Smart Grid Technology – Security Challenges, Vulnerabilities, Threats and Solutions

Neelam B[1] Prof. Sumit B[2] Prof K.Venkat Raman [3]

MGMCET, Kamothe, Information Technology Department

2 bsumit021@gmail.com

[3]venkatr_1967@rediffmail.com

ABSTRACT*:- The traditional electrical power grid is turning out to be one of the most promising technologies into smart grid automation network. The smart grid was introduced with the aim of overcoming the weaknesses of conventional electrical grids by using smart net meters. Smart grid technology is an extended form of analog technology that has also been introduced for controlling the use of appliances by employing two-way communication. The necessity of integration in traditional electrical power grid with information and communication technology is important for facing most of the challenges regarding securities. In this paper we focus on different challenges which arrived in traditional electrical power grid in IT networks and security involving in automation (grid) network. We proposed some solutions that can be over viewed as the major vulnerabilities and security challenges in terms of cryptography and key management techniques that are required to overcome the attacks.

Index Terms— *Key Management techniques for smart grid; Security in smart grid; Attacks in smart grid;*

1. INTRODUCTION

- Smart Grid can offer a lot of potential economic and environmental benefits and Significance: Improve reliability of power quality and transmission, increased power distribution efficiency and conservation, reduced costs for electric utilities, reduced expenditures on electricity by households and businesses, Lower Greenhouse Gas (GHG) and other gas emissions.
- 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.
- It increases the risk of compromising reliable and secure power system Operation, which, nonetheless, is the ultimate objective of the Smart Grid.
- Compared with legacy power systems, the Smart Grid is envisioned to fully integrate high-speed and two-way communication technologies into millions of power equipments to establish a dynamic and interactive infrastructure. With new energy management capabilities, such as advanced metering infrastructure (AMI) and demand Response.

2. BACKGROUND

A.When and Where Smart Grid was used?

The power grid started in 1896, based in part on Nikola Tesla's design published in 1888, but recently, in the past 50 years, electricity networks have not kept pace with modern challenges, such as: security threats, national power employment and distribution, high demand of power quality and so on. Therefore, the concept of Smart Grid came out, and the term smart grid has been in use since 2005. Therefore, the National Institute of Standards and Technology (NIST) rolled out national efforts to develop the next-generation electric power system, commonly referred to as the Smart Grid .The National Institute of Standards and Technology (NIST) proposed a Smart Grid architecture composed of seven domains as shown in Fig.1

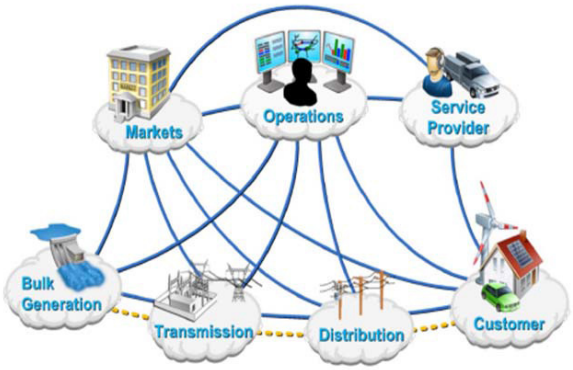

Fig.1 Server Domain Name

3. OVERVIEW OF SMART GRID

A major power grid transformation is underway. The smart grid is a constantly evolving infrastructure of digital technology and power-industry practices for improved management of electricity generation, transmission, and distribution. The smart grid's modernized controls and communication will make energy use more reliable, secure, and efficient. Smart Grid is the next generation energy supply system that fuses power supply and communication infrastructures. Smart Grid uses power and communication networks to connect homes, offices, and factories (consumers) to multiple distributed power providers (small-scale power generators) such as solar, wind, fuel cells, and facilities that store generated power. This makes it possible to provide power according to demand by tracking and predicting in real time the power demands of consumers. We expect to efficiently use the power we can generate, reduce transmission loss, and stabilize the power supply by using communications technology to control the system and balance the supply and demand of electricity. In addition, creating a smart demand and response link between consumers and power sources will help save energy.

4. ARCHITECTURE OF SMART GRID

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. 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 [2].

The Smart Grid architectural challenge is a daunting one. This is especially true for those within the electric utility industry known for their conservative approach toward incorporation of ICT-based systems to help run and manage the electric grid. Most automated grid systems in use today were built to address narrowly targeted requirement sets. As a result, a typical utility has a plethora of purchased and homegrown systems stitched together over the last three decades with point-to-point interfaces. This approach is unsustainable for a utility to efficiently and effectively implement smart grid capabilities over the next two decades. This document presents a different approach to utility system design and integration, using newer paradigms to deal with complex and legacy system integration [3].

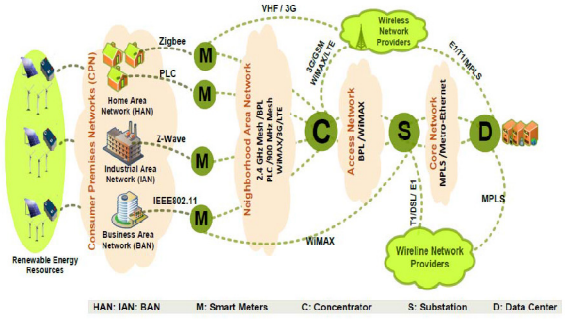

Fig 2. Smart grid architecture

Smart Grid Architectural Goals and Principles:

The next two decades will see the "Old Grid" evolve into a "Smart Grid" as legacy grid

infrastructure is merged with the latest ICT. This will put extraordinary demands on the ICT architecture; therefore, high-level goals and principles are needed to guide the smart grid architects tasked with developing any aspect of an organization's grid architecture. Additionally, a highly flexible, adaptive Enterprise Smart Grid architecture is critical for this transition to be successful. The architecture must support existing ICT infrastructure operations and be able to keep infrastructure complexity manageable as new smart grid capabilities are added.

How a utility defines its smart grid architecture will vary according to their organizations particular needs. Some possible goals are:

1. Facilitate bridging new and emerging information and communications technology to legacy architecture over extended time periods (technology roadmap).
2. Manage the increasing complexity of ICT needed to support smart grid implementation.
3. Align technology usage with the utility's smart grid strategic objectives.
4. Provide guidance on how packaged solutions can support the smart grid architectural vision.
5. Facilitate the communication of the utility's smart grid strategy and plans across the enterprise Help sell the utility's smart grid vision to business unit leadership, IT management, suppliers, regulatory agencies, contractors, etc.

5.TRADITIONAL IT NETWORK VS GRID NETWORK

Sr. No.	Properties	Traditional IT Network	Smart Grid Network
1	IT Network	Security objective-CJA.	Security objective-human safety, equipment and power lines protection, system operation.
2	Architecture	Achieved by providing more protection at the center of the network	Protection is done at the network center and edge
3	Topology	Well defined set of OS and protocol	Multiple proprietary OS and protocols specific to vendors
4	Quality of Service	To reboot devices in case of failure or upgrade	Not acceptable in automation service must be available at all time
5	Machinery	electric	digital
6	Communication	One way	Two way
7	Power Generation	centralized	distributed
8	Sensors	Small number	Full grid
9	monitoring	Manual	Automatic
10	Recovery	Manual	Automatic
11	User options	Few	More
12	OS	Common OS	Proprietary OS
13	protocols	communication protocols are common	communication protocols are different
14	Security solutions		

Table 1: Comparison between traditional IT network and grid network

6. CHALLENGES IN SMART GRID

A. proprietary OS
Some components use proprietary OS to control functionality rather than security
B. security
Automation system network was designed without regards to security.
C. performance
Security should be integrated with existing system without downgrading the performance
D. Remote access
Remote access to grid device should be monitored and controlled
E. Protocol in case of security
New protocol should have the capability of incorporating future security solutions
F. Malicious Cyber Attacks
As security challenges mainly come from malicious cyber attacks via communication networks, it is essential to understand potential vulnerabilities in the Smart Grid under network attacks.
In the Smart Grid, however, malicious behavior is a more concerned issue, as millions of electronic computing devices are used for monitoring and control purposes instead of providing data services such as file downloading and sharing. Thus, malicious attacks may induce catastrophic damage to power supplies and widespread power outage, which is a definitely forbidden case in the Smart Grid [1].

Three categories of main attacks in Smart Grid [4]

- Vulnerability attack: The vulnerability attack is mainly caused by the inherent reliability in the communication network instead of malicious attacks with specific attempts, and it can be prevented by introducing the fault diagnosis scheme.
- Data injection 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.
- Intentional attack: Intentional attack can be implemented via coordinated denial-of-service (DoS) attack and contributes to network disruption due to node disconnections in the communication network.

7. PROPOSED SOLUTIONS

A. Implicit Deny Policy-
Here the access to the network is granted only through explicit access permissions

B. Key Cryptography System-
The design of encryption schemes is the essential mechanism to protect data confidentiality and integrity in the Smart Grid [1].

- Encryption,
- Authentication, and
- Key management for power systems.

C. IPS and IDS-
It is used to protect the system from inside and outside attacks. *IPS or intrusion prevention system* is definitely the next level of security technology with its capability to provide security at all system levels from the operating system kernel to network data packets. *An intrusion detection system (IDS)* is designed to monitor all inbound and outbound network activity and identify any suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

D. VPN-
The traditional IP based network is versatile but supports only for best effort delivery. It does not ensure the QOS of the data being transferred. Smart grid requires certain QOS guarantees in terms of latency, delay variation, throughput packet loss for efficient and reliable operation. In other words Internet VPN technology can provide a better alternative to ensure security and QOS requirements of smart grid. Internet VPN technology is shared communication network architecture for a cost effective and high speed core communication network. Internet VPN provides both the functionalities and benefits of a dedicated private network. In other words, Internet VPN can provide reliable, secure, robust communication with strict QOS guarantee to smart grid over a shared network infrastructure with the same policies and services that the electric utility experiences within its dedicated private communication network [6].

E. Protocol used-

The Open Smart Grid Protocol (OSGP) is a family of specifications published by the European Telecommunications Standards Institute (ETSI) used in conjunction with the ISO/IEC 14908 control networking standard for smart grid applications. OSGP is optimized to provide reliable and efficient delivery of command and control information for smart meters, direct load control modules, solar panels, gateways, and other smart grid devices [5].

8. CONCLUSION

The traditional power systems are transforming themselves into digitally enabled smart grids. It aims at enhancing the proper communications, improvement of efficiency, increasing reliability, reduces costs of electricity services. Since the grid is more popular it is more prone to cyber attacks. Being a critical infrastructure various vulnerabilities should be identified properly and sufficient solutions should be implemented accordingly. Hence in this paper we provided different security solutions.

REFERENCES

[1]. Wenye Wang , Zhuo Lu "Cyber security in the Smart Grid: Survey and challenges" Computer Networks 57 (2013) 1344–1371.

[2]. Fadi Aloula*, A. R. Al-Alia , Rami Al-Dalkya, Mamoun Al-Mardinia.

[3]. Wassim El-Hajjb "Smart Grid Security: Threats, Vulnerabilities and Solutions" * Manuscript received June 15, 2012; revised August 15, 2012.

[4]. Cisco Systems, Inc., International Business Machines Corporation, Southern California Edison Company 2011 "Smart Grid Reference Architecture".

[5]. Yao Liu, Peng Ning Department of Computer Science," False Data Injection Attacks against State Estimation in Electric Power Grids∗" 2009 ACM 978-1-60558-352-5/09/11

[6]. https://en.wikipedia.org/wiki/Open_smart_grid_protocol.

[7]. Ekram Hossain,Zhu Han,H.vincent Poor,"Smart grid Communications And Networking"