Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 3– No.4, November 2015 – www.caeaccess.org

Cyber Security: Issues and Privacy

Anshul Shrivastava
M.Tech, Power Distribution with Spec. in Smart Grid
University of Petroleum & Energy Studies, Dehradun

ABSTRACT
In an Electrical Power system, distribution substation is an important part of linking between utility to end user consumers. It has a capability to reduce as well as increase the energy supply to the end user consumers from utility generation supply as per requirement of electricity. Though, A Smart Grid is a modernized electrical power system or grid which consist analog or digital communication, information technology and an automated system. It needs to be secured with the help of cyber security. Cyber security is essential for smart grid which requires the network data and communication system to be secured. The stored data and computers need to be secured from hackers and e-threat. With the help of cyber security, Smart Grid can be made more efficient, reliable and secure. The existing power system needs to be upgraded to the next level i.e. Smart Grid. There are lots of challenges for implementing cyber security in Indian smart grid.

Keywords
Security, Smart Grid, Cipher key management, Cryptography, Privacy.

1. INTRODUCTION
Cyber security is an essential part of power system, due to its advantages. In a power system its need to be secures each and every data of communication or storage files which has to be confidential. Basically, cyber security is the advanced digital infrastructure which is above to the existing electric grid. It is used for monitoring of grid condition, energy consumption, generation as well as distribution operations and automates the system. It is just not a cable/data network which is upgrades the existing electric grid where generation utilities generate and end consumers consume the electricity, it is moreover advance function over data network where isolate the fault as well as revenue collection makes easier. The aims/goal of smart grid are but not limited to,

1. Improve the reliability of the electrical grid
2. Improve its overall efficiency
3. Lower costs of distribution and generation
4. Allow for real time monitoring of the electrical grid

To put in effect of this goals/aim or task, smart grid will employ new digital devices or instrument which is microprocessor based in both utility and customer side. Smart meters are used for communicating between utility to customer side and give the data of energy being used with online monitoring system, grid condition and real time data usage alert to the end users.

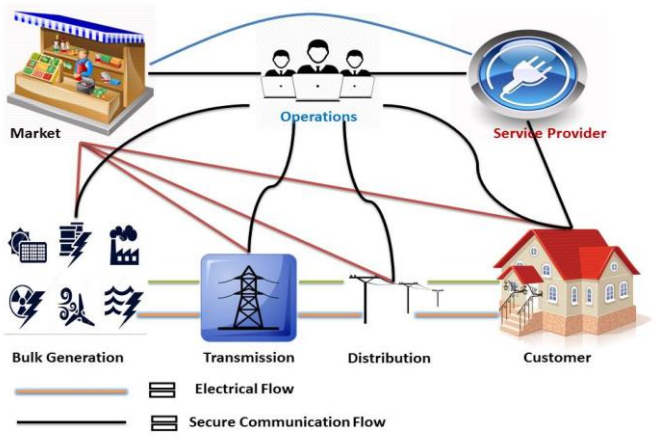

Figure 1: Data and electricity flow across a secure smart grid domain (NISTIR 7628 Guidelines)

2. CYBER VULNERABILITIES IN THE ECONOMIC POWER GRID
The legacy power grid is managed by control equipment, protective devices, real time monitoring system at substation end as well as utility side and extensive communication network.

2.1 SCADA Security
Supervisory Control and Data Acquisition (SCADA) is used for control and monitoring the existing system real time in National power grid. It is undergo the cyber security assessment as part of National SCADA Test Bed (NSTB) program. It performs various test/assessment of control system products, onsite operational environment including electric power grid facilities. Much vulnerability has been found during assessment which has to be categorized and need to be fixed in a very well manner and describes in a report. A vulnerabilities has to be included if found at least more than two times assessment. Many vulnerabilities of SCADA have not been disclosed publically according to the National Vulnerabilities Database (NVB).

Table 1: Differences between it Networks and Smart Grid

Categories	IT Networks	Smart Grid
Security Objectives	Confidentiality> Integrity> availability	Availability > Integrity > Confidentiality
Architecture	1. Flexible and dynamic topology. 2. Center server require more protection than periphery host.	1. Relatively stable tree- like hierarchy topology. 2. Some field devices requires the same security level as the control server
Technology	1. Diverse operating system. 2. Public networks. 3. IP's based communication protocol.	1. Proprietary operating systems. 2. Private networks 3. IEC 61850 and DNP based communication protocols.
Quality of Service	1. Transmission delay and occasional failure are tolerated. 2. Allow re-booting.	1. High restriction on transmission delay and failure. 2. Rebooting is not acceptable.

2.2 Substation Security

A Private company of Public Private Partnership (PPP) has to be taken care as well as evaluate the security posture of substation level of automation. A substation contain distribution and transmission level devices such as capacitor banks, circuit breaker, phase shifting transformer, relay, Power transformer, isolators, switching devices. Substation may also contain the control devices and automation devices used for control, measure and monitoring the substation component. The level of automation of substation is increased day by day according to the need which is indirectly related to the security because increased automation implies increasing of controlling devices and monitoring devices contains computer-control electronics and software based peripherals which tend to increase the potential of cyber security weakness. Increasing of automation of substation does not imply reduce security, however the study identified many vulnerabilities of substation automation devices and described the potential consequences of exploitation of substation vulnerabilities. Potential consequences leads more towards cyber-attack which is directly affect to the destruction of generator, power outages and Grid instability.

2.3 Legacy Communication Network

Various communication technologies are used in the power grid to support operations. Control

Centers within utilities, regional transmission operator/independent system operators (RTO/ISOs) are in constant communication with each other and with substations in order to maintain balance between power generation and demand, maintain voltages and frequencies, respond to changing conditions, provide real-time power market access, etc. The communication media used to transfer data between grid entities include frame relay networks, asynchronous transfer mode (ATM), public switched telephone network (PSTN), the Internet, and wireless technologies such as wireless modems, microwave, and satellites. There are also many data exchange protocols used between entities within the power grid. Some of these protocols such as Transmission Control Protocol (TCP)/Internet Protocol (IP), Hypertext Transfer Protocol (HTTP), and File Transfer Protocol (FTP) are also widely used in the global Information Technology domain. Some protocols, such as Distributed Network Protocol (DNP) 3.0, were designed for control system communications. Inter-control Center Communications Protocol (ICCP) was designed and used for communications between power grid control centers.

2.4 Legacy Grid Current Risk

Some cyber vulnerabilities have to be identified for the evaluation of assessment of cyber world in smart grid communication technologies. It needs to be addressed or being addressed that know issues should not be constructed as complete assessment of power grid security posture. Such vulnerabilities are not to be considered as vulnerabilities are in the process of being mitigated. Today, smart grid communication technology has become more preferable technologies for communication and control operation scheme, which has to be need security and cannot let it go casually. Today power grid need continuously incremental changes in technologies which being used for communication and control operations. The cyber security which has some risk can't identify easily because of vulnerabilities, consequences and complex function of threat even in a static environment. The all consequences in cyber security are unpredictable intelligent adversary, dynamic and difficult to identified, consequences are difficult to predict.

3. SECURITY OF CURRENT SMART GRID TECHNOLOGIES

Including Smart Meters, Advance Metering Infrastructure and Automatic Meter Reading are into the category of Smart Grid. Although, Smart grid technologies moreover known as Cyber Security Vulnerability

3.1 AMI Security

AMI is the key technologies which enable several smart grid technologies and it play a vital role in it. AMI is the most crucial technology which has been used for power grid to become a smart grid. It is basically seems a foundational key technology which enable smart grid technology till the end side consumer from the utility side. AMI is that crucial that we have to secure very well from hackers, e-threat with less vulnerability.

AMI need to be protected from external threat which enables a huge damage/loss into the system like grid instability etc.

3.2 Wireless Network Security

Wireless networks are commonly used in the current Smart Grid deployments. Wireless networks were employed because they have some significant advantages over other alternatives. Wireless devices are plentiful and inexpensive. Some AMI implementations use mesh networks with wireless devices to provide self-adapting multi-path multi-hop communications between AMI nodes. Mesh networks are considered very reliable because they provide redundant communication paths that compensate for failures from natural causes. For example, ZigBee is a low-cost, low-power, wireless mesh networking standard. The low cost allows the technology to be widely deployed in wireless control and monitoring applications, the low power-usage allows longer life with smaller batteries, and the mesh networking provides high reliability and a larger range. However, mesh networks are vulnerable to attack by an intelligent adversary.

3.3 Potential Attack Scenario

Consider the potential consequences of successfully attack on cyber security of smart gird, here attackers are more serious concern that they do a fake phone calls and messages to the utility side for reduction of demand side from end side consumers. From smart meters they did easily because of smart meters are work on a microprocessor based platform and it has a communication protocol, so it is more vulnerable than any one.

Actually, it all things happened cause Grid Instability, voltage fluctuation and lots of confuse to set priority matrix for load shedding.

4. CYBER SECURITY ISSUES ON SMART GRID

Traditional Power system was focusing on developing equipment to improve integrity, availability and confidentiality. Traditional power system has some communication system which gives enormous possibilities for real time monitoring and control operations. Specifically, increasing the communication system consist of RF waves more the harder to secure the system. It is more critical for cyber security to handle and cover all the aspects of the communication system. In a very broad sense, power system

comprises of communication devices including cyber security of power industry that covers all IT networks and communication issues that affect the distribution management system and power delivery system for the utility. To secure the power grid prevent, prepare for and protects against, mitigate to and recovering all the function from cyber disaster and unexpected hazards.

The smart grid security consist of four types of challenges which has to be overcome as

1. The power delivery system has a new communication development which requires a protocol, delay, bandwidth and cost of operation. To avoiding all aspects or obsolesce, it is mandatory to secure more with smart grid security development.
2. Many legacy devices has been used for communication and control operational which has limited amount of working capability.it makes more decade in the system. Most of them are function in a very particular or limited manner, which has been create lag of operation, less memory space, and computational capabilities.

To remove this legacy from the system is must require for challenging the vulnerability cause as a weakest link and has a major challenge for controlling all.

3. Such networking devices in the current power gird uses heterogeneous technologies and protocols like ICCP (Inter-control Centre Communication protocol),DNP3, Modbus etc. nevertheless, Most of them were design and control operations work in current power grid without cyber security which leads to cause e-threats, security failure.
4. It gives very specific control operations, performance without security.

Many organization are working to enhance security were trying to put lots of efforts such as NIST, NIPP, ISA and IEEE (1402). NIST Cyber Security Task Group (NIST CSTG) has been published one report were trying to say about security concern in modern power system /grid. Once I saw report, I am able to split the threats in cyber security categorized in various forms.

4.1 Device issue

Device's issue such as PLC's, RTU's and IED's are widely used in modern power grid administration to perform various tasks and maintenance.

"Smart meters" are used for calculation of energy consumption as energy meter, but it differ from conventional meter that it has a capability to communicate with the utility side to transfer the day to day consumption data and also aware the end -side consumer from daily consumption and helps to make a daily load pattern. Some potential problem was face during physical attacks i.e. Battery removal/ changing/ some modification on meters and functions like remote connect/ disconnect and outage reporting may be used by third parties.

"PHEV (Plug in Hybrid vehicle)" can be charged in different location, inaccurate billing or unwanted service will disturb the grid balance/stability.

4.2 Networking

"Internet" can be used anywhere which causes inherent threats like malicious malware file, denial of services (DoS).

"Wireless Network" can be easily attack into the layer 2/3 by injection of traffic and modification. Unless routing not provided to the layer until the security can't work and traffic are not reliable.

"Sensor Network" is so critical for power grid, tampering, intercepting, forging the data will cause damage the grid security.

4.3 Dispatching and Management

"SCADA, EMS, DMS" distribution control commands and access logs for anyone leads severe for security and damages the grid operation. Synchronizing time tagged data is essential in a wide area and without it can't be reliable for achieving the SCADA and their systems.

Load management of EMS provides both active and passive control by both costumer and service providers.

Smart Grid consists of several technologies which is self-remarkable. Micro grid is one the best example which is a decentralized distribution grid works also on Stand-alone system as well as with Tie Grid function. SCADA system is one of the major technologies which are used for monitoring "Islanding Operation" or "Islanding Mode". As per the framework, it ensures the reliability function of smart grid. Here are some points considered the increasing of risk of the system cannot be compromised.

1. Take Down the Server
2. Gaining control over the system
3. Stealing corporate data
4. Fiddling with billing information
5. Key logger software
6. Gain competitive advantage
7. Misuse the SCADA server
8. Manipulate mathematical data points
9. Change user logged data in a distant and remote DBMS

"Cipher Key Management" data management access and encryption, digital signature are required for securing the communication medium of sensors.

Under limited space and computation,

"Cryptography scheme" will lag the less security concern under due to lack of efficiency.

During emergency occurrence, device or system may be "Locked" which causes less security operation.

"Real Time Operation" some application like real time process must meet limited time constraints. Increasing of interoperability may cause unbounded and uncontrollable delay into the power system or any power grid.

5. Demand Response

Financial and legal problems arise when tampering of information of real time pricing (RTP).

Malware may affect the grid then it shows false trend of supply and demand which will not meet as per concern or scheduling

6. Protocols and Standards

Existing protocols may have some inherent false which causes some distortion and noise.

Multiple networking technologies were used for communicating and control operations such as wireless networks, fiber optical cable, land mobile radio (LMR), 3G/4G Wi-max, RS-232/485 serial link, and Wi-Fi. Potential threats were mainly focused on these areas. To secure this networks which is used for communication and operation has been ensure about security and uses advance cryptography methods.

For wired networks, Ethernet Passive Optical Networks (EPON) would be a promising solution for smart grid broadband access networks due to following metrics,

1. Backward Compatibility
2. Minimal protocol ahead
3. Low cost fiber deployment
4. Low maintenance

It is consider as next generation Gigabit-Ethernet by IEEE 802.3ah standard. A tree based EPON will broadcast massage to every ONU (Open Network Unit), on which it share same message with everywhere with OLT (Optical line Terminal). In these scenario ONU is able to gather all the traffic from OLT for limited upload bandwidth, hence it cause vulnerable for EPON that can easily be hacked such as spoofing. Using identified-based cryptography (IBC) and challenge response technology it proposes to the EPON for security and encryption.

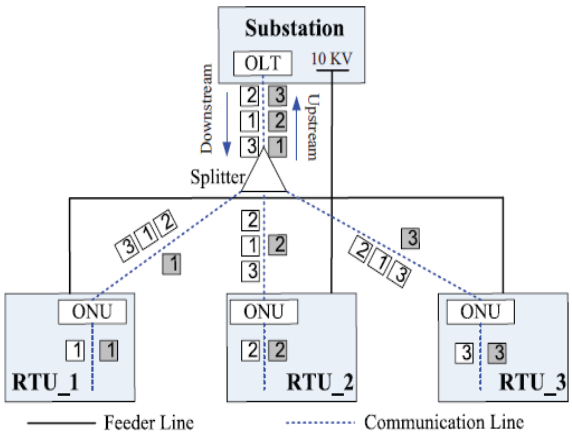

Figure 2: Typical Tree Based EPON system for the Power Grid

For Wireless Networks, airborne networks radio waves would be possible potential vulnerabilities to adversaries. Particularly, such an unprotected physical medium will cause or may disclose neighboring energy consumption data and thus cause privacy exploitation. The NIST report claim the scheme like 802.11, it can be helped to secure smart grid wireless deployment with cyber security. Moreover, further technologies could be help to secure smart grid communication system such as 802.16e (Mobile Wi-Max) and 3GPP LTE. These all are include for wireless security but are not limited to mutual or server EP (Extensible authentication Protocol), 4 way handshake, AES-CCMP (AES-Counter Mode CBC-MC Protocol), CBC-MAC (Cipher Block Chaining Message Authentication Code), 128 group encryption key, 3DES (Triple Data Encryption Standard), PKMv2 (Privacy and Key Management Version 2) RSA acknowledgement message and mutual authentication between UE (User equipment) and MME (Mobility Management Entity).

For sensor networks, researchers have reached to conclusion on that wireless mesh network should be deployed in the AMI. Primary reason for this mesh network can be overcome bad links by using redundant communication path. IT industries have witnessed a series of attacks against wireless mesh technologies such as message modification, cross-layer traffic injection, node impersonation etc. Most existing system such as routing protocol doesn't secure the path and data. Without routing security traffic is not reliable in the system which causes many distortions.

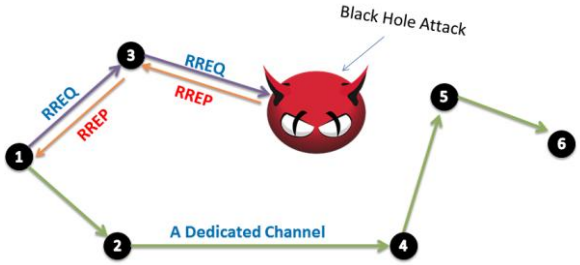

Figure 3: Black Hole against AODV routing protocol

AODV "Ad-Hoc on demand Distance Vector" is routing protocol in Zigbee networks which is suggested. It takes/ established the path in less time. From Research, researchers found that during routing mechanism a "Black Hole" attacks found, which is suffered and create cause discarding of path establishment message. To establish the path in a very secure manner, they suggested a dedicated path between individual two communication principles for communicating. It shows that recommendation could improve the network throughout enough to meet the meter reading requirement and protocols.

5. RECOMMENDATIONS FOR PRIVACY ISSUES

As per the NIST, a report delivery has been published on the consumer to utility privacy impact assessment (PIA) of the smart grid. Some points should be considered for design principle to address privacy issues in the smart grid which is:

1. An organization should ensure that information security and privacy policies and practices exist and are documented followed. Audit data should be present to monitor all data access and modification.
2. Before collecting and sharing personal information and energy use data, a clearly-specified notice should be announced.
3. Available choices should be presented to all users, and don't disclose the personal information.
4. Only personal information that is required to fulfill the stated purpose should be collected from individuals.

5. Personal information should be always protective form unauthorized modification, copying, disclosure, access, use, loss and theft.

6. The information provided to the third parties should be minimized such that it only fulfills the requirement or purpose of relevant services.

6. FUTURE RESEARCH DIRECTION

Three areas should be considered always which has to be taken care i.e. 1) Integrity and Confidentiality, 2) Robust and efficient dispatching and management model 3) establishing universal policies and standards to securing communication technologies. It has also examined the security or privacy concern of smart grid. To eliminate personal information leakage, the "State-of-Art" technique like anonymity, access control, and accountability might provide their solutions. Possible future research direction may include this path and give enormous techniques which can be securing the whole network without issue of privacy concern and less control operation security fear.

7. CONCLUSION

This paper mainly gives an overview of cyber security and privacy issues in the smart grid. Accordingly to existing research, I may conclude that almost every aspect related to IT Technology in the smart grid has potential vulnerabilities due to inherent security risk in the general IT environment which needs to be more secure. The paper also provides the future research direction and has to implement new methodologies and techniques which secure more than existing system

Cyber Security and its privacy issue in the smart grid are new areas in the field of power industry, electrical engineering, electronics technologies and Computer science. More in-depth it needs more research in the field of cyber security require to develop such a promising power grid in the near future.

8. REFERENCES

[1] "Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issues" by Wayne F. Boyer Scott A. McBride in April 2009

[2] "Cyber Security and Privacy Issues in Smart Grids" by Jing Liu and Yang Xiao, Senior Member, IEEE, Shuhui Li, Wei Liang, C. L. Philip Chen, Fellow IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 14,NO. 4, FOURTH QUARTER 2012

[3] Cisco system Inc., "Internet protocol architecture for the smart grid", white paper, Jul. 2009, available at:http;//www.cisco.com/web/strategy/docs/energy/CISCO_IP_INTEROP_STDS_PPR_TO_NIST_WP.pdf.

[4] U.S. DOE, "Smart grid system report, "White paper, Jul. 2009, available at: http://www.oe.energy.gov/SRGMMain_090707_lowers.pdf"Cyber security in the smart grid", by India smart grid Knowledge portal available athttp://indiasmartgrid.org/en/technology/Pages/Cyber-Security.aspx

[5] U.S. DOE, "Smart grid system report," White Paper, Jul.2009,availableat:http://www.oe.energy.gov/SGSRMain-090707 lowres.pdf.

[6] U.S. NETL, "A systems view of the modern grid," White Paper, Jan. 2007, available at: http://www.smartgrid.gov/white papers.

[7] J. Gadze, "Control-aware wireless sensor network platform for the smart electric grid," IJCSNS International Journal of Computer Science and Network Security, vol. 9, no. 1, Jan. 2009, pp. 16-26.

[8] D. Dvian and H. Johal, "A smart grid for improving system reliability and asset utilization," CES/IEEE 5th International Power Electronics and Motion Control Conference, Shanghai, China, Aug. 2006, pp. 1-7.

9. AUTHOR PROFILE

Anshul Shrivastava received the B.E. in Electrical and Electronics Engineering from MITS, Ujjain (India) in 2014 and presently in M. Tech in Power Distribution with specialization in Smart Grid from University of Petroleum & Energy Studies, Dehradun (India), presently he is working on Cyber Security in Smart Meter's billing system under Centre for Information technology at University of Petroleum & Energy Studies.