARCH with 1.6-GHz P4 CPU and 1-GB RAM to facilitate performance comparison.

Table 12 shows the comparison of computation times of encryption algorithms between TS7250 and LARCH. We can observe from Table 12 that TS7250 spends much more time than LARCH to perform the same encryption algorithm. The RSA encryption time increases much faster than the DES-CBC time as the key length increases. For example, when the RSA key length goes from 512 bits to 1024 bits, the signature time in the IED increases from 39.57 ms to 228.18 ms. The computation time even becomes second-level when the key length is larger than 2048 bits. Table 12 demonstrates that the computational ability of an IED indeed becomes a bottleneck for the delay performance especially when adopting asymmetric key cryptography.

Table 12: Benchmarking of encryption speed for symmetric and asymmetric schemes.

Host Name	Encryption Suits	Key Length (bytes)	Time (ms)
LARCH (Intel P4 1.66GHz, 1GB RAM)	DES-CBC	16	8.79
		64	8.17
		256	8.09
		1024	8.07
	RSA	512	0.83
		1024	3.83
		2048	21.17
		4096	32.82
TS7250 (200MHz ARM9, 32MB SDRAM)	DES-CBC	16	192.91
		64	185.69
		256	186.22
		1024	183.81
	RSA	512	39.57
		1024	228.18
		2048	1457.14
		4096	10080.00

¹<http://www.freedm.ncsu.edu/>

This case study shows via quantitative results that symmetric key cryptography is a better choice for real-time IED communications in power distribution and transmission systems. While asymmetric key cryptography (with long key size) has wide applications to protect customers' sensitive information in the AMI and home-area networks, where communication traffic is non-time critical.

6.2. Authentication

Authentication is a crucial identification process to eliminate attacks targeting data integrity. Intuitively, design of authentication for the Smart Grid can leverage existing authentication protocols in conventional networks, which have been extensively studied for decades. However, it is pointed out in [104] that the authentication design process is prone to significant errors if adequate care is not taken for power systems. Consequently, in this subsection, we first present the basic requirements for authentication protocol design in the Smart Grid, then classify existing authentication protocols for power systems. Finally, we use a case study in a small-scale substation network to compare existing protocols, and identify research challenges.

6.2.1. Basic Requirements in the Smart Grid

An authentication protocol for the Smart Grid must ensure full security to protect data integrity. In addition, the authentication protocol should meet the following requirements from the network perspective.

- High efficiency. Efficiency is crucial to achieve the high availability requirement in real-time Smart Grid applications. The indication of high efficiency is two-fold. First, the authentication schemes should not incur too much redundancy for security. However, for an authentication protocol, less redundancy in general results in less security. **For example, for a message authentication code (MAC) based authentication protocol, a MAC is generated using a keyed hash function, and appended to a message. Essentially, the MAC is redundancy to the information the message contains, making the message longer to transmit. However, it provides the authenticity of the source of the information: the longer the MAC, the harder the falsification of the information.** Hence, it is always desirable to balance a good tradeoff between redundancy and security. Second, computation involved in authentication (e.g., digital signature and verification) must be fast enough to meet timing requirements of messages in the Smart Grid. This indicates that the use of public key based authentication, which provides strong authentication at the cost of more processing overhead, will be limited in the Smart Grid, in particular in distribution and transmission systems.
- Tolerance to faults and attacks. Authentication schemes can offer strong protection against attacks targeting data integrity, **but cannot by themselves**

provide all the necessary security in an operational environment [104], especially under the circumstance of DoS attacks. Hence, authentication schemes are required to detect malicious attacks, collaborate with attack detection and response systems, and even designed to be robust to DoS attacks in the Smart Grid.

- Support of multicast. Multicast has wide applications in the Smart Grid, including monitoring, protection, and information dissemination [22, 24, 105]. For example, in a power substation, if an IED that keeps monitoring the status of a power feeder senses any anomaly (e.g., high voltage or current), it will issue a command of tripping circuit breakers to protect power equipments [24, 25]. In such a case, unicasting the same time-critical tripping command to each of the breakers unavoidably leads to large delay and potential damages of power equipments. The most efficient way is to multicast a time-critical message to all related breakers that belong to the same multicast group. Hence, authentication schemes in the Smart Grid must be able to efficiently support multicast.

6.2.2. Overview of Authentication Schemes for Power Systems

The fundamental requirement for authentication design is to provide efficient multicast authentication schemes for the Smart Grid applications. Therefore, few recent works [106–108] are designed toward this objective, i.e., fast multicast authentication protocols for power control systems.

The most straightforward multicast authentication scheme is to use public key based authentication, which is also recommended by a recent security standard for substation communication, IEC 62351 [109]. In public key based multicast authentication, all receivers share the public key of the sender. The sender signs a message with its own private key, then each receiver uses the sender's public key to verify the message. The scheme is communication-efficient as only one authenticator is appended to the message; however, it is quite computationally inefficient (e.g. RSA in Table 12) for embedded devices in power systems.

An intuitive alternative is to use computationally efficient symmetric key instead of public key. However, sharing only one symmetric key across a multicast group cannot guarantee adequate security, because when multiple nodes share a single key, it is easy for an attacker that has obtained the key by compromising a node to masquerade as a different sender and inject fake information into the network.

Therefore, the security community has made significant efforts to design some form of asymmetry across receivers to develop fast and efficient multicast authentication. In general, multicast authentication can be categorized into three categories [110]: secret-information asymmetry, time asymmetry and hybrid asymmetry, as shown in Fig. 6.

- Secret-information asymmetry. The underlying idea of secret-information asymmetry is that all receivers

Table 13: Comparison of multicast authentication schemes.

Multicast Scheme	Computation Complexity	Packet buffering	Synchronization	Packet overhead	Smart Grid Application
Public key based	High	No	No	L	IEC 62351 [109]
Secret-information asymmetry	Low	No	No	$L \times N$	Truncated MAC [107, 108]
Time asymmetry	Low	Yes	Yes	L	-
Hybrid asymmetry	Low	No	Lose	L	TV-HORS [106]

In the table, L is the length of the authentication information for one key, and N is the number of receivers

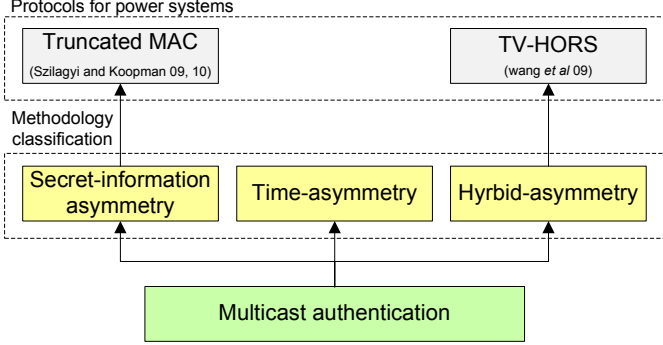


Figure 6: Classification of multicast authentication and related work in power systems.

are associated with different secrets at the sender. The sender computes the corresponding authenticator of a message with each receiver’s secret, appends all authenticators to the message and multicasts it to all receivers. When receiving the message, each receiver uses its own secret to verify the authenticity of the message. This method is the most intuitive one, but suffers from the scalability problem. Thus, existing solutions (e.g., [111]) attempted to balance a good tradeoff between the scalability and security. Recently, based on secret-information asymmetry, Szilagyi and Koopman proposed multicast authentication [107, 108] schemes for embedded control system applications. The schemes validate truncated message authentication codes (MACs) across multiple packets to achieve a good tradeoff among authentication cost, delay performance, and tolerance to attacks, thereby showing their potential use in Smart Grid applications.

- **Time asymmetry.** This approach uses different keys in different time slots (rather than in different receivers). The sender and receivers are synchronized with each other. The sender discloses a key to all receivers after they have received and buffered the message. The key is only valid in a limited time interval, thereby preventing malicious users from forging messages after obtaining the key. Time-asymmetry methods (e.g., TESLA [112, 113]) have excellent computational efficiency and low communication overhead. However, packet buffering and delayed key disclosure limit the

use of time-asymmetry in time-critical applications in the Smart Grid.

- **Hybrid asymmetry.** As we can see, secret-information asymmetry can verify packets as soon as they are received but needs to balance a tradeoff between security and scalability. Time asymmetry has low overhead and is robust to attacks since a single key is used in a short time period, but has the problem of packet buffering. The main idea of hybrid asymmetry is to combine the two asymmetry mechanisms together to achieve time efficiency, scalability, and security at the same time. To this end, researchers introduced one-time signature (OTS) [110] as a primitive to efficiently authenticate multicast messages. However, the “one-timed-ness” characteristic greatly confines the usage of OTS [114], which implies a complicated key management scheme. To mitigate the limitation of OTS, researchers relaxed the constraint of “one-timed-ness” to “n-timed-ness” and developed the scheme of hash to obtain random subsets (HORS) [115], which is considered as one of the fastest cryptographic primitives to date in signature generation and verification. Recently, based on HORS, Wang *et al* [106] established a very fast multicast authentication protocol, time valid HORS (TV-HORS), for time-critical messages in the Smart Grid. However, the evident drawback of such hybrid-asymmetry methods is that they require a large public key size on the order of 10 KB [110], resulting in non-negligible overhead for both communication and storage.

We compare different multicast authentication schemes in Tables 13 from which we see that although only few works deal with multicast authentication for power systems, they in fact fall into distinct categories in multicast authentication. The lack of time-asymmetry based schemes is mainly due to packet buffering that inevitably delays the authentication process of a message, which is quite undesirable in real-time control systems.

In the next, we use a case study in a small-scale power substation network to offer a practical view on the network performance of multicast authentication in power systems.

6.2.3. Experimental Study in Power Substation Network

We set up a small-scale power substation network based on IEC 61850 and 100Mbps Ethernet. The network is used

for local monitoring and protection for power equipments (corresponding to *Case 1* in Section 4). To demonstrate the performance of authentication schemes with different computational capabilities, we use laptops that can dynamically adjust the CPU speed to emulate IEDs. We set up a simple multicast group with one sender and two receivers.

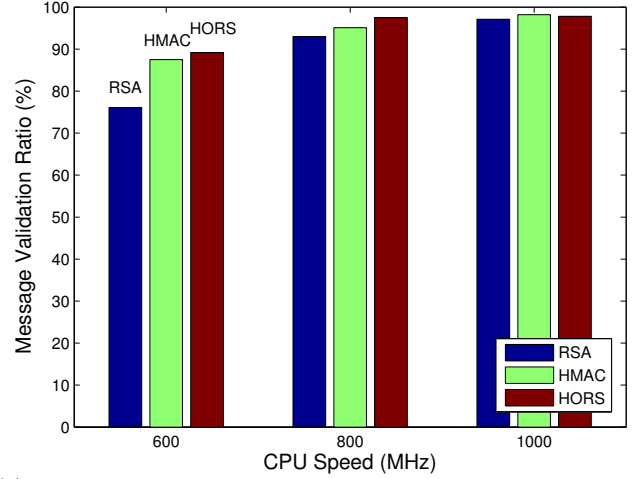
For experiments, we choose to implement three fundamental cryptographic primitives: RSA (defined in IEC 62351), HMAC (basis for secret-information asymmetry), and HORS (basis for hybrid asymmetry). We integrate these primitives into the time-critical GOOSE (3ms limit) communication module in IEC 61850.

Note that for cryptographic primitives, different parameters (e.g., key length and hash functions) lead to distinct security performance. Therefore, we adopt recommended setups for RSA, HMAC and HORS [115, 116] to achieve equivalent security performance. Specifically, we choose a 1024-bit key for RSA; we use SHA-1 and a 128-bit key for HMAC; and we use parameters given in [115] for HORS. In addition, we use OpenSSL 0.9.81², which offers optimized C codes for cryptographic processes, to efficiently generate MACs and digital signatures.

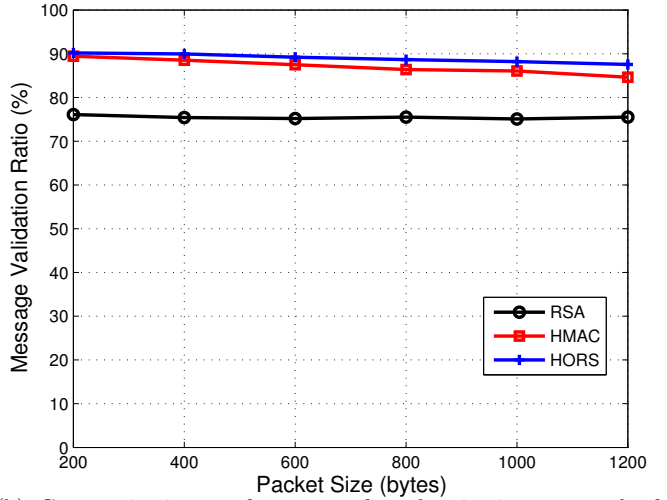
To offer a clear performance comparison, we first need to choose an appropriate performance metric. Since in the Smart Grid, the message delay is critical for power applications. A message is considered valid only if its delay is smaller than the timing requirement. Accordingly, we use the message validation ratio to measure the performance of different authentication schemes. The message validation ratio is defined as the probability that the delay of a message is smaller than its delay threshold. In our case, it means the probability that a secure GOOSE message is successfully delivered from the transmitter to a receiver before the deadline (3ms).

Fig. 7(a) shows message validation ratios of authentication protocols for multicast GOOSE messaging as a function of CPU speed. We can see from Fig. 7(a) that when the CPU speed is as low as 600MHz, RSA leads to the worst communication performance, while HMAC and HORS have approximately the same performance. This indicates that although RSA is recommended by IEC 62351, its low computational efficiency indeed affects the communication performance of time-critical applications for IEDs with limited computational abilities. We also studied the impact of packet size as shown in Fig. 7(b). We note that for RSA, HMAC and HORS, packet size has slight effects on the communication performance. This is because GOOSE packets will be hashed into message digests with a fixed length, such as 160 bits by SHA-1 and 256 bits by SHA-256, thereby mitigating the effect of the variation of packet size.

From the case study, we see that the IEC 62351 recommendation, RSA, is in fact not ready to be used in



(a) Communication performance of authentication protocols for GOOSE messaging as a function of CPU speed. The packet size is fixed to 400 bytes.



(b) Communication performance of authentication protocols for GOOSE messaging as a function of packet size. The CPU speed is fixed to be 600 MHz.

Figure 7: Experimental evaluation of authentication schemes for power systems.

time-critical communications between practical embedded devices for power systems. Either hardware support or more powerful CPU is essential to empower IEDs with capabilities of efficient RSA computation, which inevitably increases the cost of secure communications in the Smart Grid. On the other hand, HMAC and HORS based authentication schemes show promising communication performance. Nevertheless, their stability and performance in large-scale networks still need to be explored.

6.3. Key Management

Encryption and authentication are essential cryptographic processes for the Smart Grid to protect data integrity and confidentiality. Moreover, cryptographic countermeasures for the Smart Grid entail not only such cryp-

²<http://www.openssl.org/>

tographic processes, but also key management on different scales, from tens (e.g. a power substation network) to millions of credentials and keys (e.g. the AMI network). Inadequate key management can result in possible key disclosure to attackers, and even jeopardizing the entire goal of secure communications in the Smart Grid. Therefore, key management is another critical process to ensure the secure operation of the Smart Grid. Based on cryptographic primitives, key management can be also classified into public key infrastructure and symmetric key management.

- Public key infrastructure (PKI). PKI is a mechanism that binds public keys with unique user identities by a certificate authority (CA). Users have to obtain certificated public keys of their counterparts from the CA before initiating secure and trustworthy communication with each other.
- Symmetric key management. This is the key management scheme for symmetric cryptography, which includes key generation, key distribution, key storage, and key update. Accordingly, it requires more coordination and interaction between two or more entities than PKI. However, the advantage of symmetric key cryptography is the efficiency for large amounts of data.

As key management for conventional computer networks has been well categorized and summarized in several survey papers [117, 118], in the following, we focus on the new requirements of key management for the Smart Grid, and present an overview of existing key management schemes for power systems.

6.3.1. Function Requirements

As key management is a critical mechanism for Smart Grid security, the NIST report [29] has made considerable efforts to discuss security issues associated with key management in the Smart Grid. Thus, according to [29], we summarize the basic requirements that are relevant to key management as follows.

- Secure management. Such a requirement includes the proper use of algorithms and parameters (e.g., key size and lifetime), robustness to key compromise and known attacks. The key management system is also required to provide adequate protection of cryptographic materials, as well as sufficient key diversity.
- Scalability. For small-scale networks, like community energy systems, power substation networks that usually consist of tens of IEDs, scalability may not be an issue. However, the scalability becomes a major issue for large-scale systems, such as wide-area transmission systems and the AMI network.
- Efficiency. Here, we consider three aspects: computation, storage, and communication because of their

impact on the overall system performance. The cryptographic process should be computationally efficient as well as memory-usage-efficient as Smart Grid low-processing-devices may have limited RAM space (e.g. 4kb–12kb [29]). The protocols involved in the key generation, distribution, usage, and refreshment should also induce low communication overhead, which is important to time-critical scenarios in the Smart Grid.

- Evolvability. As Smart Grid equipments are often required to have an average life of 20 years [29], the key management system should have the ability to integrate newly-designed cipher suites and protocols to enhance security and efficiency in the Smart Grid.

6.3.2. Key Management in Power Systems

The Smart Grid consists of heterogeneous communication networks, including time-critical (e.g. for protection) and non-real-time (e.g., for maintenance) networks, small-scale (e.g., a substation system) and large-scale (e.g., the AMI system) networks, wireless and wireline networks. It is not practical to design a single key management infrastructure to generate and distribute keys for all networks in the Smart Grid. Therefore, key management schemes should be carefully chosen to meet the network and security requirements of various systems in the Smart Grid. In the following, we summarize existing key management frameworks for power systems.

- Single symmetric key can be shared among all users, which is the most efficient yet the least secure way to provide secure communication. If an attacker obtains the key by compromising a device, it can easily inject falsified information to the entire network. Unfortunately, it is indeed used in existing metering systems where the same symmetric key is shared across all meters and even in different states [29]. **If tamper-proof devices are deployed, the single symmetric key scheme can be very efficient to exchange information secretly. However, it is not practical to consider all devices as tamper-proof ones. For example, meters are usually exposed in neighborhoods and lack physical protection [119], it may be relatively easy for an attacker to compromise a meter to obtain the shared symmetric key.**
- SKE, a key establishment scheme for SCADA systems [120], was proposed by Sandia National Laboratories. SKE divides SCADA communication into two categories: master-slave and peer-to-peer, which use symmetric key and public key schemes, respectively. SKE is an elementary key management scheme for the SCADA system with low-cost security. It neither includes a full-fledged key management infrastructure, nor supports efficient multicast and broadcast that are essential in power systems.

Table 14: Comparison of key management schemes for power systems.

Scheme	Robust to key compromise	Support of multicast	Scalability	Power system application
Single-key	No	Yes	$O(1)$	Meter network
SKE	Yes	No	$O(N)$	SCADA
SKMA	Yes	No	$O(N)$	SCADA
ASKMA	Yes	Yes	$O(N)$	SCADA
ASKMA+	Yes	Yes	$O(N)$	SCADA
SMOCK	Yes	No	$O(\log N)$	Experimental system

In the table, N is the number of nodes in the key management system.

- SKMA, a key management architecture for SCADA systems [121], was proposed to overcome the limitations of SKE. A key distribution center (KDC) is used to maintain a long term key for each node. In SKMA, a node must maintain two types of long terms keys: node-to-KDC and node-to-node. The former is manually installed on a node; and the latter is obtained from the KDC. A session key is generated using the node-to-node key when two nodes communicate with each other. However, SKMA still does not support multicast. Key update and revocation are also issues of SKMA.
- ASKMA, an advanced key-management architecture for SCADA systems, was designed in [122] to use a logical key hierarchy (LKH) to achieve efficient key management among all nodes. ASKMA has two major advantages compared with SKE and SKMA: 1) it supports multicast and broadcast, 2) it is computationally efficient for node-to-node communication. However, it is less efficient during the multicast communication process.
- ASKMA+ was proposed in [123] to further improve the efficiency of ASKMA. In ASKMA+, the authors divided the key structure into two classes applying the Iolus framework [124] and constructed each class as a LKH structure. ASKMA+ was shown both multicast-efficient and storage-efficient compared with ASKMA.
- SMOCK, scalable method of cryptographic key management, was proposed in [125] to achieve light-weight key management for mission-critical wireless networks with application to power grids. SMOCK entails almost zero communication overhead for authentication, offers high service availability and good scalability. Whereas, SMOCK is not fully designed with multicast and is more computationally cumbersome, thereby increasing the burden of embedded devices in power systems.

Table 14 shows the comparison of existing key management schemes in terms of security, functionality, scalability and applications. It is noted from this table that the majority of existing work focuses on key management for the SCADA network. ASKMA+ is the most efficient key management scheme with support of multicast. However, it

still suffers from the scalability problem. SMOCK shows good scalability, however, it neither supports multicast, nor is computationally efficient. Overall, as we can see from Table 14, current schemes have not yet provided a perfect key management solution for the Smart Grid.

6.4. Summary and Research Challenges

We have discussed cryptographic mechanisms to prevent the Smart Grid from network attacks targeting integrity and confidentiality, including encryption, authentication, and key management. In the following, we summarize the research challenges with respect to security mechanisms for the Smart Grid.

6.4.1. Tradeoff between Security and Latency

Delay performance and security are two fundamental goals in authentication design for the Smart Grid. However, they are usually paradoxical in practice. For instance, in public key based schemes, the longer the key size, the more secure an authentication scheme is. On the other hand, the longer the key size, the worse the delay performance is. Therefore, it is highly desirable to assess the tradeoff between security and time-criticality in order to adopt appropriate authentication schemes in the Smart Grid.

Our initial experimental results indicate that HMAC-based (for secret-information asymmetry) and HORS-based (for hybrid asymmetry) schemes can be viewed as potential solution candidates for authentication in the Smart Grid, as they provide very fast and efficient authentication processes. Yet, fine-grained authentication protocols still need to be developed for different time-critical Smart Grid applications because of the explicit and stringent timing requirements in power systems.

6.4.2. Emerging Physical-Layer Authentication

As we can see, conventional authentication schemes have to strike a tradeoff between security and time-criticality. Recently, physical-layer authentication (e.g., [126–129]) emerges as a promising alternative for fast and low-overhead authentication. Compared with conventional data origin authentication mechanisms that exist at the link layer and above, physical-layer authentication usually requires no additional bandwidth to transmit authentication information.

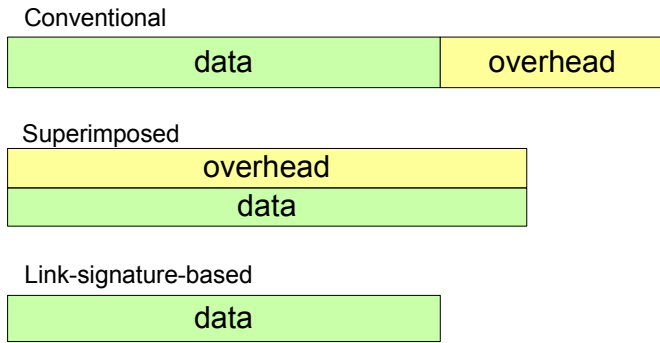


Figure 8: Comparison of conventional data origin authentication and physical-layer authentication including superimposed and link-signature-based schemes.

As shown in Fig. 8, physical-layer authentication can be mainly classified into superimposed authentication [128] and link-signature-based authentication [126, 127, 129]. In superimposed authentication, authentication is added into the physical-layer signal via a carefully designed modulation on the waveforms. Hence, authentication information and data information are transmitted at the same time to the receiver, thereby reducing the communication overhead. In link-signature-based authentication for wireless networks, the physical-layer link signature (or channel impulse response) has the reciprocal property between a transmitter-receiver pair, which provides a unique secret for the pair to authenticate with each other. Therefore, authentication can be performed in the channel estimation process at the physical layer and even requires no overhead to transmit.

Given the nice property, i.e., low-overhead and short latency, of emerging authentication mechanisms at the physical layer, they are considered as a promising approach in the Smart Grid, especially in wireless-based systems. However, dynamic, time-varying characteristics of wireless channels may result in error-prone authentication results. How to assess such a risk and design robust physical-layer authentication is quite challenging for Smart Grid applications.

6.4.3. Symmetric Key Management for Time-Critical Systems

For time-critical applications in the Smart Grid, symmetric key cryptography is more appropriate than public key cryptography because of its computational efficiency. However, symmetric key management is a major issue associated with symmetric cryptography. As stated in [29], symmetric keys often have a shorter lifespan than asymmetric keys due to the amount of data that is protected using a single key. Limiting the amount of data protected by a symmetric key helps reduce the risk of compromise of both the key and the data. This means that the key management system has to keep generating new keys and distributing them to power devices via communication networks frequently, which entails not only the critical trust

problem between the key producer and key consumers, but also the risk of key disclosure during the key distribution process. However, little attention has been focused on the design of this critical process for symmetric key management in the literature. Therefore, symmetric key management still remains as an important yet open issue in the Smart Grid.

6.4.4. Key Management for Advanced Metering Infrastructure

From Table 14, most existing work addresses the design of key management for the SCADA network, while overlooking that for the AMI network. The AMI network is a large-scale communication network across multiple Smart Grid domains including utility companies, customers, and metering systems. Because communication traffic in these systems is not as sensitive as time-critical applications, it is highly expected that low-cost asymmetric key management systems will be deployed to avoid the complexity of symmetric key management in the AMI network. However, key management for the AMI network is still challenging.

One important issue is the scalability of key management in the AMI network. As we can see, SMOCK in Table 14 shows promising results for the AMI network. However, it solves the scalability problem by introducing a combinatorial design of public key cryptography, involving multiple computations of digital signature. Such a design significantly increases the computational complexity and thereby may be not suitable for low-cost smart meters in the AMI network.

On the other hand, the AMI network is also a basis for new Smart Grid functionalities in home-area networks. For example, by using the demand response system, customers can dynamically manage their consumption of electricity in response to the real-time price in the electric market. There are intricate relations between customers, markets, companies, and policies during the communication in the AMI network. Conventional PKI schemes may not be efficient in such a network. Emerging key management architectures, such as attribute-based encryption [130] and policy-based encryption [131], may have potential applications in the AMI network.

In addition, many communication standards are proposed to be used in the AMI networks, in particular ZigBee that features a low-rate and low-power wireless transmission technology [20]. Existing security issues in ZigBee [132], such as the deficiency in the network and link key management, must also be addressed before we widely deploy ZigBee products in AMI networks.

7. Design of Secure Network Protocols and Architectures

To deal with potential security threats in the Smart Grid, countermeasures and defense strategies will be

widely deployed and integrated into network protocols and architectures. Therefore, compared with legacy power systems, the Smart Grid features full-fledged communication protocol stacks to accomplish the goal of secure and efficient communications in the entire network. In this section, we review the secure protocols and architectures for the Smart Grid, and then summarize research challenges.

7.1. Protocols and Standards for Secure Power System Communication

Recently, many efforts have been made in the power community to develop secure protocols for power grids, most of which are leveraging existing protocol suites to achieve secure communications, such as IPsec [133] and transport layer security (TLS) [22]. Besides existing protocol suites, security extension for power communication protocols also becomes a primary focus in the literature and standardization. In the following, we briefly present the security extensions for the two widely-used power grid communication protocols, DNP3 and IEC 61850.

7.1.1. Secure DNP3

DNP3 is currently extensively-used for both intra-substation and inter-substation communications in US power systems [6]. DNP3 was designed originally without any security mechanism. Since it is not very practical to upgrade all legacy DNP3-based power systems into new ones in one day, it is essential to modify or even overhaul DNP3 to adopt more security functionalities to make a large number of legacy power devices keep pace with security requirements in the Smart Grid.

Researchers [134–136] have already started to design security functionalities for DNP3 based on two main solutions: 1) modify the original protocol to introduce security mechanisms to the DNP3 stack; 2) insert a security layer between the TCP/IP layer and the DNP3 protocol stack. The former will provide the security suits only for DNP3 regardless of the lower layer configuration, however, it needs tedious modification of the protocol stack and requires the upgrade of communication systems in power devices. The latter, shown in Fig. 9(a), does not need to change any of the DNP3 protocol stack. It enables legacy systems to communicate with the Smart Grid via protocol translation devices.

From the above description, it is clear that inserting a security layer between DNP3 and TCP/IP is more desirable to make legacy devices compatible with smart grid devices. Specifically, the objective of this security layer is to help the DNP3 protocol achieve basic security requirements for integrity and confidentiality. At the transmitter, the security layer intercepts DNP3 packets distributed to the TCP/IP layer, encrypts the data, then sends encrypted packets into the TCP/IP layer. At the receiver, the security layer decrypts data packets from the TCP/IP layer, and passes them to the application layer (DNP3 layers). Either symmetric or asymmetric algorithms can be

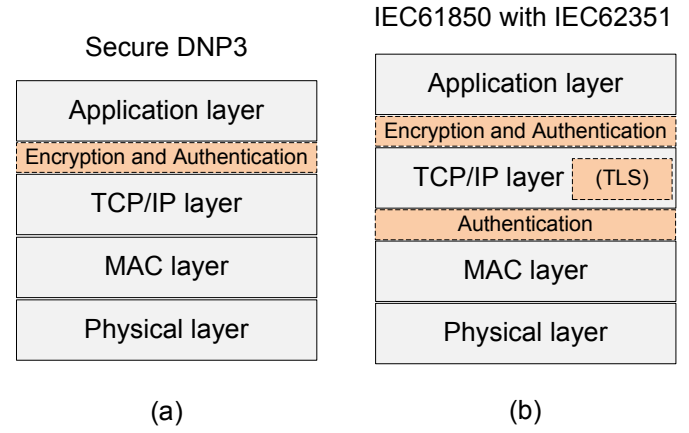


Figure 9: Secure DNP3 and IEC 61850 with IEC 62351.

used to provide protection of integrity and confidentiality for DNP3 packets. For example, MAC-based authentication is designed and implemented in [137] as a security extension to DNP3-based communication for distribution automation systems.

7.1.2. IEC 61850 and IEC 62351

IEC 61850, a recent standard for substation communication, comes without its own security mechanisms. The security of IEC 61850 relies on IEC 62351 [109], which is a standard proposed to handle the security for a series of protocols including IEC 61850. **In the following, we briefly discuss how IEC 62351 enforces security for IEC 61850.**

IEC 62351 defines both authentication and encryption mechanisms for IEC 61850 communication. As shown in Fig. 9(b), it includes two essential security layers.

1. An authentication and encryption layer above the TCP/IP layer. This layer enforces TLS to use symmetric cryptography and MACs for message confidentiality and authenticity. This layer is intentionally used for less time-critical messages based on TCP/IP in substation systems.
2. An authentication layer between the MAC and IP layers. This layer is specifically used for authenticating time-critical messages in IEC 61850 that do not pass through the TCP/IP layer, i.e., GOOSE and SMV. To ensure that such messages can be delivered in a timely manner, IEC 62351 defines no data encryption mechanism for this layer, thus time-critical messages in IEC 61850 are only protected for authenticity.

Compared with secure DNP3, IEC 61850 with IEC 62351 is a modern power communication protocol that balances the tradeoff between security and time-criticality by using two distinct security layers for different message types in power systems. It can be expected that more comprehensive security layering mechanisms will be proposed to achieve both security and QoS requirements for message delivery in the Smart Grid.

7.2. Secure Data Aggregation Protocols

Secure DNP3 and IEC 61850 with IEC 62351 are proposed to achieve end-to-end security for power grid communications. Besides such end-to-end security protocols, secure data aggregation protocols are also proposed for the Smart Grid [138, 139], since the *bottom-up* traffic model (device-to-center) is pervasive in power systems, such as metering reading in the AMI network and device monitoring in the SCADA network. In such a communication model, data aggregation protocols with in-network data processing will be more efficient than end-to-end routing protocols by which each node attempts to find its own route to the center.

As secure data aggregation requires more computing resources and introduces additional delay overhead, existing work focuses on secure data aggregation protocols for the AMI network whose communication traffic is less time-critical [138, 139]. A recent approach in [138] constructs a spanning tree rooting at the collector device to cover all of the smart meters. Aggregation is performed in a distributed manner in accordance with the aggregation tree in which each node collects data samples from its children, aggregates them with its own data, and sends the intermediate result to the parent node. In addition, homomorphic encryption is used to protect data privacy so that inputs and intermediate results are not revealed to smart meters on the aggregation path.

Another recent work [139] proposes a secure aggregation protocol for the wireless-based AMI network. In [139], end-to-end security is achieved via a shared secret between the source and the destination; hop-by-hop security is enforced at the physical/MAC layers via pairwise keys between a node and its next-hop neighbors. Data will be aggregated at each hop to save communication overhead and reduce overall network traffic load.

It has been shown [138, 139] that data aggregation can be an efficient and effective alternative for metering reading in the AMI network. There are still several issues associated with current approaches. For example, both [138] and [139] assume that all nodes are trustworthy and there is no attack along the aggregation path. However, in practice, an attacker can actively involve itself in the data aggregation process and forge its own data to manipulate the aggregation results. The collection center will lose a large amount of information if an aggregation result is corrupted by the attack. Accordingly, secure aggregation protocols for the Smart Grid need to protect data integrity and confidentiality, and also be resilient to malicious attacks.

7.3. Secure Network Architecture

We have introduced the design of secure protocols to achieve secure data delivery between nodes in the Smart Grid. In the following, we introduce the design of physical and logical network architectures that limits or isolates the communication domains of individual nodes in the Smart

Grid. Generally, there are two proposed secure network architectures for the Smart Grid.

- Trust computing based architecture [13, 140, 141]. In this architecture, a trust computing system is introduced in power communication and information systems to authenticate and certificate data information in the Smart Grid. For example, a trust computing architecture is proposed in [140] for the SCADA network, in which a trust system is deployed at or near the SCADA center to validates input, identities, assess security risks, detect bad data and initiate appropriate alerts and response actions. Distributed trust computing hardware is also proposed in [141] to form a security infrastructure for power networks.
- Role-based network architecture [142]. In this design, an authentication network structure is proposed based on functional roles. In [142], the power communication network is divided into multiple domains, each of which contains one network control center and several microgrids. A microgrid can include a number of roles, defined as a collection of privileges that can be executed by the authorized users. Thus, cross-domain access is strictly restrained by role models to enhanced security.

Overall, the design of secure network architectures for the Smart Grid touches upon a very broad scope of issues in networking, trust computing, and cryptographic systems. Therefore, it requires a comprehensive view on intricate security requirements, policies, network and entity models in the Smart Grid.

7.4. Summary and Research Challenges

In this section, we have reviewed security extensions for power communication protocols, secure data aggregation protocols and secure network architectures proposed for the Smart Grid. In the following, we present research challenges related to secure protocol and architecture design.

7.4.1. Efficient and Secure Communication Protocols for Wide-Area Power Systems

Power systems feature a number of time-critical messages with specific delay thresholds. Different time-critical messages in the Smart Grid should have different QoS guarantees in the communication protocol stack. For instance, IEC 61850 with IEC 62351 in Fig. 9, has multiple security mechanisms, including TLS and its own application-layer security for less time-sensitive messages and MAC-layer security for time-critical messages.

Thus, appending a unified security layer to the protocol stack is not always the optimal solution for secure communications in power systems. Table 15 shows the diversity of security mechanisms that are currently used at distinct layers to achieve secure communications in power systems. We note that at the network and transport layers, power

Table 16: **Summary of potential applications of existing security schemes to the Smart Grid and solutions needing to be investigated.**

Category	Generation/Transmission/Distribution	Markets/Customer/Service Provider
DoS attack detection:	<i>Need fast detection</i>	Based on existing intrusion detection
DoS attack mitigation:	Wireline: based on Internet solutions <i>Wireless: need delay-efficient schemes</i>	Wireline: based on Internet solutions Wireless: existing anti-jamming schemes
Encryption:	Tamper-proof devices with symmetric key	Symmetric or public key
Authentication:	Wireless: physical-layer authentication <i>Wide-area: need fast E2E authentication</i>	Wireless: physical-layer authentication Wide-area: secure E2E data aggregation
Key management:	<i>Need delay-efficient key management</i>	<i>Need large-scale key management</i>

Table 15: Security mechanisms that are currently used at different communication layers.

Layer	Security mechanism
Application	Authentication for MMS*
Transport	TLS for IEC 61850
Network	IPSec for PMU applications
MAC	Authentication for GOOSE/SMV

(*MMS stands for manufacturing message specification [22].)

systems still rely on the Internet security mechanisms including TLS and IPSec. This indicates that current power devices can only use Internet security protocols to communicate with each other in multi-hop communication networks for wide-area power systems (e.g., power transmission networks). However, such mechanisms are built upon the throughput-oriented Internet and may not be the optimal solution for delay-oriented power systems. Therefore, it is promising to design new network/transport-layer protocols to achieve secure and efficient end-to-end message delivery for wide-area power systems in the Smart Grid.

7.4.2. Secure Routing and Aggregation Protocols

Recent works [138, 139] have shown that data aggregation protocols are effective solutions for the *bottom-up* traffic in the Smart Grid. On one hand, such protocols reduce the overhead of secure communications by aggregating packets along the path; on the other hand, they will incur more data processing delay at each hop. Moreover, such data aggregation introduces two additional security problems that **have not yet been solved** by existing approaches [138, 139]. First, an attacker can actively participate in the aggregation process to inject falsified information to the network. How to accurately identify attackers and prevent them from joining the aggregation path becomes a critical issue to be addressed for secure data aggregation protocols. Second, the attacker can also obtain a large amount of sensitive information by successfully decrypting one aggregation packet. This means that packets with more aggregation results require stronger protection for confidentiality. How to design strong data encryption schemes along the aggregation path is also a challenging issue in the Smart Grid.

8. Discussions and Remaining Challenges

So far, we have analyzed potential cyber security threats, reviewed existing security solutions, and summarized research challenges in the Smart Grid. We notice that there have already been several surveys touching upon the topics of Smart Grid security [12, 15, 16, 143, 144]. Our survey features more detailed use case studies to analyze potential security attacks in different systems for the Smart Grid, e.g., Cases 1–5 in Section 4. In addition, we also offer first-hand experimental results on real-world power devices in Section 6. Our survey not only comprehensively discusses state-of-the-art technologies for Smart Grid security, but also is complementary to the coverage of existing survey papers.

In previous sections, we have summarized research challenges for Smart Grid security. We note that due to distinct features of different Smart Grid domains, a security solution may be potentially applicable to one domain but not the others. Thus, it becomes necessary and useful to summarize the applications of existing security solutions to different parts in the Smart Grid to offer a top-down overview of the remaining challenges in Smart Grid security research, which is briefly illustrated in Table 16.

From Table 16, we can observe that many security methods and schemes could be applicable to the Smart Grid, especially in domains that interact with customers (i.e., the Markets/Customer/Service Provider domains). While in the Generation/Transmission/Distribution domains, which are responsible for the process of power delivery, attack detection, mitigation, authentication and key management still remain as challenging security issues due to the large network scale and more demanding requirements for security design. For example, for jamming mitigation in wireless Smart Grid applications, existing approaches can be readily adapted to the Markets/Customer/Service Provider domains, but are not applicable or may encounter problems in the Generation/Transmission/Distribution domains because of the stringent timing requirements of message delivery in these domains, which is detailed in Section 5. The Generation/Transmission/Distribution domains require security solutions to not only protect information exchange, but also meet the requirements for data communication and

processing, thereby posing a practical challenge for security designers.

9. Conclusions

Cyber security in the Smart Grid is a new area of research that has attracted rapidly growing attention in the government, industry and academia. In this paper, we presented a comprehensive survey of security issues in the Smart Grid. We introduced the communication architecture and security requirements, analyzed security vulnerabilities through case studies, and discussed attack prevention and defense approaches in the Smart Grid. We also summarized the design of secure network protocols to achieve efficient and secure information delivery in the Smart Grid.

As we have reviewed, cyber security is still under development in the Smart Grid, especially because information security must be taken into account with electrical power systems. Features of the Smart Grid communication network, such as heterogeneous devices and network architecture, delay constraints on different time scales, scalability, and diversified capabilities of embedded devices, make it indeed impractical to uniformly deploy strong security approaches all over the Smart Grid. Consequently, the Smart Grid requires fine-grained security solutions designed specifically for distinct network applications, making cyber security for the Smart Grid a very fruitful and challenging research area in the future.

Acknowledgement

The authors would like to thank Mr. Xiang Lu for setting up power substation networks and providing experimental results used in Section 6. **The authors would also like to thank the anonymous reviewers for their valuable comments that substantially improved this paper.**

References

- [1] G. Lu, D. De, W.-Z. Song, SmartGridLab: A laboratory-based smart grid testbed, in: Proc. of IEEE Conference on Smart Grid Communications, 2010.
- [2] A. Huang, M. Crow, G. Heydt, J. Zheng, S. Dale, The future renewable electric energy delivery and management (freedm) systems: The energy internet, Proceedings of the IEEE (1) (2011) 133–148.
- [3] Office of the National Coordinator for Smart Grid Interoperability, NIST framework and roadmap for smart grid interoperability standards, release 1.0, NIST Special Publication 1108 (2010) 1–145.
- [4] V. C. Gungor, F. C. Lambert, A survey on communication networks for electric system automation, Computer Networks (2006) 877–897.
- [5] T.-I. Choi, K. Y. Lee, D. R. Lee, J. K. Ahn, Communication system for distribution automation using cdma, IEEE Trans. Power Delivery 23 (2008) 650–656.
- [6] S. Mohagheghi, J. Stoupi, Z. Wang, Communication protocols and networks for power systems - current status and future trends, in: Proc. of Power Systems Conference and Exposition (PES '09), 2009.
- [7] H. J. Zhou, C. X. Guo, J. Qin, Efficient application of GPRS and CDMA networks in SCADA system, in: Proc. of IEEE power and Energy Society General Meeting (PES '10), 2010.
- [8] A. Aggarwal, S. Kunta, P. K. Verma, A proposed communications infrastructure for the smart grid, in: Proc. of Proc. of Innovative Smart Grid Technologies Conference Europe (ISGT), 2010.
- [9] H. Sui, H. Wang, M.-S. Lu, W.-J. Lee, An AMI system for the deregulated electricity markets, IEEE Trans. Industry Applications 45 (6) (2009) 2104 – 2108.
- [10] M. LeMay, R. Nelli, G. Gross, C. A. Gunter, An integrated architecture for demand response communications and control, in: Proc. of 41th Hawaii International Conference on System Sciences (HICSS' 08), 2008.
- [11] A. R. Metke, R. L. Ekl, Smart grid security technology, in: Proc. of Innovative Smart Grid Technologies Conference Europe (ISGT), 2010.
- [12] G. N. Ericsson, Cyber security and power system communication - essential parts of a smart grid infrastructure, IEEE Trans. Power Delivery 25 (2010) 1501–1507.
- [13] A. R. Metke, R. L. Ekl, Security technology for smart grid networks, IEEE Trans. Smart Grid 1 (2010) 99–107.
- [14] W. Wang, Y. Xu, M. Khanna, A survey on the communication architectures in the smart grid, Computer Networks 55 (2011) 3604–3629.
- [15] Y. Yan, Y. Qian, H. Sharif, D. Tipper, A survey on cyber security for smart grid communications, IEEE Communications Surveys and Tutorials 14 (2012) 998–1010.
- [16] J. Liu, Y. Xiao, S. Li, W. Liang, C. Chen, Cyber security and privacy issues in smart grids, IEEE Communications Surveys and Tutorials 14 (2012) 981–997.
- [17] R. A. Leon, V. Vittal, G. Manimaran, Application of sensor network for secure electric energy infrastructure, IEEE Trans. Power Delivery 22 (2007) 1021–1028.
- [18] D. Pendarakis, N. Shrivastava, Z. Liu, R. Ambrosio, Information aggregation and optimized actuation in sensor networks: Enabling smart electrical grids, in: Proc. of the IEEE Conference on Computer Communications (INFOCOM '07), 2007.
- [19] A. Ghassemi, S. Bavarian, L. Lampe, Cognitive radio for smart grid communications, in: Proc. of IEEE Conference on Smart Grid Communications, 2010.
- [20] Z. Alliance, RF micro devices features ember ZigBee technology in new family of high performance front end modules for smart energy applications, 2010.
- [21] T. Baumeister, Literature review on smart grid cyber security, Tech. Report.
- [22] IEC Standard, IEC 61850: Communication networks and systems in substations.
- [23] M. E. Crovella, A. Bestavros, Self-similarity in world wide web traffic: Evidence and possible causes, IEEE/ACM Trans. Networking 5 (6) (1997) 835 – 846.
- [24] T. S. Sidhu, Y. Yin, Modelling and simulation for performance evaluation of IEC61850-based substation communication systems, IEEE Trans. Power Delivery 22 (3) (2007) 1482–1489.
- [25] P. M. Kanabar, M. G. Kanabar, W. El-Khattam, T. S. Sidhu, A. Shami, Evaluation of communication technologies for IEC 61850 based distribution automation system with distributed energy resources, in: Proc. of the IEEE Power and Energy Society General Meeting (PES '09), 2009.
- [26] M. J. Karam, F. A. Tobagi, Analysis of the delay and jitter of voice traffic over the Internet, in: Proc. of IEEE INFOCOM '01, 2001.
- [27] D. M. Lavery, D. J. Morrow, R. Best, P. A. Crossley, Telecommunications for smart grid: Backhaul solutions for the distribution network, in: Proc. of IEEE power and Energy Society General Meeting (PES '10), 2010.
- [28] M. S. Thomas, I. Ali, Reliable, fast, and deterministic substation communication network architecture and its performance simulation, IEEE Trans. Power Delivery 25 (2010) 2364–2370.
- [29] The Smart Grid Interoperability Panel - Cyber Security Working Group, Guidelines for smart grid cyber security, NISTIR

- 7628 (2010) 1–597.
- [30] C.-L. Chuang, Y.-C. Wang, C.-H. Lee, M.-Y. Liu, Y.-T. Hsiao, J.-A. Jiang, An adaptive routing algorithm over packet switching networks for operation monitoring of power transmission systems, *IEEE Trans. Power Delivery* 25 (2010) 882–890.
 - [31] K. Curtis, A DNP3 protocol primer, DNP Users Group (2005) 1–8.
URL <http://www.dnp.org>
 - [32] M. Cagalj, S. Ganeriwal, I. Aad, J.-P. Hubaux, On selfish behavior in CSMA/CA networks, in: *Proc. of IEEE INFOCOM'05*, Vol. 4, 2005, pp. 2513–2524.
 - [33] A. A. Cardenas, S. Radosavac, J. S. Baras, Performance comparison of detection schemes for MAC layer misbehavior, in: *Proc. of IEEE INFOCOM'07*, 2007, pp. 1496–1504.
 - [34] K. Pelechrinis, G. Yan, S. Eidenbenz, Detecting selfish exploitation of carrier sensing in 802.11 networks, in: *Proc. of the IEEE Conference on Computer Communications (INFOCOM '09)*, 2009.
 - [35] Z. Lu, X. Lu, W. Wang, C. Wang, Review and evaluation of security threats on the communication networks in the smart grid, in: *Proc. of Military Communications Conference (MILCOM' 10)*, 2010.
 - [36] D. Jin, D. M. Nicol, G. Yan, An event buffer flooding attack in dnp3 controlled scada systems, in: *Proceedings of the 2011 Winter Simulation Conference*, 2011.
 - [37] U. Premaratne, J. Samarabandu, T. Sidhu, R. Beresh, J.-C. Tan, An intrusion detection system for IEC61850 automated substations, *IEEE Trans. Power Delivery* 25 (2010) 2376–2383.
 - [38] Z. Lu, W. Wang, C. Wang, From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic, in: *Proc. of IEEE INFOCOM 2011*, 2011.
 - [39] Y. Liu, P. Ning, M. Reiter, False data injection attacks against state estimation in electric power grids, in: *Proc. of ACM Computer and Communication Security (CCS)*, 2009.
 - [40] O. Kosut, L. Jia, L. Tong, Improving detectors for false data attacks on power system state estimation, in: *Proc. of 44th Annual Conference on Information Sciences and Systems (CISS '10)*, 2010.
 - [41] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, T. J. Overbye, Detecting false data injection attacks on DC state estimation, in: *Proc. of the First Workshop on Secure Control Systems (SCS 2010)*, 2010.
 - [42] H. Sandberg, A. Teixeira, K. H. Johansson, On security indices for state estimators in power networks, in: *Proc. of the First Workshop on Secure Control Systems (SCS 2010)*, 2010.
 - [43] O. Kosut, L. Jia, R. J. Thomas, L. Tong, Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures, in: *Proc. of the IEEE Conference on Smart Grid Communications*, 2010.
 - [44] M. Strasser, S. Capkun, C. Popper, M. Cagalj, Jamming-resistant key establishment using uncoordinated frequency hopping, in: *Proc. of IEEE Symposium on Security and Privacy*, 2008, pp. 64–78.
 - [45] C. Popper, M. Strasser, S. Capkun, Jamming-resistant broadcast communication without shared keys, in: *Proc. of USENIX Security Symposium (Security '09)*, 2009.
 - [46] Y. Liu, P. Ning, H. Dai, A. Liu, Randomized differential DSSS: Jamming-resistant wireless broadcast communication, in: *Proc. of IEEE INFOCOM '10*, 2010.
 - [47] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, D. Zamboni, Analysis of a denial of service attack on tcp, in: *Proc. of IEEE Symposium on Security and Privacy (S&P 1997)*, 1997.
 - [48] A. Yaar, A. Perrig, D. Song, Pi: A path identification mechanism to defend against DDoS attacks, in: *Proc. of IEEE Symposium on Security and Privacy (S&P 2003)*, 2003.
 - [49] J. Mirkovic, P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, *SIGCOMM Comput. Commun. Rev.* 34 (2) (2004) 39–53.
 - [50] S. Ranjan, R. Swaminathan, M. Uysal, A. Nucci, E. Knightly, Ddos-shield: Ddos-resilient scheduling to counter application layer attacks, *ACM/IEEE Trans. Networking* 17 (1) (2009) 40–53.
 - [51] S. Sridhar, G. Manimaran, Data integrity attacks and their impacts on SCADA control system, in: *Proc. of IEEE power and Energy Society General Meeting (PES '10)*, 2010.
 - [52] F. Pasqualetti, R. Carli, F. Bullo, A distributed method for state estimation and false data detection in power networks, in: *Proc. of IEEE Conference on Smart Grid Communications*, 2011.
 - [53] O. Vukovic, K. C. Sou, G. Dan, H. Sandberg, Network-layer protection schemes against stealth attacks on state estimators in power systems, in: *Proc. of IEEE Conference on Smart Grid Communications*, 2011.
 - [54] T. T. Kim, H. V. Poor, Strategic protection against data injection attacks on power grids, *IEEE Trans. Smart Grid* 2 (2) (2011) 326–333.
 - [55] A. Giani, E. Bitar, M. McQueen, P. Khargonekar, K. Poolla, M. Garcia, Smart grid data integrity attacks: Characterizations and countermeasures, in: *Proc. of IEEE Conference on Smart Grid Communications*, 2011.
 - [56] M. Esmalifalak, H. A. Nguyen, R. Zheng, Z. Han, Stealth false data injection using independent component analysis in smart grid, in: *Proc. of IEEE Conference on Smart Grid Communications*, 2011.
 - [57] L. Jia, R. J. Thomas, L. Tong, Malicious data attack on real-time electricity market, in: *Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2011, pp. 5952–5955.
 - [58] L. Xie, Y. Mo, B. Sinopoli, False data injection attacks in electricity markets, in: *Proc. of IEEE Conference on Smart Grid Communications*, 2010.
 - [59] Y. Yuan, Z. Li, K. Ren, Modeling load redistribution attacks in power systems, *IEEE Trans. Smart Grid* 2 (2) (2011) 382–390.
 - [60] K. Jain, Security based on network topology against the wiretapping attack, *IEEE Wireless Communications* 11 (1) (2004) 68–71.
 - [61] C. V. Wright¹, S. E. Coull, F. Monrose, Traffic morphing: An efficient defense against statistical traffic analysis, in: *Proc. of ISOC Network and Distributed System Security Symposium (NDSS)*, 2009.
 - [62] H. Li, L. Lai, W. Zhang, Communication requirement for reliable and secure state estimation and control in smart grid, *IEEE Trans. Smart Grid*.
 - [63] L. Sankar, S. Kar, R. Tandon, H. V. Poor, Competitive privacy in the smart grid: An information-theoretic approach, in: *Proc. of IEEE Conference on Smart Grid Communications*, 2011.
 - [64] U. Premaratne, J. Samarabandu, T. Sidhu, B. Beresh, J.-C. Tan, Evidence theory based decision fusion for masquerade detection in IEC61850 automated substations, in: *Proc. of the 4th International Conference on Information and Automation for Sustainability (ICIAFS 2008)*, 2008.
 - [65] Wi-Fi Alliance, Wi-Fi for the smart grid: Mature, interoperable, security-protected technology for advanced utility management communications, Report (2009) 1–14.
 - [66] B. Akyol, H. Kirkham, S. Clements, M. Hardley, A survey of wireless communications for the electric power system, Report of Pacific Northwest National Laboratory (2010) 1–73.
 - [67] J. D. L. Ree, V. Centeno, J. S. Thorp, A. G. Phadke, Synchronized phasor measurement applications in power systems, *IEEE Trans. Smart Grid* (2010) 20–27.
 - [68] Reuters, Landis+Gyr technology enables full service smart grid coverage, Mar. 31, 2009.
URL <http://www.reuters.com/article/pressRelease/idUS191587+31-Mar-2009+PRN20090331>
 - [69] M. Li, I. Koutsopoulos, R. Poovendran, Optimal jamming attacks and network defense policies in wireless sensor networks, in: *Proc. of IEEE INFOCOM'07*, 2007, pp. 1307–1315.
 - [70] M. Cagalj, S. Capkun, J. P. Hubaux, Wormhole-based anti-jamming techniques in sensor networks, *IEEE Trans. Mobile Computing* 6 (1) (2007) 100–114.

- [71] H. Li, Z. Han, Manipulating the electricity power market via jamming the price signaling in smart grid, in: Proc. of IEEE Globecom Workshop on Smart Grid Communications, 2011.
- [72] W. Xu, W. Trappe, Y. Zhang, T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in: Proc. of ACM MobiHoc '05, 2005, pp. 46–57.
- [73] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, B. Thapa, On the performance of IEEE 802.11 under jamming, in: Proc. of IEEE INFOCOM '08, 2008, pp. 1265–1273.
- [74] J. Markoff, Before the gunfire, cyberattacks, The New York Times, Aug. 13, 2008.
URL <http://www.nytimes.com/2008/08/13/technology/13cyber.html?em>
- [75] Factsheet - Root server attack on 6 February 2007, ICANN.
URL <http://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf>
- [76] The Submarine[link].
URL <http://www.paulgraham.com/submarine.html#f4n>
- [77] K. Lin, K. E. Holbert, PRA for vulnerability assessment of power system infrastructure security, in: Proc. of 37th Annu. North American Power Symposium, 2005, pp. 43–51.
- [78] J. Yu, A. Mao, Z. Guo, Vulnerability assessment of cyber security in power industry, in: Proc. of IEEE Power and Energy Society General Meeting (PES '06), 2006, pp. 2200–2205.
- [79] C. F. Kucuktezan, V. M. I. Genc, Dynamic security assessment of a power system based on probabilistic neural networks, in: Proc. of Innovative Smart Grid Technologies Conference Europe (ISGT), 2010.
- [80] N. Liu, J. Zhang, H. Zhang, W. Liu, Security assessment for communication networks of power control systems using attack graph and MCDM, IEEE Trans. Power Delivery 25 (2010) 1492–1500.
- [81] T. Sommestad, M. Ekstedt, L. Nordstrom, Modeling security of power communication systems using defense graphs and influence diagrams, IEEE Trans. Power Delivery 24 (2009) 1801–1808.
- [82] D. Kundur, X. Feng, S. Liu, T. Zourntos, K. L. Butler-Purry, Towards a framework for cyber attack impact analysis of the electric smart grid, in: Proc. of IEEE Conference on Smart Grid Communications, 2010.
- [83] U. Premaratne, J. Samarabandu, T. Sidhu, R. Beresh, J.-C. Tan, Security analysis and auditing of IEC61850-based automated substations, IEEE Trans. Power Delivery 25 (2010) 2346–2355.
- [84] J. Yang, Y. Chen, W. Trappe, Detecting spoofing attacks in mobile wireless environments, in: Proc. of IEEE SECON '09, 2009.
- [85] J. Yang, Y. Chen, W. Trappe, J. Cheng, Determining the number of attacks and localizing multiple adversaries in wireless spoofing attacks, in: Proc. of IEEE INFOCOM '09, 2009.
- [86] Y. Sheng, K. Tan, G. Chen, D. Kotz, A. Campbell, Detecting 802.11 MAC layer spoofing using received signal strength, in: Proc. of the 27th IEEE Conference on Computer Communications (INFOCOM '08), 2008.
- [87] A. L. Toledo, X. Wang, Robust detection of MAC layer denial-of-service attacks in CSMA/CA wireless networks, IEEE Trans. Inform. Forensics and Security 3 (2008) 347–358.
- [88] A. Hamieh, J. Ben-Othman, Detection of jamming attacks in wireless ad hoc networks using error distribution, in: Proc. of IEEE ICC '09, 2009.
- [89] J. Cabrera, L. Lewis, X. Qin, W. Lee, R. Prasanth, B. Ravichandran, R. Mehra, Proactive detection of distributed denial of service attacks using mib traffic variables-a feasibility study, in: 2001 IEEE/IFIP International Symposium on Integrated Network Management Proceedings, 2001, pp. 609–622.
- [90] K. Pelechrinis, G. Yan, S. Eidenbenz, S. V. Krishnamurthy, Detecting selfish exploitation of carrier sensing in 802.11 networks, in: Proc. IEEE INFOCOM 2009, 2009, pp. 657–665.
- [91] F. Cleveland, Enhancing the reliability and security of the information infrastructure used to manage the power system, in: Proc. of the IEEE Power and Energy Society General Meeting (PES '07), 2007.
- [92] P. P. Parikh, M. G. Kanabar, T. S. Sidhu, Opportunities and challenges of wireless communication technologies for smart grid applications, in: Proc. of IEEE power and Energy Society General Meeting (PES '10), 2010.
- [93] A. D. Wood, J. A. Stankovic, G. Zhou, DEEJAM: Defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks, in: Proc. of IEEE SECON '07, 2007, pp. 60–69.
- [94] J. T. Chiang, Y.-C. Hu, Dynamic jamming mitigation for wireless broadcast networks, in: Proc. of IEEE INFOCOM '08, 2008.
- [95] V. Navda, A. Bohra, S. Ganguly, D. Rubenstein, Using channel hopping to increase 802.11 resilience to jamming attacks, in: Proc. of IEEE INFOCOM '07, 2007, pp. 2526–2530.
- [96] A. Goldsmith, Wireless Communications, Cambridge University Press, 2005.
- [97] R. A. Scholtz, Multiple access with time hopping impulse modulation, in: Proc. of IEEE MILCOM, 1993.
- [98] C. Popper, M. Strasser, S. Capkun, Anti-jamming broadcast communication using uncoordinated spread spectrum techniques, in: IEEE Journal on Selected Areas in Communications, 2010.
- [99] W. Xu, W. Trappe, Y. Zhang, Anti-jamming timing channels for wireless networks, in: Proc. of ACM Conference on Wireless Security (WiSec), 2008, pp. 203–213.
- [100] M. J. Mihaljevic, R. Kohn, On wireless communications privacy and security evaluation of encryption techniques, in: Proc. of IEEE Wireless Communications and Networking Conference (WCNC '02), 2002.
- [101] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, Analyzing and modeling encryption overhead for sensor network nodes, in: Proc. of ACM International Conference on Wireless Sensor Networks Applications, 2003.
- [102] Y. W. Law, J. Doumen, P. Hartel, Benchmarking block ciphers for wireless sensor networks, in: Proc. of IEEE International Conference Mobile Ad-hoc Sensor Systems (MASS '04), 2004.
- [103] G. Gaubatz, J.-P. Kaps, E. Ozturk, B. Sunar, State of the art in public-key cryptography for wireless sensor networks, in: Proc. of IEEE International Conference Pervasive Computing Commun. Workshops (PERCOMW), 2005.
- [104] H. Khurana, R. Bobba, T. Yardley, P. Agarwal, E. Heine, Design principles for power grid cyber-infrastructure authentication protocols, in: Proc. of the Forty-Third Annual Hawaii International Conference on System Sciences (HICSS '10), 2010.
- [105] N. Liu, J. Zhang, W. Liu, Toward key management for communications of wide area primary and backup protection, IEEE Trans. Power Delivery 25 (2010) 2030–2032.
- [106] Q. Wang, H. Khurana, Y. Huang, K. Nahrstedt, Time-valid one-time signature for time critical multicast data authentication, in: Proc. of the IEEE Conference on Computer Communications (INFOCOM '09), 2009.
- [107] C. Szilagyi, P. Koopman, Low cost multicast authentication via validity voting in time-triggered embedded control networks, in: Proc. of IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2009.
- [108] C. Szilagyi, P. Koopman, Low cost multicast authentication via validity voting in time-triggered embedded control networks, in: Proc. of Workshop on Embedded System Security, 2010.
- [109] IEC Standard, IEC 62351: Data and communication security.
- [110] Y. Challal, H. Bettahar, A. Bouabdallah, A taxonomy of multicast data origin authentication: issues and solutions, IEEE Communications Surveys Tutorials (2004) 34–57.
- [111] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, B. Pinkas, Multicast security: a taxonomy and some efficient constructions, in: Proc. IEEE Conference on Computer and Communications (INFOCOM '99), 1999.
- [112] A. Perrig, R. Canetti, D. Song, J. D. Tygar, Efficient and secure source authentication for multicast, in: Proc. of Net-

- work and Distributed System Security Symposium, (NDSS '01), 2001, pp. 35–46.
- [113] A. Perrig, R. Canetti, J. D. Tygar, D. Song, Efficient authentication and signing of multicast streams over lossy channels, in: Proc. of IEEE Symposium on Security and Privacy, 2000, pp. 56–73.
 - [114] D. Naor, A. Shenhav, A. Wool, One-time signatures revisited: Have they become practical? (2005) 1–20. URL <http://eprint.iacr.org/2005/442.pdf>
 - [115] L. Reyzin, N. Reyzin, Better than BiBa: Short one-time signatures with fast signing and verifying, in: Proc. of Seventh Australasian Conference on Information Security and Privacy, 2002.
 - [116] NIST, NIST Special Publication 800-57: Recommended for Key Management. Part 1: General (Revised) (2007) 1–142.
 - [117] S. Rafaeli, D. Hutchison, A survey of key management for secure group communication, ACM Computing Surveys 35 (2003) 309–329.
 - [118] A. M. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure, P. Spilling, A survey of key management in ad hoc networks, IEEE Communications Surveys and Tutorials 8.
 - [119] I. Rouf, H. Mustafa, M. Xu, W. Xu, R. Miller, M. Gruteser, Neighborhood watch: Security and privacy analysis of automatic meter reading systems, in: Proc. of ACM Conference on Computer and Communications Security (ACM CCS), 2012.
 - [120] C. Beaver, D. Gallup, W. Neumann, M. Torgerson, Key management for SCADA. URL <http://www.sandia.gov/css/documents/013252.pdf>
 - [121] R. Dawson, C. Boyd, E. Dawson, J. Manuel, G. Nieto, SKMA - a key management architecture for SCADA systems, in: Proc. of Australasian Workshops on Grid Computing and E-Research, 2006.
 - [122] D. Choi, H. Kim, D. Won, S. Kim, Advanced key-management architecture for secure SCADA communications, IEEE Trans. Power Delivery 24 (2009) 1154–1163.
 - [123] D. Choi, S. Lee, D. Won, S. Kim, Efficient secure group communications for SCADA, IEEE Trans. Power Delivery 25 (2010) 714–722.
 - [124] S. Mittra, Iolus: A framework for scalable secure multicasting, in: Proc. of ACM SIGCOMM, 1997.
 - [125] W. He, Y. Huang, R. Sathiyam, K. Nahrstedt, W. C. Lee, SMOCK: A scalable method of cryptographic key management for mission-critical wireless ad-hoc networks, IEEE Trans. Inform. Forensics and Security 4 (2009) 140–150.
 - [126] J. Zhang, M. H. Firooz, N. Patwari, S. K. Kasera, Advancing wireless link signatures for location distinction, in: Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom '08), 2008.
 - [127] Y. Liu, P. Ning, H. Dai, Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures, in: Proceedings of the IEEE Symposium on Security and Privacy, 2010.
 - [128] P. L. Yu, J. S. Baras, B. M. Sadler, Physical-layer authentication, IEEE Trans. Inform. Forensics and Security 3 (2008) 38–51.
 - [129] J. Zhang, S. K. Kasera, N. Patwari, Mobility assisted secret key generation using wireless link signatures, in: Proceedings of the IEEE Conference on Computer Communications (INFOCOM'10), 2010.
 - [130] R. Bobba, O. Fatemeh, F. Khan, A. Khan, C. A. Gunter, H. Khurana, M. Prabhakaran, Attribute-based messaging: Access control and confidentiality, ACM Trans. Information and System Security 13 (2010) 4.
 - [131] R. Bobba, H. Khurana, M. AlTurki, F. Ashraf, PBES: A policy based encryption system with application to data sharing in the power grid, in: Proc. of the 4th ACM Symposium on Information, Computer and Communications Security (ASIACCS '09), 2009.
 - [132] G. Dini, M. Tiloca, Considerations on security in zigbee networks, in: Proc. of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), 2010.
 - [133] J. Zhang, C. A. Gunter, Application-aware secure multicast for power grid communications, in: Proc. of IEEE Conference on Smart Grid Communications, 2010.
 - [134] M. Majdalawieh, F. Parisi-Presicce, D. Wijesekera, DNPsec: Distributed network protocol version 3 (DNP3) security framework, in: Advances in Computer Information, and Systems Sciences, and Engineering: Proceedings of IETA 2005, 2006, pp. 227–234.
 - [135] L. H. Jeffrey, H. G. James, C. P. Sandip, Cyber security enhancements for SCADA and DCS systems, Technical Report TR-ISRL-07-02, University of Louisville (2007) 1–27.
 - [136] G. Gilchrist, Secure authentication for DNP3, in: Proc. of IEEE Power and Energy Society General Meeting (PES '08), 2008, pp. 1–3.
 - [137] I. H. Lim, S. Hong, M. S. Choi, S. J. Lee, T. W. Kim, S. W. Lee, B. N. Ha, Security protocols against cyber attacks in the distribution automation system, IEEE Trans. Power Delivery 25 (2010) 448–455.
 - [138] F. Li, B. Luo, P. Liu, Secure information aggregation for smart grids using homomorphic encryption, in: Proc. of IEEE Conference on Smart Grid Communications, 2010.
 - [139] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris, D. Barthel, Secure lossless aggregation for smart grid M2M networks, in: Proc. of IEEE Conference on Smart Grid Communications, 2010.
 - [140] G. M. Coates, K. M. Hopkinson, S. R. Graham, S. H. Kurkowski, A trust system architecture for SCADA network security, IEEE Trans. Power Delivery 25 (2010) 158–169.
 - [141] N. Kuntze, C. Rudolph, M. Cupelli, J. Liu, A. Monti, Trust infrastructures for future energy networks, in: Proc. of IEEE power and Energy Society General Meeting (PES '10), 2010.
 - [142] A. Hamlyn, H. Cheung, T. Mander, L. Wang, C. Yang, R. Cheung, Computer network security management and authentication of smart grids operations, in: Proc. of the IEEE Power and Energy Society General Meeting (PES '08), 2008.
 - [143] P. McDaniel, S. McLaughlin, Security and privacy challenges in the smart grid, IEEE Security and Privacy 7 (2009) 75–77.
 - [144] H. Khurana, M. Hadley, N. Lu, D. A. Frincke, Smart-grid security issues, IEEE Security and Privacy 8 (2010) 81–85.