Chapter 3
Wireless Infrastructure in Industrial Control Systems

Selcuk Uluagac, Kemal Akkaya, Apurva Mohan, Mehmet H. Cintuglu, Tarek Youssef, Osama Mohammed, and Daniel Sullivan

3.1 Introduction

The diverse components of an ICS discussed in the previous chapter must communicate with other components of the ICS. To do so, they are often connected within a "wired" communication architecture. Although wired connections render valuable reliable services to the infrastructure elements, nature or man-made disasters can damage the ICS wired communication infrastructure. It is just one of the reasons why wireless technologies are gradually gaining popularity in ICS architectures, especially as ICS systems undergoing extensive upgrade efforts in the last few years. Nevertheless, although wireless technologies (e.g., Wireless Local Area Network [WLAN]) are maturing and standardizing (NIST 2009) as viable solutions, they are not yet fully exploited as part of upgrade efforts.

Still, replacement of wired communications with wireless is likely to continue at an accelerated pace. This is because incorporating wireless technologies into existing ICSs can bring many benefits including: (1) lowering installation costs and maintenance, (2) providing ad-hoc on-demand deployment architecture that is robust and agile in responding to cyber and physical threats, and (3) providing redundancy, which is critically important in ICSs.

S. Uluagac (✉) • K. Akkaya • M.H. Cintuglu • T. Youssef • O. Mohammed
Department of Electrical & Computer Engineering, Florida International University, Miami, FL, USA
e-mail: suluagac@fiu.edu

A. Mohan
Honeywell ACS Labs, Integrated Security Technology, Golden Valley, MN, USA

D. Sullivan
Adelphi Laboratory Center, US Army Research Laboratory, Adelphi, MD, USA

E.J.M. Colbert, A. Kott (eds.), *Cyber-security of SCADA and Other Industrial Control Systems*, Advances in Information Security 66,
DOI 10.1007/978-3-319-32125-7_3

In this chapter, we explore how current state-of-the art wireless communications technologies could be utilized in ICSs with a goal to protect these systems against malicious cyber and physical activities. To provide a more concrete context for this discussion, we focus on an ICS as applied to smart grid systems. We first provide a general overview of the wireless technologies that can be used by ICSs, exploring the suitability of current wireless technologies with ICSs. Then, we discuss the pertinent cyber and physical threats to the ICSs. Next, as a case study, we discuss how an existing smart grid system could be integrated with the wireless technologies, focusing on the implementation of a real smart grid hardware/software testbed developed at the Electrical and Computer Engineering Department at the Florida International University.

3.2 Wireless Technologies for ICSs

In this section, we first discuss the benefits of including wireless technologies into ICSs. Then, we explore different wireless technologies for the ICSs.

A typical wired ICS infrastructure considering a multi-tier Smart-Grid architecture is given in Fig. 3.1 as an example. In the architecture, the data is collected by the field devices including, phasor measurement units [PMUs], PLCs, IEDs during the different phases of the smart grid (i.e., power generation, transmission, and distribution). Moreover, the customer side with smart meters and electrical vehicles is also included in this ICS infrastructure.

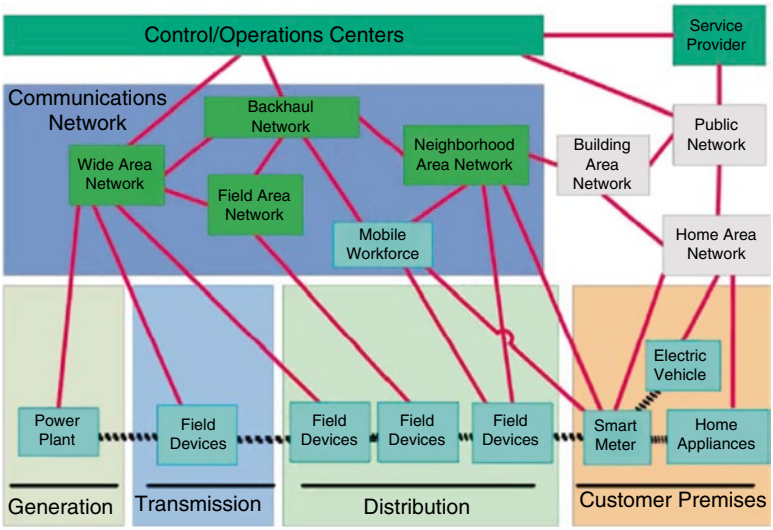

Fig. 3.1 An example ICS communication architecture (e.g., smart grid)

All these devices at different phases are normally connected with wires to the communication architecture. Although wired connections render valuable reliable services to the infrastructure elements, nature or man-made disasters can damage the ICS communication infrastructure. In fact, deploying wireless-enabled equipment (e.g., PMUs, PLCs, IEDs, smart meters) in lieu of wired ones in an ICS infrastructure brings several benefits. The equipment can be easily deployed without redundant cables. In this way, the cost of cabling and installation for the infrastructure can be further decreased with the integration of wireless equipment. There are numerous wireless technologies that can offer different communication ranges. This provides a flexible deployment strategy where even redundancy, which is a desired feature in an ICS architecture against failures, can be achieved. Even in disaster conditions, the wireless equipment can be easily integrated into the ICS architecture and operations can be recovered faster than a fully wired ICS infrastructure. This type of infrastructure-independent integration of wireless equipment can provide a self-healing feature to the damaged ICS infrastructure. Finally, the impact on the higher layer protocols that are used in the ICS network (e.g., IEC 61850, DNP3) to carry the collected data would be minimum because only the physical layer (wireless medium) will be changed in the protocol stack.

As ICSs collect mostly sensor data from devices, the need for bandwidth and speed may not be as stringent as other technologies. Instead, the primary design objectives are reliability, adaptability, availability, safety, and scalability. To this end, several wireless technologies have been designed and are being used in ICS infrastructures for a number of years now. According to a recent report (Moore 2013) about wireless use in industry, the protocols in significant use are IEEE 802.11x (23 %), Bluetooth (21 %), and cellular (15 %). IEEE 802.11x and cellular systems are technologies that are also adopted broadly outside the ICS environment and are well-understood. The newest version for low energy Bluetooth Low Energy (BLE) is gaining wide adoption in ICS systems. Moreover, about a third of the wireless protocols used in ICS such as Wireless HART, ISA 100.11a, Z-Wave, and Zigbee are proprietary. Microwave and satellite technologies are also used for accessing the RTUs within and beyond line-of-sight, respectively. These wireless protocols are briefly introduced in the rest of this section. Note that pertinent security threats will be articulated in Sect. 3.3.

3.2.1 WirelessHART

WirelessHART is a technology from the Highway Addressable Remote Transducer (HART) Communication Foundation, which is one of the widely used industrial standard for real-time applications (Song et al. 2008; Yang et al. 2010). It is a centralized wireless network that uses a central network manager to provide static routing and communications schedules. WirelessHART builds its physical layer based on IEEE 802.15.4-2006 and specifies the Data Link, Network, Transport, and Application layers as seen in Table. 3.1.

The network manager in WirelessHART maintains a complete list of all devices and has full knowledge of the network topology. It gets this information by pulling the neighbor tables from each network device. This neighbor table contains a list of all devices that a network device can connect to. Each node can act as a router on behalf of others. The network manager is also responsible for network configuration and network monitoring. Within this network manager, there is a security manager, which will be responsible for key generation. These devices are shown in Fig. 3.2.

Table 3.1 Wireless HART protocol stack

TCP/IP layer	Wireless HART layer
Application	Predefined data types
TCP/UDP	Reliable stream transport
IP	Graph-based redundant mesh routing
MAC	IEEE 802.15.4 compliant TDMA
Physical	IEEE 802.15.4 2.4 GHz

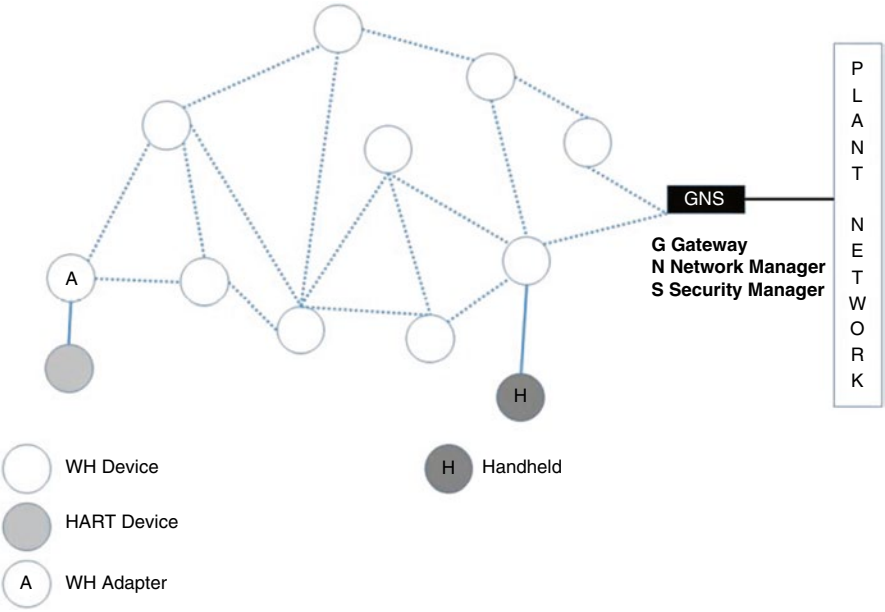

Fig. 3.2 WirelessHART protocol operation illustration (Nixon and Round Rock 2012)

3.2.2 ISA 100.11a Standard

Similar to WirelessHART, ISA 100.11a is suitable for applications in the electric power system such as a substation or a generation plant (Akyol et al. 2010). It describes a mesh network designed to provide secure wireless communication to process control. It builds the Data Link Layer, Network Layer, Transport Layer, and Application layer; on top of the Physical layer of IEEE 802.15.4-2006 as shown in Table 3.2.

ISA100.11a supports two types of network topology: star and mesh. ISA100.11a has routing mechanisms at two different levels: (1) subnet-level mesh routing, and (2) back-bone-level routing. While subnet-level mesh routing is performed at the data link layer, backbone-level routing is performed at the network layer. At the subnet-level, graph routing and source routing are used. Different from Wireless HART, it is based on User Datagram Protocol (UDP) and can work with Ipv6 through the use of Ipv6 over Low power Wireless Personal Area Network (6LowPAN), which is an adaptation layer to support 128 bit IP addresses.

The network architecture for ISA 100.11a is very similar to that of Wireless HART in terms of meshing among the involved nodes such as sensors, actuators and portable devices. It also uses a gateway that is capable of providing security and network management as shown in Fig. 3.3.

Table 3.2 ISO 100.11a protocol stack

TCP/IP layer	ISO 100.11a layer
Application	ISA native protocols
TCP/UDP	UDP
IP	6LowPAN
MAC	IEEE 802.15.4
Physical	IEEE 802.15.4 2.4 GHz

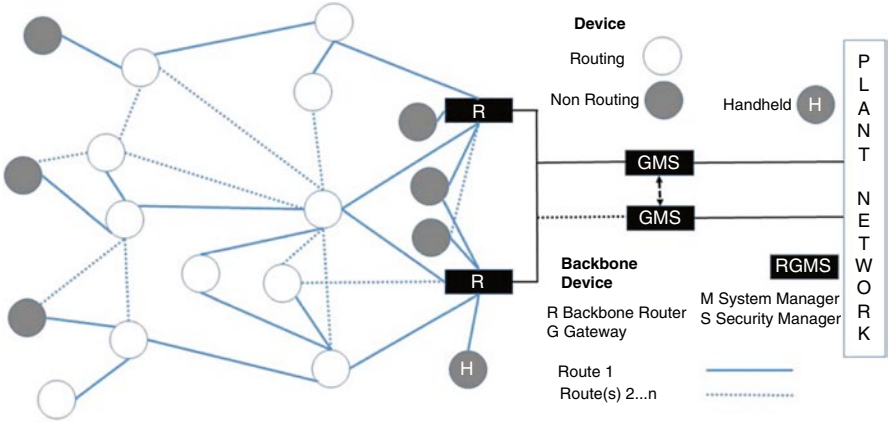

Fig. 3.3 ISA 100.11a (Nixon and Round Rock 2012)

3.2.3 Z-Wave

Z-Wave is a proprietary technology developed by Zen-Sys (Z-wave 2015) and is intended for home control and automation (Gomez and Paradells 2010). Z-Wave has two basic types of devices: controller and slave. A controller device can issue control commands while a slave is an end device that executes commands from the controller. Controllers are differentiated further based on their functions in the network. A primary controller is the only controller in the Z-Wave mesh network that has the ability to include or exclude devices in the network and hence it has the latest network topology in its routing table. Other controllers copy their information from the primary controller when they join the network. Typical primary controllers are portable (e.g., a battery-operated remote control) while secondary controllers are typically static and connected to a power source. Slave devices may also forward a message if the received command message requested them to do so. A special slave, called a routing slave, is allowed to send messages to other nodes without being requested to do so. A routing slave has predefined static routes to some nodes when it joins the network.

Z-Wave employs a source routing mechanism at the routing layer. The controller that initiates the message stores a complete route of up to four hops to the destination in the frame. Every intermediate node forwards the message according to this route.

3.2.4 Zigbee

ZigBee is the specification of a low-cost, low-power wireless communications solution, meant to be integrated as the main building block of ubiquitous networks (Zigbee Alliance, 2009). It is maintained by the ZigBee Alliance, which develops the specification and certifies its proper implementation. ZigBee defines a communication layer at layer 3 and above in the Open System Interconnection (OSI) model. Zigbee transmits at 868 MHz, 915 MHz, and 2.4 GHz in the Industrial, Scientific, Medical (ISM) radio band at 250 kbps with a range up to 10 m. However, the distance to send data is much greater when multiple radios form a mesh network. It builds on the foundation of the IEEE 802.15.4 standard at the MAC and physical layers. These layers are shown in Table 3.3. There are three kinds of nodes in a ZigBee network: coordinator, end device, and router. These nodes can organize in a mesh or tree-based architecture

Table 3.3 Zigbee protocol stack

TCP/IP layer	Zigbee
Application	Application objects
TCP/UDP	Application support sublayer
IP	Zigbee tree or mesh
MAC	IEEE 802.15.4
Physical	IEEE 802.15.4 2.4 GHz

to communicate the collected data from sensors to a root node. Zigbee is an open standard and has been used for many other applications such as Internet of Things. Hence, it can be easily adapted to use in a wireless-enabled ICS infrastructure.

3.2.5 Bluetooth

Bluetooth is based on the open IEEE 802.15.1 standard and operates in the 2.4 GHz ISM band. The Bluetooth Special Interest Group (SIG) maintains the standard. Bluetooth is susceptible to interference from other devices, which emit radio frequencies (RF) in this band such as Zigbee, Wi-Fi, microwave ovens, baby monitors, welding machines, and high voltage lines. Bluetooth is available in two versions: Classic Bluetooth and Bluetooth low-energy (BLE). Accelerometers, temperature and pressure sensors are available with Bluetooth, and vendors can offer new features (called profiles) for an ICS such as RS-232 or RS-485 emulation in order to replace serial wires (Nilsson 2013). One use of Bluetooth is in pole-mounted RTUs for the electrical grid. A technician can drive close to a utility pole and access the RTU remotely with a laptop computer without de-energizing the transmission lines or placing personnel at risk (connectBlue 2011). Bluetooth operates in a master-slave paradigm. One master node can communicate with 7 slave nodes in a piconet. The role of master and slave can be changed between nodes. Bluetooth has 128 bit authentication and encryption. Prior to Bluetooth version 4.1, the Secure and Fast Encryption Routine+(SAFER+) block cipher provided the cryptographic algorithms. In BLE, Advanced Encryption Standard-Counter with Cipher Block Chaining Media Authentication Code (AES-CCM) is the cipher. See NIST Special Publication 800-121 Rev 1 for guidelines to secure Bluetooth links (NIST 2012). Devices can be up to 10 meters apart, and longer range modules can extend the range to 1 km line of sight (Publitek European Editors 2013). Bluetooth currently does not have a mesh capability, however, the SIG formed a Bluetooth Smart Mesh Working Group to design an architecture for mesh networks (Bluetooth SIG 2015).

3.2.6 Microwave

Microwave links are used in SCADA and EMS to connect the control center with remote RTUs, which are in line-of-sight. Utilities are replacing microwave towers with fiber optic cables along their pipeline or transmission tower right-of-ways, however, microwave relays can be useful when crossing rivers. Microwave is ultra-high frequency (UHF) radio operating between 1 GHz to 300 GHz. Microwave can be deployed in point-to-point links or point-to-multipoint. Point-to-point links have transceivers at each site and directional antennas. Point-to-multipoint networks will have a master station with an omni-directional antenna (Marihart 2001). Microwave is vulnerable to interception and the frequencies of

licensed carriers are available from the Federal Communications Commission (FCC). While legacy microwave towers may not encrypt their links, today's microwave radios are available with built-in encryptors, which are certified as Federal Information Processing Standard 140-2 compliant.

3.2.7 Satellite

Very small aperture satellites (VSAT) link the control centers with remote sites which are beyond line of sight, and therefore, unsuitable for microwave. Examples of VSAT use in ICS are communications with offshore oil platforms or electrical substations, which do not have telephone service. Also, VSAT can enable an EMS to monitor substations separated by forests and mountain ranges. The remote VSAT sites operate in a star topology by exchanging messages with a central satellite hub. Two technologies are available for VSAT service and they have their own strengths. One technology is Time Division Multiple Access (TDMA) and the second is Single Channel Per Carrier (SCPC). With TDMA, each VSAT terminal has a time slot to exchange messages the satellite operations center. Multiple customers can share the satellite link bandwidth, which can result in cost savings. However with SCPC, a dedicated link exists between the satellite hub and each VSAT terminal. SCPC may have a greater cost of ownership than TDMA for a large number of VSAT sites (EMC Satcom Technologies 2015).

3.3 Cyber and Physical Threats to Wireless ICSs

In this section, we discuss the security of the wireless-enabled ICS infrastructure. First, we introduce a generic threat model, and then articulate specific threats for the wireless ICS technologies. Finally, we list the desired security services for the wireless ICS.

3.3.1 Generic Threat Model

Conceptually, the threats to the wireless-enabled smart grid could be listed from four different complementary perspectives: (1) Method-specific, (2) target-specific, (3) protocol-specific, and (4) identity-specific.

Method-specific threats define how the threats are executed. The method-specific threats can be either passive or active. In the passive method, the attacker only monitors (or eavesdrops), records the communication data occurring in the wireless medium, and analyzes the collected ICS data to gain meaningful information. In the active one, the attacker tries to send fake authentication messages, malformed packets, or replay a past communication to the components

of the ICS infrastructure. As passive threats are surreptitious, it is harder to catch their existence. However, it is easier to catch the existence of an active attacker, but its damage to the smart grid can be relatively higher than the passive threats.

Target-specific threats classify the attacks according to which device the threats target. Any device such as IEDs, PMUs, PLCs, and smart meters could be valuable targets for potential malicious activities.

In *protocol-specific threats*, the attackers aim to exploit the vulnerabilities associated with the networking protocols, software suits (DNP3, IEC 61850, IEEE C37.118 Syncrophasor Protocol, Modbus, etc.) that run in the smart grid. Finally, depending on the identity of the attacker, i.e., whether an attacker is a legitimate member of the network during an attack or not, she can be defined as insider or outsider attacker. Insiders are more dangerous than the outsiders as they have more knowledge about the internal architecture of the wireless-enabled ICS infrastructure.

In reality, there is no hard line between these attacking models and they complement each other because an insider could be a passive attacker trying to exploit IEC 61850 on an IED in the ICS infrastructure. The threat model for the wireless-enabled ICS infrastructure is presented in Fig. 3.4.

3.3.2 Specific Threats for Wireless ICS Technologies

In this sub-section, we present specific threats to wireless technologies in ICS. These specific threats are based on the proprietary protocols (e.g., WirelessHART, ISA 100.11.a, ZigBee, etc.) introduced in the previous section.

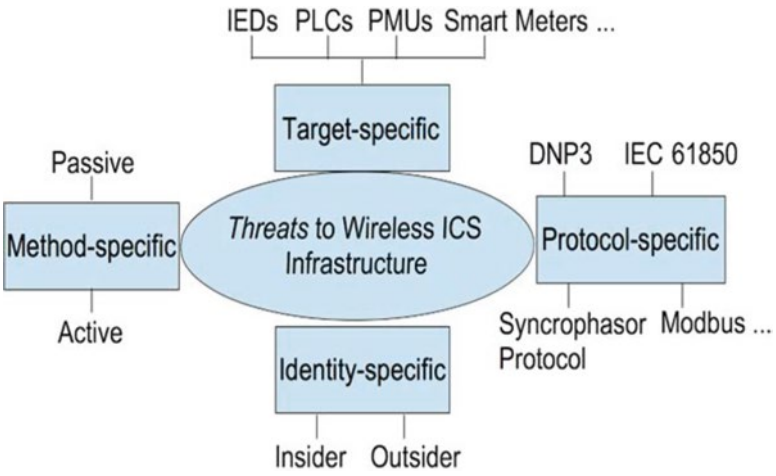

Fig. 3.4 Threats to wireless ICS infrastructure

Those proprietary protocols are typically not well-vetted and often times rely on the fact that their design and implementation are not known to the general public. This is partly true because hackers find it easiest to attack protocols with well-known and published vulnerabilities, but this fact alone does not provide enough security to proprietary protocols.

Key Generation, Distribution, and Management—Secure key generation, distribution, and management are one of the biggest challenges in securing industrial wireless systems. Proprietary systems face this challenge even more because proprietary key management schemes to build trust could become a big impediment to interoperability. One of the security threats in proprietary systems arise with key generation using protocols that are non-compliant to NIST 140-2 standard (NIST 2011). Also maintaining a secure out of band channel for distributing keys, and their management aspects like revocation, refresh, providing desirable properties like forward and backward secrecy are non-trivial challenges. Adding to the complexity is the fact that deployed systems have unique environmental and deployment characteristics which constrain the solution set available for designing secure mechanisms. Standardized protocols like ZigBee, WirelessHART, or ISA 100.11a use specific key management mechanisms. Although standardized protocols have a well-vetted key management mechanisms, vulnerabilities in the systems typically stem from faulty design or weaker implementation. Sometimes when new constraints are added to well-vetted protocols, it leads to lowering the security. BLE is an example of this where additional constraints to energy usage led to a redesign of the existing security mechanisms making them weaker and vulnerable to many attacks (La Polla et al. 2013). The current version of BLE is 4.0 which has a number of well-known vulnerabilities like eavesdropping, secret key brute force leading to integrity and confidentiality compromise, vulnerable key exchange, guessable pseudo random number sequence for frequency hopping, etc. most of which were not present in the parent Bluetooth protocol.

Jamming—Jamming is a common problem in personal area network wireless technologies. Jamming can occur inadvertently due to high levels of noise especially for protocols in the ISM band, but such jamming is temporary and does not have a huge negative consequence. On the other hand, jamming can be used as an effective tool by an attacker to create availability issues in wireless systems. This becomes especially concerning if the wireless device is a control device and making it unavailable could enable a hacker to gain unauthorized access to resources or removing control of an ICS process leading to a disaster.

Battery exhaustion attacks—This attack is executed when an attacker engages a wireless device to perform some computation while being anonymous. The attacker continues the operation until the battery of the device is completely exhausted, leading to availability issues. An example of this could be an attacker trying to authenticate to a wireless device using an automated script. This becomes a larger problem in remote unmanned areas where replacing the battery at regular intervals could be a problem.

Resource-constrained end devices—Resource constrained end devices using wireless technologies have fewer resources like processing and memory to dedicate to the security functions. An example would be a device with an 8 or 16 bit

microcontroller with limited memory. Often, these devices are not capable of implementing security best practices and are forced to compromise with weaker implementations. However, with cheaper memory and faster processors this risk is become a lesser concern.

Protection on the device—Lack of advanced protection technologies on wireless end devices is another specific attack vector. Protecting security secrets like crypto keys, certificates, credentials, etc. on end devices is a challenge that opens up avenues for attackers. Newer devices are using more advanced mechanisms that block access to them in the field post-deployment, however, this problem still plagues legacy devices.

3.3.3 Desired Security Mechanisms

Desired security mechanisms are usually defined by the national and international standardization bodies (e.g., National Institute of Standards and Technology [NIST], International Telecommunication Union [ITU]) and are used by many researchers and practitioners who aim to develop secure systems. In this sub-section, we use the security architecture suggested by the ITU's Recommendation X.800 (ITU 1991) documentation, which is referred to as the Security Architecture for Open Systems Interconnect (OSI) as our guideline in addressing the threats discussed in the previous sub-section.

Confidentiality: Confidentiality refers to the protection of the exchanged content (e.g., gathered data, reports, commands) among the components of the ICS infrastructure devices such as IEDs, PMUs, PLCs, Smart Meters. A malicious entity, which has the privilege to access the content, should not be able to decode the exchanged messages in the network. Confidentially also entails the protection against any unintended information leakage from the applications, controllers, and devices within the ICS infrastructure. This is particularly important because the data generated and collected by any ICS equipment, e.g., PMUs, IEDs are usually very periodic. Data collection policies associated with the collected data may be discovered with simple timing or side-channel analysis. Similarly, an increased delay in the traffic can inform a potential attacker about the behavior of the ICS infrastructure. This unintended information disclosure from data devices, applications, and ICS controllers should also be considered as part of any confidentiality service.

Traditionally, confidentiality can be provided by adopting either symmetric or asymmetric key-based encryption schemes (Stallings and Brown 2015). In symmetric encryption, one key is utilized among the PMUs, PLCs, smart meters, IEDs, applications, and other networking equipment and controllers. Examples of symmetric encryption that can be utilized for the smart grid include AES, Rivest Cipher 4 (RC4). On the other hand, in asymmetric encryption, a pair of two keys (aka public and private) are utilized among the communicating components of the ICS infrastructure. RSA and elliptic curve cryptography (ECC) are the two most important examples of asymmetric encryption that could be deployed. Moreover, the maturing state-of-the art encryption mechanisms

based on fully-homomorphic-encryption (FHE) (Gentry 2009) could be utilized for specifically preserving the privacy of the traffic. FHE ensures that a user's personal information is not leaked to servers or a third party.

Specifically, the FHE encryption scheme, ε, has an algorithm, $Evaluate_{\varepsilon}$ that, given plaintext, $\neq_1, \neq_2, \ldots, \neq_t$, for any valid ε, private, public key pair (sk, pk), any circuit C, and any ciphertext $\psi_i \leftarrow Encrypt(pk, \pi_i)$, yields

$$\psi \leftarrow Evaluate_{\varepsilon}(pk, C, \psi_1, \psi_2, \ldots, \psi_t) \tag{3.1}$$

such that $Decrypt_{\varepsilon}(sk, \psi) = C(\pi_1,,,\pi_2,,,\ldots,,,\pi_t)$

A typical scenario of FHE is illustrated in Fig. 3.5. The user sends the information encrypted with public key, pk, by function *Encrypt* to the server. The server does operations on the encrypted numbers with function *Evaluate* with pk and outputs ψ. The server sends ψ back to the user. The user, then, decrypts with function *Decrypt* using her private key sk and obtains the result of $C(\pi_1,,,\pi_2,,,\ldots,,,\pi_t)$. In this way, the server conducts the desired operation for the user without acquiring any plaintext.

Authentication: Authentication involves guaranteeing the genuineness of the communication among the ICS infrastructure devices. An authentication mechanism verifies if the exchanged information stems from the legitimate participants of the infrastructure because a malicious entity (e.g., a compromised IED) may be able to inject counterfeit content or resend the same content into the ICS. More specifically, an adversarial ICS application may attempt to insert fake application data that may circumvent policies imposed by other applications. Adversaries may also insert malicious data to damage the system by influencing the state estimation, which is crucial to evaluate the system demand.

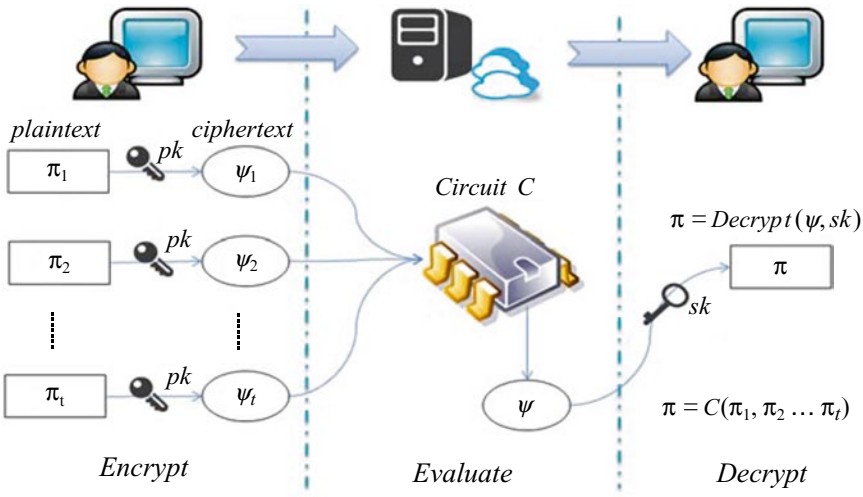

Fig. 3.5 Illustration of fully homomorphic encryption

Authentication can fundamentally be provided based on three factors (Stallings and Brown 2015): (1) *Knowledge factor*: the proof of the knowledge of some secret (e.g., passwords) is provided to the authenticator. Symmetric, asymmetric key-based encryption schemes, and hashing algorithms can all be utilized as part of the authentication mechanism with the knowledge factor. (2) *Possession factor*: authenticator verifies the claimant using the credentials provided by a specialized hardware. Electronic cards, smart cards, smart tokens physically owned by the claimant can be utilized and integrated with the wireless-enabled ICS infrastructure devices and applications. (3) *Identity factor*: the authenticator utilizes features uniquely identifying in the verification of the claimant. Both static or dynamic patterns that can identify the devices and applications can be utilized. For instance, behavioral information from the devices and applications such as communication patterns, timing patterns, delays can all be utilized (Liu et al. 2014) as part of this authentication method. Within the wireless-enabled ICS infrastructure, all of these authentication techniques can be individually or a combination of one or more of the techniques could be adopted. If more than one factor is utilized, the authentication is called multi-factor authentication.

Integrity: Integrity refers to the capability to detect if the exchanged content between the communicating devices of the ICS infrastructure have been altered or not. Moreover, the integrity service involves ensuring that the exchanged content is not deleted, replication of old data, counterfeit, or stale because the nature of the messages in the wireless-enabled ICS infrastructure is very time-sensitive.

Integrity is usually provided by appending the cryptographic digest of the message content to the message itself (Stallings and Brown 2015). When the PMUs, PLCs, IEDs, applications, networking equipment and controllers receive the message, they can check to see if the digest of the content matches the digest they compute on their end. If the digests match each other, then the message is deemed legitimate and not to have changed from its original content. Content digests in integrity are usually created with the usage of hashing algorithms. There are several hashing algorithms such (e.g., MD5, Secure Hash Algorithm-2 [SHA-2]) in use today, which do not require the presence of keys unless they are specifically designed to work with keys like keyed- hashing (e.g., hash message authentication code [HMAC], cipher-based authentication code [CMAC]). Alternatively, integrity can be provided as part of a digital authentication mechanism utilizing symmetric and asymmetric encryption techniques. For instance, the last block of the encrypted data in AES can be appended to the message that would be sent as the integrity code. In a similar fashion, a private key in the asymmetric encryption techniques (e.g., RSA, ECC) can be used to pro-vide the integrity code appended to the message.

Access Control: With access control, unauthorized use of a resource in the wireless-enabled ICS infrastructure is prevented. Access control addresses permissible actions that an entity of the ICS infrastructure has with content or a service. For instance, IEDs should not be allowed to have the privileges on PMUs. Proper security measures must prevent any unauthorized access. An unauthenticated application might try to access resources for which it does not have authorized privileges. Or, an authenticated application, IED, PMU, or PLC may abuse its privileges.

Access control is usually achieved through four different methods (Stallings and Brown 2015): (1) *discretionary access control* (*DAC*); (2) *mandatory access control* (*MAC*); (3) *role-based access control* (*RBAC*); and (4) *attribute-based access control* (*ABAC*). In DAC, access control decisions are made based on the exclusive rights that are set for the applications, IEDs, PMUs, and PLCs. An entity in DAC can enable another entity to access its resources. In MAC, access control function considers the criticality of the resources, rights of the applications, and the ICS devices dependent on the resources. In MAC, an entity can not enable another entity for to access its resources. In RBAC, access control decisions are based on the roles created within the ICS infrastructure. A role can include more than one entity e.g., IEDs. Moreover, a role defines the capabilities of an entity with a certain role. Finally, in ABAC, the access control decisions are based on the features of the applications, IEDs, PMUs, and PLCs, resources to be accessed, and environmental conditions.

Availability: Due to the threats to wireless-enabled ICS infrastructure, some portion of the infrastructure or some of the functionalities or services provided by the ICSs could be damaged and unavailable to the participants of the infrastructure. For instance, some PLCs could be compromised and they could cease functioning. A Denial-of-Service (DoS) type attack can overwhelm the communication links. In a similar fashion, an ICS device can be a single point of failure. Moreover, adversaries may jam the wireless medium, effectively hampering all the communications. Thus, high availability ensures that the necessary functionalities or the services provided by the wireless-enabled ICS infrastructure are always carried out, even in the case of attacks.

Usually, an ICS infrastructure usually includes redundant components to ensure the continuous operation during failures. In a similar fashion, the wireless-enabled ICS infrastructure can be designed with such redundancy to achieve high availability.

Accountability: With accountability (aka non-repudiation (Stallings and Brown 2015)) wireless-enabled ICS infrastructure ensures that a device or a software component (e.g., applications, IEDs, PMUs, and PLCs) can not refute the reception of a message from the other device or application or the sending of a message to the other device or application in the communication.

Accountability can be provided as a service bundled inside authentication and integrity. For instance, a digital signature scheme (DSS) (Stallings and Brown 2015), which is based on utilizing encryption methods would address accountability. Additionally, proper auditing mechanisms and logs should be utilized to provide accountability in the wireless-enabled ICS infrastructure.

3.3.4 Additional Security Mechanisms

In this sub-section, we will present some security mechanisms to address the cyber threats identified in the threat model in Sect. 3.3.2.

Key Generation, Distribution, and Management—The threats in key generation, distribution, and management are typically addressed by conforming to standards and implementing best practices in wireless systems. For example, secure

key related process standards like NIST 140-2 provide guidance. Protocols also leverage deployment specific characteristics for leveraging infra-structural support. For example, in advanced metering infrastructure (AMI), the metering infrastructure is used as a secure out of band mechanism to exchange shared secret keys. Key generation can be done using software libraries that are compliant with NIST 140-2 making it easier for systems to main compliance.

Jamming—Jamming of wireless channels is a hard problem to counter directly as it exploits the physical properties of wireless systems by drastically reducing the SNR on the wireless channel. As such, jamming risks are mitigated by a number of compensating controls in wireless systems. Traditional mechanisms like frequency hopping are deployed. Additionally, heartbeat signals, acknowledgements, anomaly detection (high SNR for some periods of time), etc. are used to detect and mitigate jamming in wireless systems.

Battery Exhaustion Attacks—Battery exhaustion attacks may not be completely avoidable, but their impact can be minimized in most cases. Techniques such as prolonging the sleep time for devices, rapid message filtering before more interactive processing of messages, etc. are mechanisms to minimize their impact.

Resource constrained devices could use hardware based security provided by cryptographic chips to secure cryptographic information on the devices. Hardware based protection can provide strong protection for cryptographic keys, certificates, etc. as well as provide on chip support for cryptographic algorithms like SHA-256 and AES-256.

3.4 Integration of Wireless Technologies to an Existing ICS Infrastructure: Smart Grid and Micro-Grid Case

In this section, we study how wireless technologies can be integrated into an existing testbed. For this, we utilize the Smart Grid Testbed located within the Electrical and Computer Engineering Department at Florida International University (FIU) as a case study as part of our ongoing work (Salehi et al. 2012a, b)

3.4.1 FIU Smart Grid Testbed

The FIU Smart Grid Testbed is shown in Fig. 3.6. The FIU testbed provides an excellent environment for implementation and validation of the wireless communication infrastructure and providing security against the threats. It consists of a small scale AC/DC hybrid power system, which includes reconfigurable transmission lines and bus bars, several microgrids, storage devices, and a variety of renewable energy emulators for wind turbines, photovoltaic (PV) solar panels, and fuel cells. All these devices are inter-connected for control purposes and serves as a research and education laboratory for real-time, real-world smart grid applications (Youssef et al. 2015).

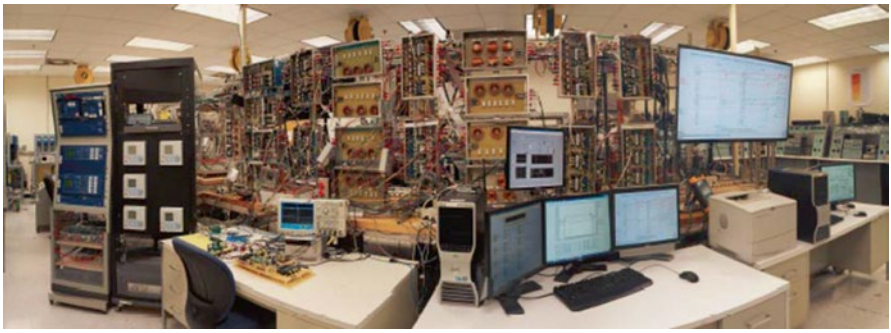

Fig. 3.6 A view of the Smart Grid testbed at Florida International University (FIU)

In a smart grid, wide-area monitoring and protection aims to provide protection and control for globally interconnected transmission networks. One or several Phasor Data Concentrators (PDC) are operated as central controller which collects substation measurements from the deployed phasor measurement units (PMUs) on transmission level (Cintuglu et al. 2015a, b; Cintuglu and Mohammed 2013a, b; Mazloomzadeh et al. 2013a, b, 2015; Mohamed et al. 2013). Measurements from dispersed substations are collected in a central controller to monitor system status in very precise synchronization. The time synchronization is generally established using Inter-Range Instrument Group-B (IRIG-B) code by a satellite clock to have a proper time reference value from a global positioning system (GPS) clock to accomplish reliable synchronized measurements from the whole network. In a wide-area protection and control scheme, central control units may force local substations to carry out mandatory emergency and remedial actions such as controlled islanding in case of blackout. Under-frequency load shedding schemes and aggregated distributed generation control can be adopted according to global monitoring feedback.

As part of our ongoing work to upgrade the FIU Smart Grid testbed, a wireless-enabled (PMU)/IED and PLC components are shown in Fig. 3.7 a and b, respectively. In these devices, the current and voltage analog measurements are converted to digital values via with analog/digital converters. The sampling rate defines the frequency response of the anti-aliasing filters. The sampling clock is phase-locked with the GPS clock pulse. The microprocessor calculates the positive sequence of the current and voltage measurement values. The time-stamp is created identifying the universal time coordinated (UTC). PMU time-stamped measurements are transferred over the wireless medium to the PDC using one of the technologies discussed earlier. PLCs are used as wireless power system field actuators for load switching, governor control, and automatic voltage regulator (AVR) control.

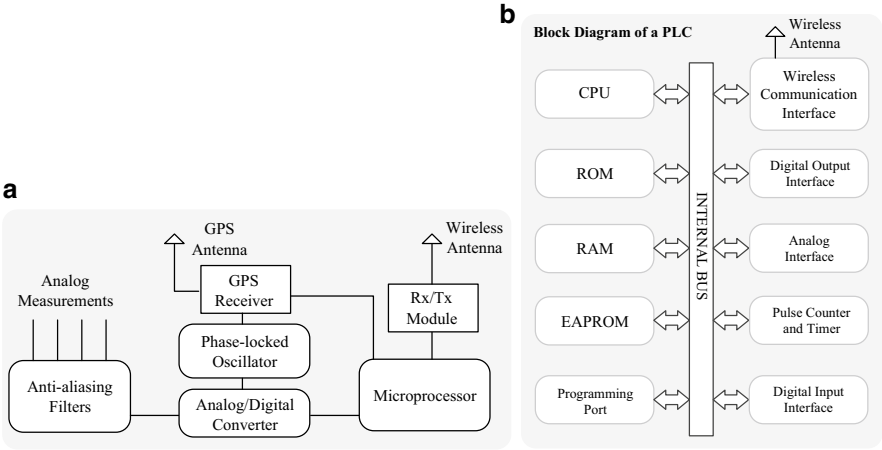

Fig. 3.7 (**a**) PMU/IED components, (**b**) PLC block diagram

3.4.2 Test Case: Handling Islanding Situation via Wireless Communication

Power systems would result in instability when exposed to severe abnormal contingencies, natural disasters, and man-made attacks. Depending on generation and load balance, this spurs an islanding condition. When the power import is terminated by an islanding situation, the initial generation and load imbalance causes a frequency drop (Cintuglu and Mohammed 2013a, b; Mazloomzadeh et al. 2015). Spinning reserve of the generators is utilized to respond to the frequency fall in accordance with droop adjustments. The recovery can continue until all generator valves are fully open. Beyond this point, load shedding and the stored energy reserve of microgrids should be initiated to enable continuous recovery. A wireless-enabled infrastructure can allow for optimal efficiency in the integrated operation of the entire system during recovery in an islanding situation (Cintuglu et al. 2015a, b; Cintuglu and Mohammed 2013a, b).

Specifically, we first formulate the problem as an optimization problem, which involves the minimization of the sum of all generation and distributions costs over the islanded network, subject to generation capacity constraints, load balance requirements, and any other limitations that need to be taken into account. The decisions involve the selection of loads to shed at the disruption instance, the amount of power to be generated at each of the sources, e.g., microgrids, and the allocation of the generated power over the local loads. This is a complex nonlinear optimization problem due to the dependence between load shedding decisions and subsequent generation and resource allocation decisions, which introduce integer variables and non-convexities in standard formulations of the problem. Hence, development of special solution procedures is required to address this initial deterministic decision problem.

To demonstrate the basics of this problem setup, we provide the following general description involving a sample cost structure. Without loss of generality, assume that the islanded area consists of a set M of microgrids only, where each microgrid

m∈M corresponds to a generation source. Moreover, let L refer to the set of local loads. In the recovery stage, depending on the aggregated microgrid capacity, local generation must match local loads:

$$\sum_{i=1}^{N} S_{Gi} - \sum_{j=1}^{M} S_{Lj} \geq 0 \tag{3.2}$$

where S_G is the complex power generated by each of the |M| sources and S_L is the complex power consumed by each of the |L| loads. Whenever the load surpasses the generation, the following intelligent load-shedding conditions are take place:

$$P_{ILS} = P_{island} - \sum_{i=1}^{M} P_{triplist} \tag{3.3}$$

$$Q_{ILS} = Q_{island} - \sum_{i=1}^{M} Q_{triplist} \tag{3.4}$$

$P_{triplist}$ and $Q_{triplist}$ are respectively a list of the active and reactive power needs of the loads ordered by priority. P_{island} and Q_{island} are respectively the total active and reactive power of the substation in islanded mode. Thus, P_{ILS} and Q_{ILS} determine if the substation has enough active and reactive power resources to meet the loads. The synchronous generator will have the typical quadratic cost function given:

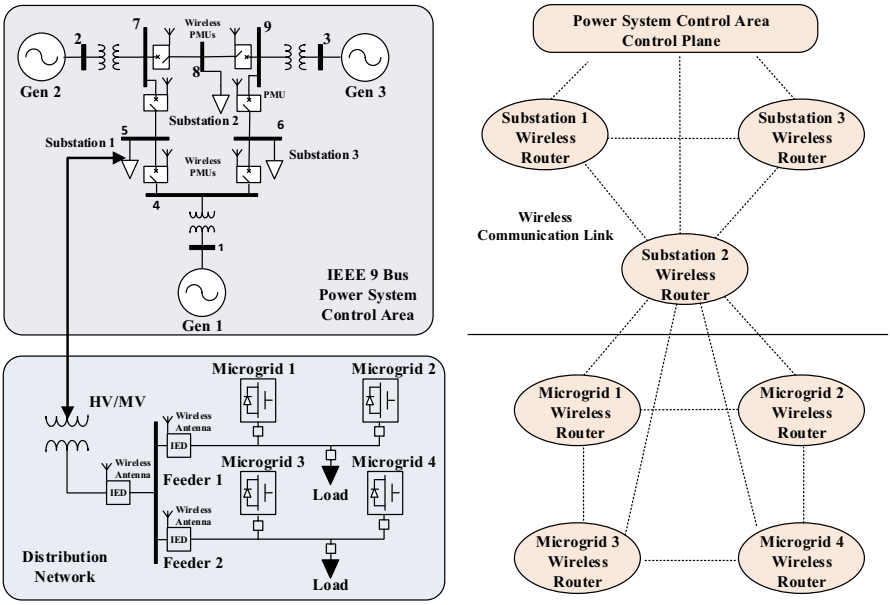

Fig. 3.8 Physical power system and wireless communication links

$$F_i\left(P_{Gi}\right) = \sum_{i=1}^{n} a_i + b_i P_i + c_i P_i^2 \tag{3.5}$$

A high level view of this communication and the control infrastructure model with wireless equipment is given in Fig. 3.8. Wireless communication links between substation and microgrid wireless-enabled PMUs are established along with the power system physical infrastructure.

3.5 Summary and Conclusions

Deploying wireless-enabled equipment in an ICS infrastructure brings several benefits.

The equipment can be deployed more easily, the deployment strategy is more flexible, deployment costs are typical smaller, and operations can be recovered faster in the case of system failure. A wireless deployment only involves changing the physical layer for ICS communication protocols. ICSs can have a much lower bandwidth requirement and transmission speeds may not be as stringent. Some examples of wireless communication protocols used in ICSs are given in the chapter.

The security of the wireless-enabled ICS infrastructure can be accomplished by combating threats in the following four perspectives: (1) Method-specific, (2) target-specific, (3) protocol-specific, and (4) identity-specific. Some examples of specific security issues are key generation, key distribution, key management, jamming (intentional and noise), battery resource exhaustion attacks, and the lack of security features in wireless end devices. Security architectures from NIST and the ITU are available to improve confidentiality, authentication, integrity, access control, availability, and accountability in wireless infrastructure.

Integrating wireless technologies into ICS infrastructure presents ample unique research challenges in security and networking to engineers and scientists. As a case study, we discussed how an existing smart grid with several micro-grids could be integrated using wireless technologies. Security research of wireless ICS infrastructure is ongoing in the smart grid hardware/software testbed at the Florida International University.

References

Akyol, B., Kirkham, H., Clements, S., & Hadley, M. (2010). *A survey of wireless communications for the electric power system*. Prepared for the US Department of Energy.

Bluetooth Special Interest Group. (2015). *Bluetooth technology adding mesh networking to spur new wave of innovation*. Retrieved June 24, 2015, from http://www.bluetooth.com/Pages/Press-Releases-Detail.aspx?ItemID=224.

Cintuglu, M.H., Elsayed, A., & Mohammed, O.A. (2015). Microgrid automation assisted by synchrophasors. *6th Innovative Smart Grid Technologies Conference (ISGT North America), Washington, DC*.

Cintuglu, M.H., Ma, T., & Mohammed, O.A. (2015). Aggregated active distribution networks for secondary control of islanded power systems. *IEEE Power & Energy Society General Meeting*.

Cintuglu, M. H., & Mohammed, O. A. (2013). Islanding detection in microgrids. *Power and Energy Society General Meeting (PES)*.

Cintuglu, M. H., & Mohammed, O. A. (2013). Simulation of digitalized power systems using PMU and intelligent control. *48th IEEE IAS Annual Meeting, Orlando, USA*.

connectBlue. (2011). *Wireless access to pole mounted RTUs*. Retrieved June 12, 2015, from http://www.connectblue.com/fileadmin/Connectblue/Web2006/Documents/References/Schneider_Electric_RTU.pdf.

Gentry, C. (2009). *A fully homomorphic encryption scheme*. Ph.D. thesis, Stanford University.

Gomez, C., & Paradells, J. (2010). Wireless home automation networks: A survey of architectures and technologies. *IEEE Communications Magazine, 48*, 92–101.

ITU Recommendation X.800. (1991). *Security architecture for open systems interconnection for CCITT applications*. International Telecommunications Union.

La Polla, M., Martinelli, F., & Sgandurra, D. (2013). A survey on security for mobile devices. *IEEE Communications Surveys & Tutorials, 15*(1), 446–471.

Liu, W., Uluagac, A., & Beyah, R. (2014). Maca: A privacy-preserving multi-factor cloud authentication system utilizing big data. *IEEE INFOCOM Big Data Workshop*, pp. 518–523.

Marihart, D. (2001). Communications technology guidelines for EMS/SCADA systems. *Institute of Electrical and Electronic Engineers (IEEE) Transactions on Power Delivery, 16*(2), 181–1188. Retrieved June 24, 2015, from http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=915480.

Mazloomzadeh, A., Cintuglu, M. H., & Mohammed, O. A. (2013). Islanding detection using synchronized measurement in smart microgrids. *IEEE PES Conference on Innovative Smart Grid Technologies Latin America (ISGT LA), Sao Paulo, Brazil*, pp. 1–7.

Mazloomzadeh, A., Cintuglu, M. H., & Mohammed, O. A. (2015). Development and evaluation of a laboratory based phasor measurement devices. *Accepted for Presentation and Publication at the 6th Innovative Smart Grid Technologies Conference (ISGT North America), Washington, DC, USA*.

Mazloomzadeh, A., Mohammed, O., & Zonouz, S. (2013). TSB: Trusted sensing base for the power grid. *IEEE SmartGridComm symposium, Vancouver, Canada*.

Mohamed, A. G., Youssef, T., & Mohammed, O. A. (2013). Wide area monitoring and control for voltage assessment in smart grids with distributed generation. *Proceedings of the 2013 PES Innovative Smart Grid Technologies Conference (ISGT North America), Washington, DC, USA*.

Moore, T. (2013). *The world market for wireless technology by share of units in industrial applications*. Retrieved from http://www.controleng.com/single-article/research-wireless-use-in-industry/5b97f5d429813c649a05240ad5efd280.html.

National Institute of Standards and Technology. (2012). *Guide to Bluetooth security (NIST SP 800-121 Rev 1)*. Gaithersburg, MD. Retrieved June 24, 2012, from http://csrc.nist.gov/publications/drafts/800-121r1/Draft-SP800-121_Rev1.pdf.

Nilsson, R. (2013). *Industrial wireless: Bluetooth can be robust, easy to use*. Retrieved June 12, 2015, from http://www.controleng.com/single-article/industrial-wireless-bluetooth-can-be--robust-easy-to-use/cbd481b6e65b08d2e743f8e09fb95528.html.

Nixon, M., & Round Rock, T.X. (2012). *A comparison of WirelessHART™ and ISA100*. 11a. Whitepaper, Emerson Process Management.

Publitek European Editors. (2013). *Using Bluetooth for data communications in industrial automation*. Retrieved June 12, 2015, from http://www.controleng.com/single-article/industrial-wireless-bluetooth-can-be-robust-easy-to-use/cbd481b6e65b08d2e743f8e09fb95528.html.

Salehi, V., Mohamed, A., Mazloomzadeh, A., & Mohammed, O. A. (2012a). Laboratory-based smart power system, part I: Design and system development. *IEEE Transactions on Smart Grid, 3*(3), 1394–1404.

Salehi, V., Mohamed, A., Mazloomzadeh, A., & Mohammed, O. A. (2012b). Laboratory-based smart power system, part II: Control, monitoring, and protection. *IEEE Transactions on Smart Grid, 3*(3), 1405–1417.

EMC Satcom Technologies. (2015). *TDMA vs. SCPC*. Retrieved June 24, 2015, from http://www.emcsatcom.com/component/docman/doc_download/26-tdma-vs-scpc-in-satellite-networks%3FItemid%3D&ei=l7GKVda3KMO4ggTOg4CwDA&usg=AFQjCNHi_RE2U7Yt4s7L7kYx60zBbcEbFg&bvm=bv.96339352,d.eXY.

Song, J., Han, S., Mok, A., Chen, D., Lucas, M. & Nixon, M. (2008). WirelessHart: Applying wireless technology in real-time industrial process control. *IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS)*, pp. 377–386.

Stallings, W., & Brown, L. (2015). *Computer security: Principles and practice* (3rd ed.). Prentice Hall.

The US National Institute of Standards and Technology (NIST) (2009). *The smart grid interoperability standards roadmap*. Electric Power Research Institute (EPRI). Tech. Rep.

The US National Institute of Standards and Technology (NIST). (2011). *FIPS PUB 140-2, Security requirements for cryptographic modules.*

Yang, D., Xu, Y., & Gidlund, M. (2010). Coexistence of ieee802.15.4 based networks: A survey. *IECON 2010—36th Annual Conference on IEEE Industrial Electronics Society*, pp. 2107–2113.

Youssef, T. A., Elsayed, A., & Mohammed, O. A. (2015). DDS based interoperability framework for smart grid testbed infrastructure. *15th IEEE International Conference on Environments and Electrical Engineering*.

Zigbee Alliance. (2009). *IEEE 802.15. 4, ZigBee standard*. On http://www.zigbee.org.

Z-Wave Alliance. (2015). On http://z-wavealliance.org.