International Journal of Electrical and Computer Engineering.
ISSN 0974-2190 Volume 8, Number 2 (2016), pp. 99-107
© International Research Publication House
http://www.irphouse.com

Power Dispatching and Security Challenges in Smart Grid Management and its Solution through Key Management: An Overview and Issues

Abdullah Umar[1], Yash Pal Singh[2] and Adla Sanober[3]

[1]Research Scholar (EE), F/o - Engineering, OPJS University, Churu, Raj., India.
[2]Professor (EE), F/o - Engineering, OPJS University, Churu, Raj., India.
[3]Assist. Professor (CS/ IT), F/o – Engineering & Technology, NIT - Patna, Bihar, India.

Abstract

Information and communication technology (ICT) used in smart grid to operate, monitor and control data to achieve high efficiency, reliability, economics and sustainability. However, smart grids are more vulnerable to security attacks compared to traditional grids because they connect to the Internet and wireless networks. Key management is important security challenge to achieve data confidentiality and integrity in smart grid. Many key management solutions have been devised to fulfil these requirements but they have weakness such as lack of flexibility, scalability and support message communication. This paper describes existing security challenge issues and their solutions for smart grid and SCADA system and also discussed their limitations.

Keywords: Smart Grid, SCADA, Cyber Security, Key Management.

1. INTRODUCTION

Smart grid generally refers to a next-generation power grid in which the generation, transmission, distribution, and management of electricity are upgraded and automated by incorporating advanced computing and communication technologies for improving the efficiency, reliability, economics, and safety of the grid. A smart grid brings great performance benefit to the power industry and enables end users to optimize their power consumption; however, the heavy dependence on communication networks has made smart grids vulnerable to a wide range of cyberspace threats. For example, it has been shown that security breaches in smart grids can result in a variety of serious consequences, from blackouts and physical damage of infrastructure to the leakage of customer information [1]. There are many challenges and issues in the smart grid such as energy metering control and dispatching, connectivity, new trust models and security. However, recently cyber-attacks on critical infrastructure have highlighted security as a major requirement on smart grid [9].

According to a report published by krebson-security, in May 2010, FBI investigated hacking of smart grid meters in Puerto Rico. The bureau distributed an intelligence alert about its findings to select industry personnel and law enforcement officials. The FBI said it believes that former employees of the meter manufacturer and employees of the utility were altering the meters in exchange for cash and training others to do so because of “the ease of exploitation and economic advantage to the hacker and the electric customer. Therefore, it is important to ensure that the data carried by smart grid system is kept confidential and that no one but the right receiver can access the data [5].

Considering the vast scale and complex architecture of a smart grid, it is not difficult to understand that the vulnerabilities associated with the smart-grid communication system may also be enormous. Those security vulnerabilities need to be properly addressed to ensure that smart grids are not only secure and function correctly, but that they also maximize their adoption and successfully fulfil the promise of smart-grid investment.

Although most of the architectures, frameworks, and roadmaps for smart grids have already been defined by the governments, industry, and academia, there are still many important security and privacy issues in smart grid communications. These issues are now considered by governments and industry to be one of the highest priorities for smart-grid design, and they must be resolved before smart grids can be operationally ready for the market.

Traditionally, electricity is provided to customers via central power plants; however, these systems suffer from the lack of reliability. Control of the electrical infrastructure by Supervisory Control and Data Acquisition (SCADA) plays an important role in smart grids. SCADA is a system that allows a user to collect data from one or more distant fields and send control commands to those fields. The control system provides a visual management interface for the network operators to remotely control and configure the power network. While power utilities have designed various control systems to manage their electricity grid, most of them depend on SCADA systems to supervise their infrastructure [5].

Currently, many key management schemes [6, 8] for smart grid and SCADA system have been proposed to achieve end-to-end secure communication. However, these schemes suffer from limitations such as lack of real-time constraints, scalability, and support message communication in different scenarios. To achieve high confidentially in a smart grid, a robust and efficient key management solution is required. In this survey paper, we present and discuss the existing key management solutions for smart grid and SCADA system, and outline their limitations. We have also highlighted some open research issues related to key management in smart grid. Since, the electricity grid - one of the oldest critical infrastructures - which has been controlled by SCADA, and smart grid plays an important role as a control system for intelligent monitoring in electricity grid. Therefore, we consider key management for smart grid and SCADA system.

2. SMART GRID

2.1 Smart Grid Architecture

The major components in smart grid architecture are Electric Household Appliances, Renewable Energy Resources, Smart Meter, Power utility Centre and Service provider [3], as illustrated in Fig.1 [4]. Electrical Household Appliances (smart and legacy) are suspected to be able to communicate with smart meters via a House Area Network (HAN) assisting efficient energy intake control to all home devices. Renewable energy resources are solar and wind power that provides home devices through local generate electricity. Smart meter contains a microcontroller that has memory, digital ports, timers, real-time, and serial communication facilities. Smart meters sign-up the power intake generally and transmit it to the utility server, connect or detach a customer source of energy and send out alarms in case of a problem. Power utility communicates with smart meters to control energy intake. Service provider's suppliers identify contracts with customers to provide electricity for individual devices companies interact with internal devices via messages carried by the smart meter. To identify such interaction, service providers should sign-up with the electric utility and obtain electronic accreditations for their details and public keys. The accreditations are then used to facilitate secure marketing communications with customers [7].

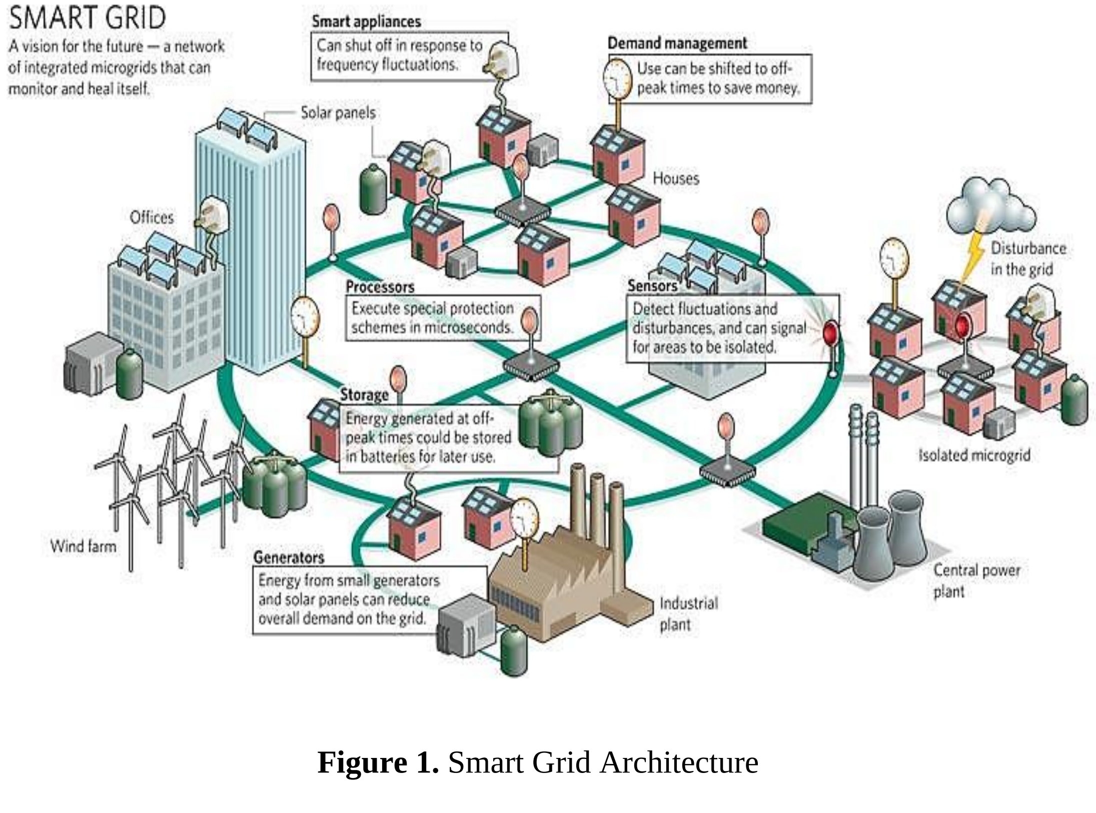
SMART GRID
A vision for the future — a network of integrated microgrids that can monitor and heal itself.
Smart appliances
Can shut off in response to frequency fluctuations.
Demand management
Use can be shifted to off-peak times to save money.
Solar panels
Houses
Offices
Disturbance in the grid
Processors
Execute special protection schemes in microseconds.
Sensors
Detect fluctuations and disturbances, and can signal for areas to be isolated.
Storage
Energy generated at off-peak times could be stored in batteries for later use.
Isolated microgrid
Wind farm
Generators
Energy from small generators and solar panels can reduce overall demand on the grid.
Industrial plant
Central power plant

Figure 1. Smart Grid Architecture

Smart grids are characterized by two types of communication: Home Area Network (HAN) and Wide Area Network (WAN). A HAN connects the in-house smart devices across the property with smart meters. The HAN can connect using Zigbee, wired or wireless Ethernet, or wireless Bluetooth. A WAN, on the other hand, is a bigger network that joins the smart meters, companies, and energy application. The WAN can connect using WiMAX, 3G/GSM/LTE, or fibre optics. A smart meter functions as an entrance between the in-house devices and the exterior parties to provide needed information [8] as shown in Fig.2.

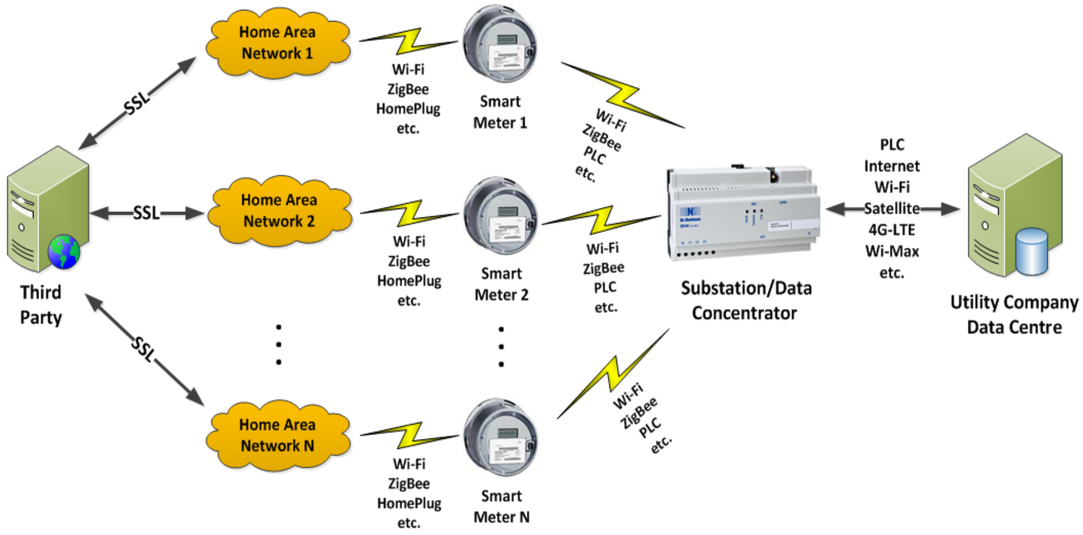
Home Area Network 1
Home Area Network 2
Home Area Network N
SSL
SSL
SSL
Third Party
Wi-Fi ZigBee HomePlug etc.
Wi-Fi ZigBee HomePlug etc.
Wi-Fi ZigBee HomePlug etc.
Smart Meter 1
Smart Meter 2
Smart Meter N
Wi-Fi ZigBee PLC etc.
Wi-Fi ZigBee PLC etc.
Wi-Fi ZigBee PLC etc.
Substation/Data Concentrator
PLC Internet Wi-Fi Satellite 4G-LTE Wi-Max etc.
Utility Company Data Centre

Figure 2. Smart grid communication and control system.

2.2 Smart Grid and SCADA

SCADA system plays an important part in smart grids. SCADA is a technology that allows a user to collect data from one or more distant fields and send control commands to those fields. A SCADA system handles sensitive data for several industries, including natural gas, water management networks, transportation control, power grids, and so on, each of which is important for normal day-to-day lives. SCADA includes a number of Remote Terminal Units (RTUs) that collect field data. SCADA system is a technology that helps smart grid to reduce operational and maintenance cost, ensure the reliability of power supply, and provides tolerant of attacks against physical and cyber security. Hence, without a secure SCADA system, it is impossible to deploy the smart grid system [8].

The following major challenges faced in securing the smart grid:

A. Access Control and Identity Management

It is important to ensure that data transmitted via smart grids is kept confidential and that no one but the intended receiver is able to see the message. In addition, the smart grid contains many components that are interconnected. Because of security concerns related to this, authentication is needed to verify the identity of the receiver in order to avoid any disruption or exploitation. Access to the control centre, transmission, and distribution grids is allowed only for authenticated users, groups, and services [5].

B. Privacy and Security Policies

There is a huge necessity for suitable security policies to establish relationships among consumers, utilities, and third parties, although applying security and privacy policies should not result in unsatisfactory latencies.

C. Threat Defence

There is much vulnerability inherent to target smart grids; therefore, it is necessary to protect the grids from defined threats by building an effective, layered defence system to function broadly across the entire grid infrastructure.

Threat defence provides network segmentation and access control to defend against denial-of-service (DoS). In addition, it provides a suite of security technologies such as firewall, intrusion prevention system (IPS) and virtual private network (VPN) [6].

D. Physical Security

Smart grid systems can have thousands, and often even millions of remote points and field area networks. This makes it challenging to maintain the physical security of the smart grid. The geographical dispersion of these systems also means that it may be difficult to access all of the terminals for maintenance [7].

E. Connectivity

Communications connectivity in smart grids implies a transition towards an Internet-like distributed environment in which huge numbers of devices are interconnected. This is one of the emerging challenges in this area and as such the application of protective techniques is important.

3. INFORMATION ASSURANCE AND SECURITY CONCEPTS AND POLICIES

Information Assurance and Security issues ultimately involve protection of information [1]. Information protection criteria are usually specified in policies such as confidentiality, integrity, and availability. The researchers included accountability as a separate policy even though it can be viewed as Integrity issue because it is critical for the smart grid. NIST has defined these security policies as follows.

3.1. Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. The property that sensitive information is not disclosed to unauthorized individuals, entities or processes.

3.2. Integrity

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Data integrity is the property that data has not been altered in an unauthorized manner. It covers data integrity covers data in storage, during processing, and while in transit and includes the property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

3.3. Availability

Ensuring there's timely and reliable access to and use of information.

3.4. Accountability

Is the security goal that generates the requirement for actions of an entity to be traced uniquely to that entity? This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

3.5. Security Concepts and Smart Grid

With the Smart Grid's transformation of the electric system to a two-way flow of electricity and information, the Information Technology (IT) and telecommunications infrastructures have become critical to the energy sector infrastructure. Therefore, the management and protection of systems and components of these infrastructures must also be addressed by an increasingly diverse energy sector.

IT and telecommunication sectors have existing cyber security standards to address vulnerabilities and assessment programs to identify known vulnerabilities in these systems.

4. REAL STORIES-ATTACKS

Assailants with different motives and skills can take advantage of the weaknesses in security of smart grid system and can cause different levels of damage to the system. Attackers at the top level include online hackers, terrorists, workers, opponents, or client, and so on. Client may change data, information, and can get power without paying. The professionals and experts found only 9 security weaknesses for the period from 2005 to the beginning of 2010. Security experts have indicated a strong interest in the topic. Consequently, 64 vulnerabilities were found by the end of 2011. Furthermore, in the first 8 month of 2012, information about 98 security weaknesses was published.

Computer security experts who analysed the vulnerabilities say the weaknesses are not extremely risky on their own because they would mainly allow a malicious user to collapse a system or obtain sensitive data but they warn that the weaknesses could allow an enemy to obtain a hold on a system and find additional security weaknesses that could impact primary procedures [6]. According to Rautmare *et al.* [8] "the exploitation of the network control system may result in disruption and breaks in operation. That may lead to disruption of service and loss of manufacturing, neither of which is allowable".

A. Stuxnet

In 2010, Stuxnet was discovered. It is an advanced and sophisticated malware program that targets industrial control systems. Industrial control systems targeted by

Stuxnet are reprogrammed to hide any changes made by a Stuxnet attack. Iran was the country most affected by Stuxnet in the early days of its infection. However, since Stuxnet can self-replicate, other countries were affected, including Indonesia and India. Security specialists have found that Stuxnet is able to control the speed of motors, and is thus able to send nuclear centrifuges out of control [6].

B. Slammer Worm

Security Focus reported in 2003 that the Slammer Worm passed through a computer network and targeted a nuclear power plant in Ohio. For almost five hours, the safety monitoring system was disabled in the plant. The infection did not cause any harm but it alarmed the control system due to it being under possible attack [9].

C. Cyber–Physical Attack

On smart grid application by malicious users such as decrease the reading of meters "electricity bills" or to cut the servers on people life and so on. Since the smart grid reaches to each building as well as the complex of communications; therefore, it makes it difficult to guarantee the protecting physically for whole component in the system [9].

5. REMEDIAL STRATEGIES TO INCREASE THE PROTECTION OF THE SMART GRID

All connections to smart grid system should be identified. Unneeded connections to the smart grid network should be disconnected. Due to importance of data in a smart grid network and to make sure that the system has the highest security, it is recommended to disconnect it from other networks, especially when the connection sets up a pathway to or from the Internet. Security evaluations, vulnerability analysis, and security testing should be done on any remaining connections to the smart grid to protect the network and support the risk management processes with a strong strategy for any pathways to the smart grid. It is necessary to implement firewalls and intrusion detection systems (IDS). Attacks may expose default network services since the smart grid control servers were developed on open source platform or even on a commercial operator system. Therefore, to improve the security in smart grid systems, it is necessary to remove unused services and network daemons, such as billing systems or automated readings of meters, email, and other Internet services [7].

Encryption is used to secure data in the smart grid. However, it can be a time and cost consuming if it does not be handled in a proper way which it could cause additional storage and bandwidth usage. Key management is another complex issue, which needs more attention and effort. In cryptography, there are two types of keys algorithms may use symmetric keys or asymmetric keys. In symmetric key, it applies a cryptographic message with the same key for encryption and decryption. In asymmetric key, there are two types of the key pair are used. One key encrypts the message and the other decrypts the message [9].

CONCLUSION

Smart grid describes a modern technological field of resilience, performance, and efficiency across the entire power industry. These systems also handle sensitive data and it is a critical system for industry, so these networks' communications have to be protected. Thus, security features for IT systems with traditional networks are applicable to smart grid as well. Hence, smart grid can be protected in different ways, for instance, crypto graphics. However, cryptographic techniques require protected keys to secure communications in smart grid. That will ensure that the network achieves the three main requirements for security: authenticity, integrity, and confidentiality. Consequently, key management for smart grid became a considerable issue for researchers.

Currently, many key management schemes are proposed for smart grid and SCADA system. However, these schemes suffer from some limitation such as lack of flexibility, scalability and support message communication in different scenarios and so on.

REFERENCES

[1] Fan, X. and G. Gong. 2013. Security Challenges in Smart-Grid Metering and Control Systems. Technology Innovation Management Review. July 2013, 42–49.

[2] G. Lu, D. De, W.-Z. Song, Smart Grid Lab: A laboratory-based smart grid test bed, in: Proc. of IEEE Conference on Smart Grid Communications, 2010.

[3] A. Huang, M. Crow, G. Heydt, J. Zheng, S. Dale, The future renewable electric energy delivery and management (FREEDM) systems: the energy internet, Proceedings of the IEEE (1), 2011, 133–148.

[4] Office of the National Coordinator for Smart Grid Interoperability, NIST framework and roadmap for smart grid interoperability standards, release 1.0, NIST Special Publication 1108, 2010, 1–145.

[5] V.C. Gungor, F.C. Lambert, A survey on communication networks for electric system automation, Computer Networks, 2006, 877–897.

[6] T.-I. Choi, K.Y. Lee, D.R. Lee, J.K. Ahn, Communication system for distribution automation using CDMA, IEEE Transactions on Power Delivery 23, 2008, 650–656.

[7] S. Mohagheghi, J. Stoupis, Z. Wang, Communication protocols and networks for power systems – current status and future trends, in: Proc. of Power Systems Conference and Exposition (PES '09), 2009.

[8] H.J. Zhou, C.X. Guo, J. Qin, Efficient application of GPRS and CDMA networks in SCADA system, in: Proc. of IEEE power and Energy Society General Meeting (PES '10), 2010.

[9] A. Aggarwal, S. Kunta, P.K. Verma, A proposed communications infrastructure for the smart grid, in: Proc. of Innovative Smart Grid Technologies Conference Europe (ISGT), 2010.