Analysis of Cyber Attacks Vulnerabilities In Electrical Power Systems

R. Prabhakaran, S. Asha

Abstract: ***The term "Smart grid" is used for the modernized electrical power system grids. Power grids as we know it is a collection of generation units and load centers that are connected through power lines. Smart grids are a newer version of power grids which basically is the digitalization of the infrastructure with the involvement of smart meters, sensors and different types of IED's (Intelligent Electronic Devices). As the grids become smart they become vulnerable to attacks over the internet i.e., cyber attacks.***

Index Terms: ***Cyber attacks, Machine learning, SCADA Systems, Smart grid***

I. INTRODUCTION

Ever since the introduction of smart grids, they have been a target for hackers around the world. Electricity is an important necessity in every corner of the world and if the hackers can get their hands on a grid which supply electricity to a large metro city, for example, they can cause problems for a very large amount of people at the same time. Once the hackers get their hands on the actual control systems, they can cause economic losses for a country and damage to power equipment at the same time. They can also gain access to nuclear power plants as they are also digitalized.

II. HISTORY

In 60's grids were based on natural fuel such as coal, gas and oil because of which they were planted close to fossil fuel reserves. They have to be installed away from urban areas because of increased pollution. At that time use of meters was not possible so fixed and dual tariff system was introduced. Cheap night time power was used for regulating heat banks which helped managing the daily demand and also led to lesser number of turbines that needed to be turned off at night. In 70's and 90's the demand for electricity increased as did the number of power stations. But the demand outweighed the production which led to blackouts, power cuts and brown cuts. Finally in the 20's the demand pattern in the last couple of decades was studied and a general demand pattern was formed. Peaking power generators were used which would only run for short amount time as compared to normal power generators.

Later on smart meters were introduced which were used to add regular communication between power grids and end users so that live monitoring can be achieved. IED's sensed the load on the grid by monitoring changes in the power supply frequency. This was the basic model of a smart grid which constitutes smart meters, IED's renewable energy resources and a control system (SCADA). A smart grid helps in:

1. Estimating state as well as auto repairing the faulty networks.
2. Incorporate bidirectional flow of energy.
3. Managing demand.
4. Load balancing / Load adjustment – Some generators are put on standby mode. Many individual customers or a large customer gets warned to reduce their load temporarily so that the spare generators that were on hold can be started.

III. SCADA SYSTEM

SCADA stands for Supervisory control and data acquisition. When we are talking about digitalizing power grids, it is achieved through SCADA. SCADA is the primary choice for all power grids around the world. It helps monitor, gather and process real-time data with the help of many devices such as:

A. Programmable logic controllers

PLC's are digital computers that are mainly used for automating the mechanical processes. They are impact resistant and can handle very extreme temperatures. Some of the main functions of PLC's are motion control, relay control, process control etc.

B. Remote terminal units

RTU's uses wireless communication to connect SCADA to the physical objects in real time. It is suited for communication which is spread over a wider geographical area while PLC's are more suited for local connections over small areas.

C. IED's (Intelligent Electronic Devices)

IED's take data from sensors and then they can issue commands based on the received data. They can trip circuit breakers or they can lower or increase the voltage to maintain the voltage level.

SCADA make use of many IED's such as:

- **a.** Capacitors.
- **b.** Transformers.
- **c.** Protective relays – to trip circuit breakers.
- **d.** Voltage regulators.
- **e.** Circuit breaker controllers.

Revised Manuscript Received on July 05, 2019.

Prof.R. Prabhakaran, an Assistant Professor (Senior) from the School of Computing Science and Engineering, VIT University, Chennai. India

Dr. S. Asha, is an Associate Professor from the School of Computing Science and Engineering, VIT University, Chennai. India

IV. SCADA ARCHITECTURE

Commonly SCADA systems act as a tool to monitor and control an entire area. It is applicable to any kind of industry and can work for both wire and wireless systems.

a. Hardware Architecture

There is a main server which is also known as SCADA station that handles all the processes. In Fig.1 the communication between the main server and the equipment on fields is made with the help of PLC'S and RTU'S. The communication is done through WAN and LAN networks. The RTU'S receive sensor signals from the field devices and then it sends it to the main server. The server then does the computations and sends the reply to the IED'S. Based on the feedback the RTU'S perform suitable operation.

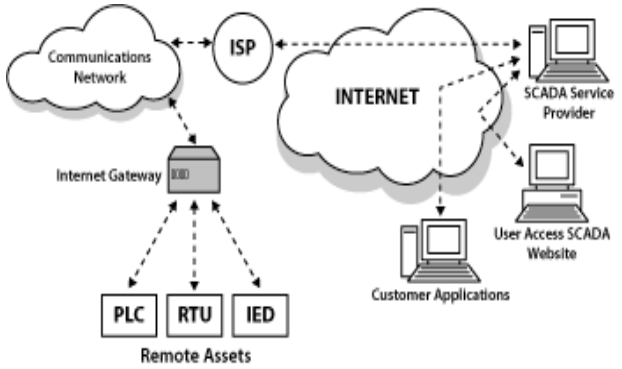

Fig.1 Operation between SCADA and Field devices

b. Software Architecture

In Fig.2 SCADA performs all the monitoring and control through a software program that is installed on the main server. Through this software the operator can get information about all the devices on field and their working status as well as he/she can perform operations. Other than that the operator can manage information, schedule maintenance, run diagnostics, access and modify archives, control various IED'S, etc.

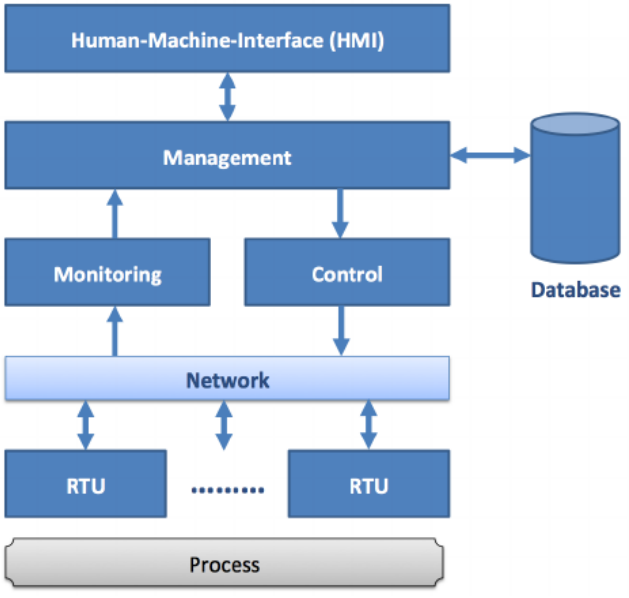

Fig.2 Operations in SCADA through software Programs

Communication in SCADA is mostly real time communication to maintain different operations. It can be operational data communication or speech communication. For the efficient implementation of all the operations the communication has to be real time. Messages should be transferred in a short amount of time.

V. PROBABLE ATTACK POINTS AND TYPES OF ATTACKS

a. DOS (Denial of Service)

In this kind of attack, the hacker floods the main server with excessive requests with no legitimate return address. The server keeps on executing the requests only to find no return address. This leads to overhead in the server which diminishes the performance and it also prevents the legitimate users from getting access to the SCADA system. Those who do manage to get access to the server have to wait for a long period of time because of the overhead.

b. Sensors

The SCADA system is dependent on sensors which take data from the field and then deliver it to the control center. The control center then makes decisions based on that data and then send those decisions back to the field where installed equipment execute them. Hackers can hack these signals which would allow them to use generated electricity.

c. Integrity attacks

The data that is being transmitted when talking about smart grids is none other than electricity aka current. By hacking the sensors the hackers can also get access to transmission lines that are providing electricity from load centers to consumers. They can corrupt the current being transmitted by messing up with the voltages. This being the case can cause synchronization errors between both sites and might cause overhead on the central server which is dealing with the problem.

d. Personal attacks

By getting their hands on the power grid hackers can gain access to renewable energy generation systems, smart meters of individual customers, nuclear power plants and many more small to medium industries that are connected to the power grids. Smart meters can then be tweaked to show lower readings than actual usage and vice versa.

e. Transportation Infrastructure

The transportation infrastructure is not far away from the reach of the attackers. The underground roadways have ventilation equipment which is dependent on electricity. In metro cities, electricity is a major part of transportation fulfillment and routing mechanisms such as traffic light are important. Failure of these services for even a small amount of time can be catastrophic.

Attack history –

2010 – "Stuxnet" worm attacked simantic wincc system.

2012 – Attack on SCADA system of Schneider Electric.
- Attack on SCADA system of Telvent in Canada.

2014 - "BlackEnergy" malware invaded many power systems.

- A hacker organization known as "Dragonfly" attacked several industries in Europe and America.

2015 – For almost a month Pennsylvania-New Jersey-Maryland Interconnection in America suffered from continuous cyber attacks.

- The infamous Ukraine blackout.

2016 – Attack on Israel's power system.

VI. OBJECTIVES

Basic objectives that need to be met for any solution to cope against the threat of cyber attacks:

1. Confidentiality

The personal details of the end user must always be protected from the hands of the attacker. This should be the number one priority of the smart grid. If the hacker gets access to the location of some important individual in the society then it can turn fatal for that particular individual.

2. Integrity

The data that is transmitted which is the current should be kept secure from the hacker. If the hacker messes with the integrity of the current and delivers more voltage than required it might put extra load on the generation centers and can also trip the circuit breakers. On the other side, the consumer might also face issues with the abundance of voltage.

3. Availability

The authorized personnel should never lose control of the smart grid. If the hacker manages to prevent the operators from gaining access to the command interface that would be a drastic situation and there would be no way for anyone to deal with the attackers as no one can get in the system. The only solution would be to turn the whole grid off which would result in massive economic loss.

VII. PREVENTION

A. Isolate Main Controls

If the operations in the smart grid can be performed while keeping the main control centre isolated from the other enterprise networks, then the risk of someone hacking the physical controls can be substantially decreased. This does not mean that the communication will be impaired; all the other safe operations will be allowed access to all systems.

B. Uninterrupted Monitoring and Log Maintenance

It will be easier to catch hackers and prevent any damage if continuous monitoring is maintained. Logs also helps as they can help to analyze what had happened after the attack and thus we can prevent the future attacks. Base lining is another feature that defines what is considered right for a smart grid. Baseline defines certain boundaries for all the sensors, IED'S, controllers and other hardware devices which help to identify if any event occurs outside the normal patterns.

C. Authentic and Regular Updates

To prevent the new emerging attacks and threats to power systems, the system should be updated frequently from authentic manufacturer.

D. Protect Power Systems from Physical Threats

Other than focusing on all the cyber threats, the smart grid should be secured enough to deal with any possible breach on site. Many ports in front of a device which are situated at the outermost layer of the grid don't have strong security and they can be accessed by a trespasser.

E. Have Backups

It won't hurt to have a backup of the system architecture and all the flowing data within the system in case of a tragedy. There should be also an offline and physical backup other than an online backup which no one can manipulate.

VIII. COUNTERMEASURES

A. Source Authentication

If we can find a way to identify the source every time data gets transmitted from the smart grid to the various users as well as for the intermediate facilities such as load centers and sensors, we can decrease the chances of an intrusion substantially. The smart grid measurement at each location has a unique signature which is called spatial signature, which can also be utilized to authenticate source [3].

B. Extracting Substation Architecture Through IED's data

A substation is a part of the smart grid which is responsible for increasing voltage at generation stations so that it can be transmitted. A substation is also used for decreasing voltage at load centers where the electricity is distributed to various customers. By extracting the architecture of a substation one can analyze cyber-physical security as well as the smart grid analysis which can help better upgrade the system [4].

C. Machine Learning in Smart Grid

Machine learning is a fairly new concept on the technology map. We know that normal computers and phones are developed keeping in mind the concept of machine learning in the last decade or so. If this machine learning can also be implemented on a system such as SCADA it will certainly improve the performance as well as the security and the speed of counter attack once an attack is detected. If the system can itself learn from the attacks that it has encountered in the past and then keep a record of it and learn from the past experiences then it can possibly perform countermeasures on its own and also keep the human interaction minimum so that the humans/operators can think ahead and come up with their own countermeasures [11].

D. Benchmarking Vulnerability Scanners

As SCADA systems are widely used in power grids, a vulnerability scanner can be really useful. If the critical issues that a smart grid faces during an attack can be recorded and if this is done for all the smart grids out there, we can develop a vulnerability scanner which will benchmark different types of attacks. This can help identify attacks based on their benchmark score and can also help us not to waste too many resources on an attack which doesn't have a high score and vice versa. Steps in vulnerability scanners are:

1. Collect system information such as device version, IED'S versions, system architecture, etc.
2. Perform cyber attacks on these features.
3. Compare the results with the known vulnerability scanner database. If the result matches then it means that the vulnerability is confirmed.

E. Modeling attack and defense

The smart grids can be tested by a trial and error mechanism in which the grid can be attacked by several kinds of attacks on the weak parts of the systems which are vulnerable to the attacks and appropriate countermeasures should be taken. This will improve the machine learning aspect of the smart grids and would help us find a more efficient solution to the existing vulnerabilities and we can also find new vulnerabilities in the process [2].

F. Integrated Anomaly Identification

Different types of attacks on the system leave different kinds of logs of footprints. For example, when talking about Stuxnet attack, first of all it intrudes the system, then it changes the file system, then it modifies the system settings and after that it changes the status of system settings. So the intrusion leaves logs of footprints which can be detected by Anomaly Detection [9].

IX. CONCLUSION

Cyber security in the smart grid is still under development. The confidentiality, integrity and availability of the system must be maintained at all times to frame a strong defense for the smart grids. Countermeasure systems with vulnerability detection protocols must be developed, tested and deployed.

REFERENCES

1. 1. Shailendra Fuloria, Ross Anderson, Kevin McGrath, Kai Hansen, Fernando Alvarez, "The Protection of Substation Communications." Presented at the SCADA Security Scientific Symposium, Jan 2010
2. Yongge Wang, "Smart Grid, Automation, and SCADA Systems Security", in Yang Xiao, editor, Security and Privacy in Smart Grids, pp. 245–268. CRC Press, July 2013.
3. He, H., Yan, J.: 'Cyber-physical attacks and defenses in the smart grid: a survey', IET Cyber-Phys. Syst.: Theory Appl., 2016, 1, (1), pp. 13–27
4. X.-H. Yu, and Y.-S. Xue, "Smart Grids: A Cyber–Physical Systems Perspective," Proceeding of the IEEE, vol. 104, no. 5, pp. 1058-1070, May. 2016.
5. P. Haller, and B. Genge, "Using Sensitivity Analysis and Cross-Association for the Design of Intrusion Detection Systems in Industrial Cyber-Physical Systems," IEEE Access, vol. 5, pp. 9336-9347, November. 2017.
6. 6. Rong Fu1 , Xiaojuan Huang1 , Yusheng Xue2 , Yingjun Wu1 , Yi Tang3, Dong Yue1 "Security Assessment for Cyber-Physical Distribution Power System under Intrusion Attacks" IEEE (2018)
7. Ying Chen, *Member, IEEE*, Junho Hong, *Member, IEEE*, and Chen-Ching Liu, "Modeling of Intrusion and Defense for Assessment of Cyber Security at Power Substations" (July 2018)
8. Yi Cui, *Member, IEEE*, Feifei Bai, *Member, IEEE*, Yong Liu, *Member, IEEE*, and Yilu Liu, "A Measurement Source Authentication Methodology for Power System Cyber Security Enhancement" (July 2018)
9. Hao Huang, Katherine Davis, "Extracting Substation Cyber-physical Architecture Through Intelligent Electronic Devices Data (2018)
10. Soumya Shrivastava, Zia Saquib, Seema Shah "Vulnerabilities of SCADA Systems and its impact on Cyber Security" (Jun 2018)
11. H. Karimipour, A. Dehghantanha1, R. M. Parizi, K. R. Choo, H. Leung, "A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-scale Smart Grids" 10.1109/ACCESS.2019.2920326, IEEE Access.

AUTHORS PROFILE

Prof.R. Prabhakaran is an Assistant Professor (Senior) from the School of Computing Science and Engineering, VIT University, Chennai. He graduated in Computer Science and engineering – 1999 from Madras University, Chennai and Post graduated in Computer Science and engineering – 2006 from PSG College of Technology, Coimbatore, Tamil Nadu. He is pursuing his Ph.D from VIT University Chennai. His area of interest includes Network security, Biometric security, Computational Intelligence, Cloud security and Cyber security. He has published nearly 10 papers in international journal. His current research interests include power system reliability and resiliency, critical infrastructure protection and smart grid cyber security.

Dr. S. Asha, is an Associate Professor from the School of Computing Science and Engineering, VIT University, Chennai. She graduated from Madras University, Chennai and completed her Ph.D from Anna University Chennai. Her area of interest includes Network security, Biometric security, Computational Intelligence, Cloud security and Cyber security. She has published nearly 25 papers in international journal and conferences. Currently she is working in computational intelligence and Cyber security.