Security Considerations in WSN-Based Smart Grids

Hanen Idoudi 1, Mustafa Saed 2

1 National School of Computer Science, University of Manouba, Tunisia
 hanen.idoudi@ensi.rnu.tn

2 Electrical and Computer Engineering, University of Detroit Mercy, USA
 saedma@udmercy.edu

Abstract—Wireless Sensor Networks (WSNs), which are composed of battery powered devices, are attracting a tremendous attention owing to their wide range of applications. Recently, their use in the smart grid to respond to several communication needs was stressed. A Smart Grid is an innovative paradigm to enhance the power grid system with communication capabilities in order to perform several tasks of monitoring and surveillance. Despite their advantages, there are several challenges facing WSN applications in the Smart Grid. Security is one of the most critical challenges. In this paper, the application of WSNs in smart grid is reviewed, and the security issues accompanying their use are discussed.

Keywords—Smart Grid, Wireless Sensor Networks, Security Threats

I. INTRODUCTION

The Smart Grid is intended to provide a next-generation electrical network supported with configurability, assessment and self-monitoring features. This new paradigm relies on information and communication technology to perform these tasks.

Wireless technologies and Wireless Sensor Networks (WSNs) for instance, were proposed as an interesting and efficient support for communications in Smart Grid.

Wireless Sensor Networks consist of small resource constrained devices that can organize themselves into a multi hop wireless network [1]. WSNs are used in a wide range of potential applications including military, medical systems, and robotic exploration. This in turn explains why researchers in the field were motivated by these types of networks in their research work.

Recently, WSNs have been adopted in Smart Grids [3, 4] because they feature rapid deployment, low cost and flexibility, and aggregated intelligence via parallel processing. While existing remote sensing, monitoring, and fault diagnostic solutions are too expensive, WSNs provide cost-effective sensing and communication solution in a remote and online setting.

WSNs are applied by utility companies and suppliers for substation automation management in addition to wireless automatic meter reading (WAMR) system. They are intended to measure and monitor the energy usage or the power lines quality and in some cases, provide a real time feedback on systems misbehavior to allow timely fault detection and avoidance tasks. Advantages of WSN applications in Smart Grid are numerous since they can offer timely and efficient monitoring of the power grid and can reduce operational costs by eliminating the need for human readers and provide an automatic pricing system for customers [5].

On the other hand, WSNs brought new challenges and issues when applied to the Power Grid. Serious security threats induced by these types of communication technologies must be dealt with efficiently to prevent the malfunctioning of the vital power grid.

The rest of this paper is organized as follows: the overview of the Smart Grid paradigm is presented in section 2. Section 3 discusses the WSNs characteristics and their applications in Smart Grid, and section 4 reviews the WSN-based Smart Grid security issues.

II. SMART GRID OVERVIEW

The smart grid is a new architecture for electric power grid infrastructure using sophisticated transmission and distribution communication networks to deliver electricity [9], [10]. The goal of smart grid is to improve the efficiency, reliability and safety of the electric systems through the new architecture of communication technologies, automated control, and dynamic optimization of electric system operations, maintenance, and planning. The main characteristics of the smart grid include information technology, automation, and interaction to provide the two-way data communication. Fig. 1 shows typical smart grid infrastructure (the combination of power system and the information
system of smart grid). It illustrates network connections of the end to end smart grid system. These connections pinpoint the communication and data management from the customer to collector to utility control center and to transmission and distribution substations where the electronic controllers are located.

The electronic controllers manage the generation and flow of electrical power. The residence block in the figure demonstrate the home area network and the components are used to communicate to smart grid network, such as smart thermostat, smart water heater, smart appliances and smart meter. There are two ways of the wireless connection in the home area network devices to a smart controller/meter through a network; Zigbee and Wi-Fi.

III. WIRELESS SENSOR NETWORKS AND SMART GRID

Wireless sensor networks (WSNs) are composed of small and resource-constrained devices communicating wirelessly and organized according to a multi-hop wireless network to route information to a specific control unit called sink. A node in the WSN has one or more sensors, embedded processor, moderate amount of memory and transmitter/receiver circuitry. Because of their wide range of potential applications including military, medical systems, precision agriculture and robotic exploration, wireless sensor networks have become a promising technology for Smart Grids.

In this section, the characteristics of WSN when applied in Smart Grids are reviewed, and then an overview of their applications in a Smart Grid context is covered.

A. WSN-based Smart Grid benefits and challenges

To perform communications in the Smart Grid, several technologies can be used [3]. However, given the adverse environment in which the Smart Grids are deployed, using a wireless infrastructure is the most suitable solution for this type of networks. Moreover, owing to their autonomous behavior, large-scale pervasive and inexpensive nature, wireless sensor networks (WSNs) are good candidate in such context.

Advantages of WSN applications in Smart Grid are abundant. These applications can offer timely and effective monitoring of the power grid, lower operational costs by abolishing the need for human readers, and offer an automatic pricing system for customers. WSNs are characterized by a straightforward and prompt deployment, low cost and flexibility and accumulated intelligence via parallel processing. They can deliver an interesting alternative to current remote sensing, monitoring and fault diagnostic solutions which are too expensive. On the other hand, WSNs provide cost-effective sensing and communication solution in a remote and online style.

Since sensor nodes are usually battery powered, conserving their energy and prolonging the network life time are considered primary goals for most of their applications when designing protocols for those networks. However, with the Smart Grids, this goal is no longer an issue since sensors can benefit directly from the power grid to be continuously powered. Hence, when establishing communications through WSNs within the context of Smart Grids other concerns must be taken into account. Deploying WSNs in a Smart Grid context introduces a number of challenges including:

- The consideration of the noisy environment produced by the electrical elements within the Smart Grid sensor nodes at the time of transmitting their data on the network.
- Taking into account the heterogeneity of both the sensor nodes and the traffic sent by the nodes.
according to the features for which the sensor node was designed.

- The need to ensure interoperability between WSNs and other existing wireless technologies to improve the reliability of data transmission to the control center.

- The security consideration which is already critical in Smart Grid and more critical with WSN.

**B. WSNs applications in Smart Grid**

WSNs are anticipated to be used essentially for Wireless automatic meter reading (WAMR) and Remote System Monitoring and Equipment Fault Diagnostics. Liu [5] classified the applications of WSNs into three categories: power generation, power delivery, and power utilization.

Since sensors are low cost and easy to deploy devices, they can be used in power generation units to measure several parameters such as steam, temperature, and air/fuel flow rates. This information is fed into the data acquisition system in the power plant for monitoring purposes to control generators' operation and prevent any malfunctioning through timely reporting of any faulty component or misbehavior.

WSNs can avoid or greatly alleviate power-grid and facility breakdowns when deployed along the power delivery systems for monitoring purposes. They can report on outage, abnormal activities and parameters thresholds, and allow timely maintenance. WSNs are envisioned to reduce electric utility operational costs by eliminating human readers. They can offer an online pricing system based on online energy consumption monitoring of customers. Besides, several home and building automation applications can benefit from WSNs including recommendation or regulatory systems for controlling power consumption of building and facilities [2],[6],[7].

**IV. SECURITY CONSIDERATIONS IN WSN-BASED SMART GRID**

Security of the WSN communications is one of the most important issues to deal with. WSNs suffer from many security threats due to their inherent characteristics. As is the case with all kinds of wireless networks, WSNs are more vulnerable to security threats originating from the open communication environment than wired networks. Unlike other wireless technologies, such as Wi-Fi, applying advanced and complex security mechanisms is not relevant due to their physical limitations. This complicates protection measures and makes WSNs more vulnerable to external attacks. Thus, WSN-based Smart Grid suffers from all the security threats facing classical WSN communications in addition to new security vulnerabilities. This complication will result in a large set of vulnerabilities to overcome.

**A. Security threats in WSN**

Many types of attacks on WSN exist. In a selective forwarding attack, malicious nodes may refuse to forward certain messages and destroy them, ensuring that they are not propagated any further. A simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet it receives. By this, neighboring nodes will conclude that the communication has failed and decide to seek another route.

In sinkhole attack, attacker advertises incorrect information, such as high quality route to a sink. An attacker can actually provide this kind of route connecting all nodes to real sink and then selectively drop packets. Because of the communication pattern (all traffic is directed to sink), WSNs are highly susceptible to this kind of attack since all the surrounding nodes of the adversary will start forwarding packets destined for a sink through the adversary, and also propagate the attractiveness of the route to their neighbors.

Sybil attack consists of a single node that pretends to be present at different parts of the network. The malicious node illegitimately presents multiple identities to other nodes in the network. The Sybil attack can significantly decrease the effectiveness of fault tolerant schemes, such as distributed storage, disparity and multipath routing, and topology maintenance.

Wormholes may convince two nodes to be neighbors when in fact they are far away from each other. Wormholes may convince distant nodes that they are close to sink. This may lead to sinkhole if a node on the other end advertises high-quality route to that sink.

Well placed wormhole can completely disorder routing since attackers may influence network topology by delivering routing information to the nodes before it would really reach them by multi hop routing. Wormholes may be used in conjunction with Sybil attack.

Nodes in WSNs learn about their neighboring nodes through HELLO packets, which are required by many WSN routing protocols. In a Hello flood attack, attackers can broadcast HELLO message to nodes and then advertise high-quality route to sink. Some routing protocols use link layer acknowledgments. Attackers may spoof acknowledgements to convince other nodes that a weak link is strong or that a dead node is alive. Consequently, a weak link may be selected for routing causing packets sent through that link to be lost or corrupted.

**B. Security threats in WSN-based Smart Grid**

The smart grid inherited all of the vulnerabilities of the traditional internet as a result of connecting the power grid to the network. These vulnerabilities demand high security measures to protect the smart grid. Through information technology, the smart grid allows customers to manage their energy services and access smart grid convenience features. However, this can cause damage to the smart grid system and
increase the possibility of cyberattacks and cascade failures propagating from one system to another [12]. The current electronic devices of the power grid do not support cryptography and data security. When the power grid was built, engineers and designers did not consider the security implementation in the electronic design. This was because there was no external communication to these electronic devices. Also, the communication between the customers and the power grid is a one-way communication, from the power grid to the customers. Therefore, the electrical power system does not have extra capacity to perform any security function. New security concerns arise when switching to the smart grid as a result of merging industrial control system (ICSs) and information technology (IT) [13]. Industrial control systems have been built without any consideration to security concerns. However, Information Technology considers security as a high priority. This requires changes to the ICS to upgrade the hardware and software of the power grid. Extra care must be taken to ensure these components will not increase vulnerabilities. Both ICS and IT personnel need to communicate with each other. There are considerable differences between the two technologies. The IT staff uses the patching server to update the system or add another level of access to the system and then forward the required update to all the hosts. This will cause the system to restart. Consequently, this will force the power grid to eventually shut down and cause blackout.

Another issue has to do with the power grid using a dedicated serial line that has low speed and very limited access. IT uses the TCP/IP protocol for communication in the Ethernet and Wi-Fi connection. This is characterized by high-speed communication and multiple accesses at the ftp server, telnet client, and web server. Consequently, many benefits to remote access and troubleshooting will be provided. Unfortunately, this will also create a new vulnerability for cyber-attacks.

The smart grid technology uses many new devices, such as Advance Meter Infrastructure (AMI), Smart Meter, and Demand Response, which allow customers to access their bills anytime in order to monitor the power consumption of home appliances and decide which one to shut down, turn on, or even schedule the appliances operation time. This will create security and privacy concerns. For example, if nobody is at home, a sophisticated cyber-attacks may result in tampering with electrical appliances. Advance Meter Infrastructure (AMI) device will be installed in residences to provide two-way communication between the customer and the power grid control center

1) Advanced Metering Infrastructure Security

Advanced Metering Infrastructure (AMI) is a part of the smart grid architecture and has been used to intelligently monitor and control power distribution and consumption [14]. AMI acquires and delivers fine-grained electricity measurements using two way communications through smart meters or other energy management devices to support real data reading in real-time services and dynamic load control in the end to end communication between end-users and energy providers.

The AMI plays a major role in controlling communications with the consumers. In AMI architecture there are two ways of the connection of the smart meters to collectors using either indirect connection or direct connection. In indirect connection, some smart meters are connected to other smart meters, which are in turn connected to the collector. In direct connection all smart meters are directly connected to the collector. In both connections, the collectors are connected to substations. Securing the AMI is vital to convince residents and business owners that smart grids are reliable and trustworthy. This implementation requires an AMI security profile to define and address all security concerns and find the solutions for these concerns. Setting up an AMI in each house and having it acting as an access point will demand monitoring, managing, and maintaining such devices [15]. The smart grid should deploy cryptography and key management to build a robust security implementation. Some of the smart grid devices permit physical access to the customer, such as smart meter, and advanced meter infrastructure. This may possibly lead to potential cryptanalysis. Furthermore, cryptography implementation requires complex hardware and software design support. All customer information and the power system must be encrypted to protect privacy and maintain integrity, and confidentiality [16]. Cryptography and key management shall be an appropriate solution to protect the smart grid from cyber-attacks, and tackle the physical access concerns of the smart grid security.

Fig. 2 depicts the direct and indirect smart meter-to-collector communication topology. The collector (C) is the center point between the substation and the smart meters (SMs) in direct connection, but in indirect connection the smart meters are connected in series to the collector, which is in turn connected to the substation.

![AMI Architecture- Smart Meters Connections Topology](image-url)
2) Utility Security

The software and the firmware will be managed by the utility, and data management between the customers and the substation will be carried out in the utility as well. This will increase the security concerns of hacking the system and vulnerabilities. Some signals travel with various vulnerabilities to many end-user devices through media networks, such as controlling and monitoring. In addition, concerns have been raised regarding the resistance of the smart grid and how it repairs itself without resulting in equipment or infrastructure damage, or blackout. The software and firmware in the system are responsible for protecting the system from unauthorized access by people, who are trying to intrude the system and tamper with databases and other information. For any application that needs to be applied in the smart grid, the secure software development life cycle should be taken into consideration. This will help to avoid the lack of oversight in this area and mitigate possible vulnerabilities to achieve security such as authentication vulnerability, authorization vulnerability, cryptographic vulnerability, input and output validation, password management vulnerability, link vulnerability and protocol errors.

3) Substation, Distribution, Transmission and Generation Security

Combining the information technology and electricity grid into smart grid network provides more efficient and reliable grid operations, and thus leads to a great many benefits, ranging from energy savings to a high degree of home automation. In spite of all benefits of the smart grid, the new technology it introduced exposes the system to many new threats. The traditional power grid automation system has been physically isolated from the corporate network. However, smart grid networks shall allow power grid automation to connect to public networks. This kind of connection will increase the vulnerability of hacking the power grid automation.

The current architecture of the power grid automation does not support the security needed to deter cyber-attacks. Wei et al. [17] proposed a new framework by introducing an additional layer of security to protect the power grid automation system from hackers and unauthorized people. They presented the needed security and safety when the power grid automation system is connected to public networks or the cloud, and divided the security layer into three major parts:

i. Security agents: The agents provide protection to the edge of the system to secure the network from the cyber-attacks. The security agents in the Control Center are more intelligent and complex than the security agents in the Intelligent Electronic Devices (IEDs).

ii. Managed Security Switch: This connects the Substations in the Control Center.

iii. Security Manager: The manager is located in the automation network and connected to switches using current IT security implementation.

V. DISCUSSION

Much work is yet to be done to enhance the security of the WSN-based smart grid network. In particular, the following should be taken care of:

1) Deploying the public key infrastructure (PKI) in the smart grid [18]. Using sensors brings limitations when using cryptographic solutions since lightweight cryptographic mechanisms should be designed to cope with physical and logical limitations of sensors.

2) Securing the trusted device profile and devising the smart grid certificate lifetime.

3) Ensuring the privacy concerns regarding customer information are resolved [19].

4) Following a robust security style for the smart grid as a future priority to achieve appropriate authentication for any device communication via the smart grid.

5) Addressing all the newly discovered vulnerabilities of the WSN-based smart grid by monitoring and tracking the communication and the data flow through the smart grid.

V. CONCLUSION

Smart grid is the next generation of power line networks. Supplying them with sensors is a key solution to support efficient and timely communication in Smart grid. Despite their advantages, WSN bring new security challenges that add to the existing smart grid security concerns. In WSN-based smart grid, both intrinsic smart grid security threats and WSN vulnerabilities should be addressed.

REFERENCES


