International Journal of Smart Grid and Clean Energy

Smart Grid Security: Threats, Vulnerabilities and Solutions

Fadi Aloul[a]*, A. R. Al-Ali[a] , Rami Al-Dalky[a], Mamoun Al-Mardini[a], Wassim El-Hajj[b]

[a] *Department of Computer Science & Engineering, American University of Sharjah, United Arab Emirates (UAE)*
[b] *Department of Computer Science, American University of Beirut, Lebanon*

Abstract

The traditional electrical power grid is currently evolving into the smart grid. Smart grid integrates the traditional electrical power grid with information and communication technologies (ICT). Such integration empowers the electrical utilities providers and consumers, improves the efficiency and the availability of the power system while constantly monitoring, controlling and managing the demands of customers. A smart grid is a huge complex network composed of millions of devices and entities connected with each other. Such a massive network comes with many security concerns and vulnerabilities. In this paper, we survey the latest on smart grid security. We highlight the complexity of the smart grid network and discuss the vulnerabilities specific to this huge heterogeneous network. We discuss then the challenges that exist in securing the smart grid network and how the current security solutions applied for IT networks are not sufficient to secure smart grid networks. We conclude by over viewing the current and needed security solutions for the smart gird.

Keywords: Smart grid security, information and communications technologies, advanced metering infrastructure

1. Introduction

Smart grids provide electricity demand from the centralized and distributed generation stations to the customers through transmission and distribution systems. The grid is operated, controlled and monitored using information and communications technologies (ICT). These technologies enable energy companies to seamlessly control the power demand and allow for an efficient and reliable power delivery at reduced cost. Via digital two-way communications between consumers and electric power companies, the smart grid system provides the most efficient electric network operations based on the received consumer's information. Security remains to be one of the most important issues in smart grid systems given the danger and inconvenience residents and companies alike might encounter if the grid falls under attack. Three main security objectives must be incorporated in the smart grid system: 1) availability of uninterrupted power supply according to user requirements, 2) integrity of communicated information, and 3) confidentiality of user's data.

The remainder of this paper is organized as follows. Section 2 gives a brief background about smart grids. Section 3 addresses the grid's main vulnerabilities. Section 4 talks about the various attackers and the types of attacks they can conduct. Section 5 points out the major challenges in proposing smart grid security solutions. Section 6 details the current and needed security solutions, and Section 7 summarizes the paper contributions.

2. Background

The National Institute of Standards and Technology (NIST) proposed a Smart Grid architecture

* Manuscript received June 15, 2012; revised August 15, 2012.
Corresponding author. Tel.: +(971) 6 5152784; fax: +(971) 6 5152979; *E-mail address*: faloul@aus.edu; aali@aus.edu.

composed of seven domains as shown in Fig. 1. The grid can be viewed as having two main components, system and network.

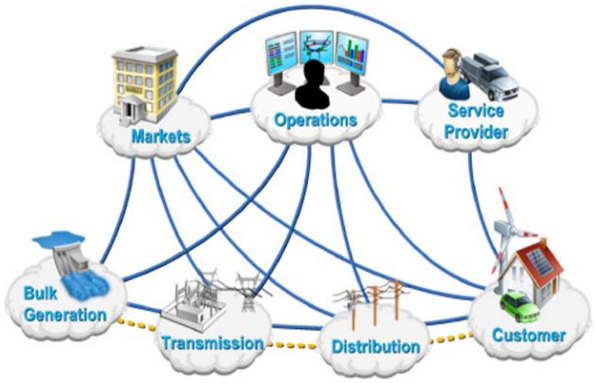

Fig. 1. Domains of a smart grid [NIST].

2.1 System Component

The major system components in smart grid are Electrical Household Appliances, Renewable Energy resources, Smart Meter, Electric Utility Operation Center and Service Providers.

*Electrical Household Appliances (*smart and legacy) are assumed to be able to communicate with smart meters via a Home Area Network (HAN) facilitating efficient power consumption management to all home devices.

Renewable Energy Resources are solar and wind energy that supply home appliances with local generate electricity.

Smart Meter is a stand-alone embedded system. Each smart meter contains a microcontroller that has non-volatile and volatile memory, analog/digital ports, timers, real-time clock and serial communication facilities. Smart meters register the power consumption periodically and transmit it to the utility server, connect or disconnect a customer power supply and send out alarms in case of abnormality. Some smart meters are equipped with relays that can be interfaced directly with smart home appliances to control them; for example, turn OFF the air conditioner during peak periods. Furthermore, the smart meter can be used in demand side management.

Electric Utility Center interacts with smart meters to regulate power consumption. It also sends consumption related instructions to smart meters and collects sub-hourly power usage reports and emergency/error notifications using General Packet Radio Service (GPRS) technology.

Service Providers establish contracts with users to provide electricity for individual devices. Service providers interact with internal devices via messages relayed by the smart meter. To establish such interaction, service providers should register with the electric utility and obtain digital certificates for their identities and public keys. The certificates are then used to facilitate secure communications with users.

2.2 Network Component

Smart grid incorporates two types of communication: Home Area Network (HAN) and Wide Area Network (WAN). A HAN connects the in-house smart devices across the home with the smart meter. The HAN can communicate using Zigbee, wired or wireless Ethernet, or Bluetooth. A WAN, on the other hand, is a bigger network that connects the smart meters, service providers, and electric utility. The WAN can communicate using WiMAX, 3G/GSM/LTE, or fiber optics. The smart meter acts as a gateway between the in-house devices and the external parties to provide the needed information. The electric utility manages the power distribution within the smart grid, collects sub-hourly power usage from smart meters, and sends notifications to smart meters once required. The smart meter receives messages from devices within HAN and sends them to the appropriate service provider. Figure 2 illustrates the basic architecture [1]. Note that while HANs are used in residential homes, Business Area Networks (BANs) and Industrial Area Networks (IANs) are used within business offices and industrial sites, respectively.

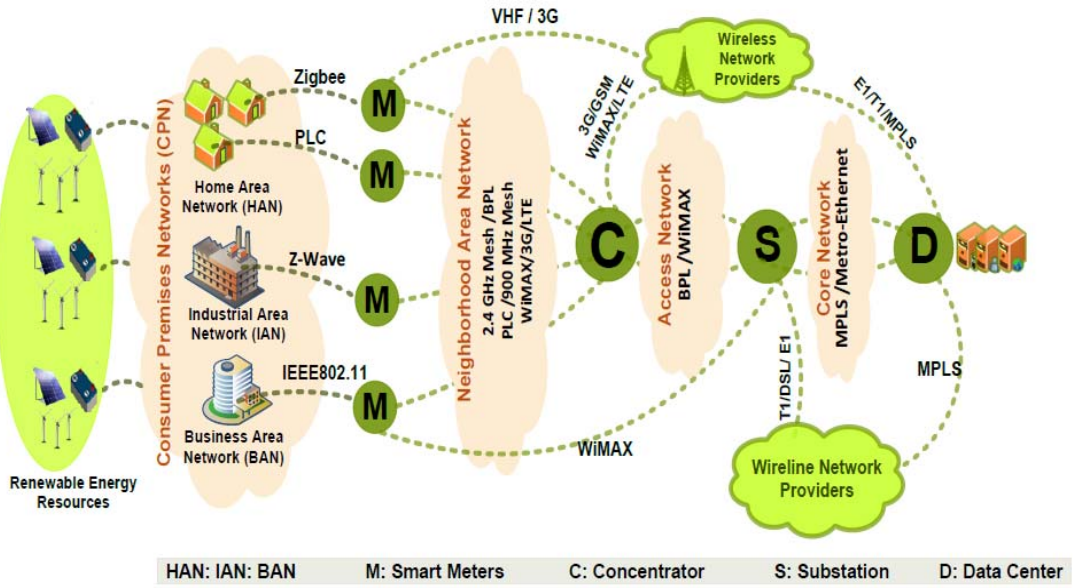

Fig. 2. Basic network architecture [1].

3. Vulnerabilities

Smart grid network introduces enhancements and improved capabilities to the conventional power network making it more complex and vulnerable to different types of attacks. These vulnerabilities might allow attackers to access the network, break the confidentiality and integrity of the transmitted data, and make the service unavailable. As proposed in [2],[3], the following vulnerabilities are the most serious in smart grids:

1) *Customer security*: Smart meters autonomously collect massive amounts of data and transport it to the utility company, consumer, and service providers. This data includes private consumer information that might be used to infer consumer's activities, devices being used, and times when the home is vacant.

2) *Greater number of intelligent devices*: A smart grid has several intelligent devices that are involved in managing both the electricity supply and network demand. These intelligent devices may act as attack entry points into the network. Moreover, the massiveness of the smart grid network (100 to 1000 times larger than the internet) makes network monitoring and management extremely difficult.

3) *Physical security*: Unlike the traditional power system, smart grid network includes many components and most of them are out of the utility's premises. This fact increases the number of insecure physical locations and makes them vulnerable to physical access.

4) *The lifetime of power systems*: Since power systems coexist with the relatively short lived IT systems, it is inevitable that outdated equipments are still in service. This equipment might act as weak security points and might very well be incompatible with the current power system devices.

5) *Implicit trust between traditional power devices*: Device-to-device communication in control systems is vulnerable to data spoofing where the state of one device affects the actions of another. For instance, a device sending a false state makes other devices behave in an unwanted way.

6) *Different Team's backgrounds*: Inefficient and unorganized communication between teams might cause a lot of bad decisions leading to much vulnerability.

7) *Using Internet Protocol (IP) and commercial off-the- shelf hardware and software*: Using IP standards in smart grids offer a big advantage as it provides compatibility between the various components. However, devices using IP are inherently vulnerable to many IP-based network attacks such as IP spoofing, Tear Drop, Denial of Service, and others.

8) *More stakeholders*: Having many stakeholders might give raise to a very dangerous kind of attack: insider attacks.

4. Attackers and Types of Attacks

The just mentioned vulnerabilities can be exploited by attackers with different motives and expertise and could cause different levels of damage to the network. Attackers could be script kiddies, elite hackers, terrorists, employees, competitors, or customers. The authors in [4] group attackers into: 1) Non-malicious attackers who view the security and operation of the system as a puzzle to be cracked. Those attackers are normally driven by intellectual challenge and curiosity. 2) Consumers driven by vengeance and vindictiveness towards other consumers making them figure out ways to shut down their home's power. 3) Terrorists who view the smart grid as an attractive target as it affects millions of people making the terrorists' cause more visible. 4) Employees disgruntled on the utility/customers or ill-trained employees causing unintentional errors. 5) Competitors attacking each other for the sake of financial gain.

Those attackers can cause a wide variety of attacks, classified into three main categories [5],[6]: Component-wise, protocol-wise, and topology-wise. Component-wise attacks target the field components that include Remote Terminal Unit (RTU). RTUs are traditionally used by engineers to remotely configure and troubleshoot the smart grid devices. This remote access feature can be subject to an attack that enables malicious users to take control over the devices and issue faulty states such as shutting down the devices. Protocol-wise attacks target the communication protocol itself using methods such as reverse engineering and false data injections. Topology-wise attacks target the topology of the smart grid by launching a Denial-of-Service (DoS) attack that prevents operators from having a full view of the power system causing inappropriate decision making. More attacks were discussed in [7]-[10] including:

1) *Malware spreading:* An attacker can develop malware and spread it to infect smart meters or company servers. Malware can be used to replace or add any function to a device or a system such as sending sensitive information.

2) *Access through database links:* Control systems record their activities in a database on the control system network then mirror the logs into the business network. If the underneath database management systems are not properly configured, a skilled attacker can gain access to the business network database, and then use his skills to exploit the control system network.

3) *Compromising communication equipment:* An attacker may compromise some of the communication equipment such as multiplexers causing a direct damage or using it as a backdoor to launch future attacks.

4) *Injecting false information (Replay Attack):* An attacker can send packets to inject false information in the network, such as wrong meter data, false prices, fake emergency event, etc. Fake information can have huge financial impact on the electricity markets.

5) *Network Availability:* Since smart grid uses IP protocol and TCP/IP stack, it becomes subject to DoS attacks and to the vulnerabilities inherent in the TCP/IP stack. DoS attacks might attempt to delay, block, or corrupt information transmission in order to make smart grid resources unavailable.

6) *Eavesdropping and traffic analysis:* An adversary can obtain sensitive information by monitoring network traffic. Examples of monitored information include future price information, control structure of the grid, and power usage.

7) *Modbus security issue:* The term SCADA refers to computer systems and protocols that monitor and control industrial, infrastructure, or facility-based processes such as smart grid processes. Modbus protocol is one piece of the SCADA system that is responsible for exchanging SCADA information needed to control industrial processes. Given that the Modbus protocol was not designed for highly security-critical environments, several attacks are possible including: (a) sending fake broadcast messages to slave devices (Broadcast message spoofing), (b) replaying genuine recorded messages back to the master (Baseline response replay), (c) locking out a master and controlling one or more field devices (Direct slave control), (d) sending benign messages to all possible addresses to collect devices' information (Modbus network scanning), (e) reading Modbus messages (Passive reconnaissance), (f) delaying response messages intended for the masters (Response delay), and (g) attacking a computer with the appropriate adapters (Rouge interloper).

5. Challenges for New Security Solutions

Security solutions developed for traditional IT networks are not effective in grid networks [6] because of the major differences between them. Their security objectives are different in the sense that security in IT networks aims to enforce the three security principles (confidentiality, integrity and availability), while the security in automation (grid) networks aims to provide human safety, equipment and power lines protection, and system operation. Moreover, the security architecture of IT networks is different than that of the Grid network since security in IT networks is achieved by providing more protection at the center of the network (where the data resides), while the protection in automation networks is done at the network center and edge. Their underlying topology is also different where IT networks use a well defined set of operating systems (OSs) and protocols, while automation networks use multiple propriety OSs and protocols specific to vendors. Finally, their Quality of Service (QoS) metrics are different in the sense that it is acceptable in IT networks to reboot devices in case of failure or upgrade, while this is not acceptable in automation networks since services must be available at all times.

These major differences between the IT and grid network security objectives necessitate the need for new security solutions specific for the smart grid network. The development of these security solutions is faced with many challenges [5],[6] including: 1) some components use propriety OS to control functionality rather than security, 2) automation system network was designed without regard to security, 3) security should be integrated with existing systems without downgrading the performance, 4) remote access to grid devices should be monitored and controlled, and 5) the new protocols should have the capability of incorporating future security solution.

6. Proposed Solutions

Having overviewed the major vulnerabilities and security challenges, this section the recent security solutions [3], [11]-[14]:

1) Identity should be verified through strong authentication mechanisms. Organizations should implement an *implicit deny* policy such that access to the network is granted only through explicit access permissions.

2) Malware protection on both Embedded and General purpose systems. Embedded systems are intended to only run software that is supplied by the manufacturer. The manufacturer is required to embed in its products a secure storage that contains keying material for software validation. Using a key, the system can validate any newly downloaded software prior to running. However, general purpose systems are intended to support third party software. For this system, up-to-date and frequently updated antivirus software along with host-based intrusion prevention are required.

3) Network Intrusion Prevention System (IPS) and Network Intrusion Detection System (IDS) technologies should augment the host-based defenses to protect the system from outside and inside attacks.

4) Vulnerability assessments must be performed at least annually to make sure that elements that interface with the perimeter are secure.

5) In some instances, user actions can open potential system vulnerabilities. As such, awareness programs should be put in place to educate the network users about security best practices for using network tools and applications.

6) Devices must know the sources and destinations they communicate with. This is accomplished through mutual authentication techniques using Transport Layer Security (TLS) or Internet Protocol Security (IPSec).

7) Devices should support Virtual Private Network (VPN) architectures for secure communication.

8) Devices must use Public key Infrastructure (PKI) to secure communication [14]. However, there are some constraints regarding cryptography and key management [15]: current devices do not have enough processing power and storage to perform advanced encryption and authentication techniques, communications in a smart grid system will be over different channels that have different bandwidths, and connectivity, where all devices, certificate authorities, and servers must be connected at all times.

9) From the huge amount of transferred data, utilities should only collect the data needed to achieve their goals.

10) Control system and IT security engineers should be equally involved in securing the smart grid network.

11) Since the life cycle of the smart grid is longer than that of the IT systems involved, all IT technologies should have the ability to be upgraded.

12) Security must be part of the smart grid design. Otherwise, security of devices becomes vendor specific; the fact that might produce many vulnerabilities because of incompatibility issues.

13) Utilities should consider utilizing third party communication companies. Letting the utilities handle all the grid communication becomes quickly a burden that the utility cannot handle. Third part companies can help in managing the communication and security issues of data transfer.

14) A robust authentication protocol is needed while communicating between smart grid parties. The protocol must operate in real-time abiding with some constraints such as minimum computational cost, low communication overhead, and robustness to attacks, especially Denial-of-Service attacks.

7. Conclusion

Traditional power systems are moving towards digitally enabled smart grids which will enhance communications, improve efficiency, increase reliability, and reduce the costs of electricity services. The massiveness of the smart grid and the increased communication capabilities make it more prone to cyber attacks. Since the smart grid is considered a critical infrastructure, all vulnerabilities should be identified and sufficient solutions must be implemented to reduce the risks to an acceptable secure level. In this paper, we surveyed the vulnerabilities in smart grid networks, the types of attacks and attackers, the challenges present in designing new security solutions, and the current and needed solutions.

References

[1] Al-Omar B, Al-Ali AR, Ahmed R, *et al*. Role of information and communication technologies in the smart grid. *Journal of Emerging Trends in Computing and Information Sciences*, 2012; 3(5):707-716.

[2] Pearson I. Smart grid cyber security for Europe. *Energy Policy*, 2011; 39(9):5211-5218.

[3] Clements S and Kirkham H. Cyber-security considerations for the smart grid. In: *Proc of the IEEE Power and Energy Society General Meeting*, 2010:1-5.

[4] Flick T and Morehouse J. *Securing the Smart Grid: Next Generation Power Grid Security*. Syngress, 2010.

[5] Wei D, Lu Y, Jafari M, *et al.* Protecting smart grid automation systems against cyberattacks. *IEEE Trans on Smart Grid*, 2011; 2(4):782-795.

[6] Wei D, Lu Y, Jafari M, *et al.* An integrated security system of protecting smart grid against cyber attacks. In: *Proc. of the IEEE PES Conference on Innovative Smart Grid Technologies*, 2010:1-7.

[7] Wang X and Yi P. Security framework for wireless communications in smart distribution grid. *IEEE Transactions on Smart Grid*, 2011; 2(4):809-818.

[8] Aravinthan V, Namboodiri V, Sunku S and Jewell W. Wireless AMI application and security for controlled home area networks. In: *Proc. of IEEE Power and Energy Society General Meeting*, July 2011:1-8.

[9] Y Mo, Kim T H-J, Brancik K, *et al.* Cyber-physical security of a smart grid infrastructure. *Proc. of the IEEE*, 2012; 100(1):195-209.

[10] Flynn B. Smart Grid Security. Presented at: Cyber Security for Process Control Systems Summer School, June 2008.

[11] Wang X and Yi P. Security framework for wireless communications in smart distribution grid. *IEEE Transactions on Smart Grid*, 2011; 2(4) 809-818.

[12] Lu Z, Lu X, Wang W and Wang C. Review and evaluation of security threats on the communication networks in the smart grid. In: *Proc. of the Military Communications Conference*, 2010:1830-1835.

[13] Cisco White Paper. [Online]. Available: *http://www.cisco.com/web/ strategy/docs/energy/white paper c11539161.pdf*

[14] Metke AR and Ekl RL. Security technology for smart grid networks. *IEEE Transactions on Smart Grid*, 2010; 1(1):99-107.

[15] Iyer S. Cyber Security for Smart Grid, Cryptography, and Privacy. *International Journal of Digital Multimedia Broadcasting*, 2011; doi:10.1155/2011/372020.