# Smart Grid Threat Analysis using NS3 Model

A Thesis

Presented in Partial Fulfillment of the Requirements for the

Degree of Master of Science

with a

Major in Computer Science

in the

College of Graduate Studies

University of Idaho

by

Sandeep Rathi

Major Professor: Michael Haney, Ph.D.

Committee Members: David Manz, Ph.D.; Jia Song, Ph.D.

Department Administrator: Terry Soule, Ph.D.

December 2018

# Authorization to Submit Thesis

This thesis of Sandeep Rathi, submitted for the degree of Master of Science with a Major in Computer Science and titled "Smart Grid Threat Analysis using NS3 Model," has been reviewed in final form. Permission, as indicated by the signatures and dates below is now granted to submit final copies for the College of Graduate Studies for approval.

| | | |
|---|---|---|
| Advisor: | Michael Haney, Ph.D. | Date |
| Committee Members: | David Manz, Ph.D. | Date |
| | Jia Song, Ph.D. | Date |
| Department Chair: | Terry Soule, Ph.D. | Date |

# Abstract

Securing smart grid [SG] is an essential part of power operations. In last few years, cyber security of SG has emerged as a critical issue because of the exponential growth in number of devices added in communication network. Such a heavy dependence on new technologies make SG to surrender in front of potential vulnerabilities associated with the new components which are not built with security in mind. The complexity and heterogeneity of components introduce new challenges in terms of security and privacy. With the demand of constant availability of power and complex interaction between components, experts possess tedious task to find vulnerabilities and threats in the communication network. Weakness in cyber security of power system is also threating for the physical security as both are deeply integrated with each other. With the complex networking of SG, it is almost impossible to secure every single node. Therefore, communication network needs constant monitoring and analysis of traffic to detect abnormal activities. To conquer security challenges, various techniques have been implemented in every aspect of SG, from implementing new architecture to upgrading control center, and deploying new secure components in Advanced Metering Infrastructure [AMI].To contribute into security of SG, we present a research which deals with threats in power systems and analyzes the impacts of these threats on control center, advanced metering infrastructure and customers. Before predicting the impact, simulated model is implemented using network simulator NS3. A model represents the communication network consist of nodes in Control Center and AMI, where substation node is transmitting data to control center node. The results of simulation are captured in the pcap files which can be analyze to conclude smooth working of smart grid.

# Acknowledgements

Firstly, I would like to thank my thesis advisor Dr. Michael Haney for his countless support in my research work. I am thankful for your invaluable advice and inspiration which helps to grow as independent researcher with the power of critical reasoning. I greatly appreciate the time you gave me from your super busy schedule for our meetings which helped me to improve my work.

I would also like to express my special appreciation and thanks to my committee member, Dr. David Manz from Pacific Northwest National Laboratory, you have been a tremendous mentor for me. I would like to thank you for supporting me mentally and financially, even when I was facing hardship in my research. I greatly appreciate the freedom you gave me to find my own path. Without your support and advice, my research would have been impossible. I enjoyed working with you and would love to work with you in future if I get a chance anytime in my life. It was fantastic to work with PNNL, and I am grateful for every PNNL member who supported me in research to reach the goal.

My sincere thanks to second committee member, Dr Jia Song for serving on my committee. I am gratefully indebted for your valuable comments and advice on this thesis.

I would like to thank Stacy for proofreading my thesis and helping me to get the better version of my work.

Finally, I am grateful to my family for their moral and emotional support in my life.

I cannot forget my friends who went through hard time together and cheered me always. Thank you: Vishwa, Karan, Aahna, Kundu, Chinu, Kamo and Diego for your unconditional support.

# Table of Contents

# List of Tables

# List of Figures

# Chapter 1: Introduction

The consumption of power is rising rapidly along with technology, so in order to meet the expectation of consumers we need a power grid which is smart enough to make some decisions more efficiently in case of an attack or natural disasters. To move forward let's discuss what smart grid means. It is an electrical distribution system which uses two way communication by exchanging data and electricity between the power plant and our houses. By using bi-directional communication it delivers power more efficiently and economically even in the adverse condition without effecting environmental health. Smart grid is capable of doing following:

1) Self-healing and Self-monitoring

2) Better resilience

3) Less power leakage

4) Improvement in operations with better load factors and system losses

5) Increased customer participation

6) Improved sensors capability

A smart grid is classified into three major categories [1]: smart infrastructure system, smart management system and smart protection system. Smart infrastructure helps to manage better power distribution in peak time where users can also generate electricity using solar panels and sends back to the power grid.The power generation in advanced infrastructure uses distributed resources like wind turbines, photovoltaic, and fuel cells which results better quality and reliability. At the same time with the increase of smart substation in the infrastructure, power flow is also getting complicated as it needs to pass through a large number of nodes with different type of devices installed on it. The smart meter is one of the main components of the smart infrastructure where information of end users can be sent at real time to the utility for billing and distribution purposes. The increase of complex infrastructure lays the foundation for smart management in the

security grid with objectives such as energy efficiency, demand profiling, cost optimization, and emission control. Demand profiling helps in matching power demand according to available supply,and this can be done using scheduling, shifting or reshaping of profile with less peak demands. The decrease in energy loss is hard to handle due to the distributed energy sources, but some research has been done to reduce it by using multi period alternating current power flow. Emission control needs to be done for environmental protection by using renewable resources and reducing CO2 emission during electricity generation. A smart protection system needs to address the issue of system reliability and failure protection. With the use of a wide number of renewable resources for power generation the stability of grid may be comprised.

## 1.1 Communication Technologies

Communication is the key element of the smart grid as huge amounts of data generates every single day. It is required to ask questions about networking and technology use for reliable flow of data from home appliances to utility. SG communication includes different types of networks like Home Area Network (HAN), Industrial Area Network (IAN), Building Area Network (BAN) and Wide Area network (WAN). Basically, information flows from a sensor and an electrical appliance to smart meters which further sends data to utility data centers. The first flow of data that is between sensor and smart meter is achieved using wireless communication like ZigBee, Z-wave or powerline communication. The second flow uses the cellular technology in order to send the data up to the data centers. There are various technologies explained in [2] according to the suitable environment along with their advantages and disadvantages. Currently, smart grid is facing challenges in both wired and wireless technology in terms of efficiency, reliability and security. The availability of new home appliances and expectations of transmitting high speed data make the decision hard to choose from available technologies.

### 1.1.1 ZigBee

Zigbee is a wireless technology which is use to communicate with other devices in a network even if vendors are different for each device. It is based on IEEE's 802.15.4 network standard. It is best suitable for HAN, where ZigBee integrated smart meters can communicate with ZigBee integrated devices and control them. It becomes very useful as home owners can check their energy consumption in real time. With the introduction of ZigBee smart energy profile this technology has been used in various applications such as automatic meters, demand response, power fraud detection, sensing and monitoring. It is now the preferred standard for HAM applications as well. The performance evaluation of ZigBee in different smart grid environment in terms of network throughput, end to end delay, energy consumption and packet delivery ratio has been discussed in [3].

### 1.1.2 Cellular Network Communication

It is a good option to send data from smart meters to utility data center for real time communication as high data rate connection is required. With the growth of 3G/4G technology data can be sent at high speed with high level security and better Quality of service (QOS). This communication helps to save money and additional time to build infrastructure for smart grid applications. In addition, technologies like GSM, CDMA, GPRS and WiMAX support different types of application used in Home Area Network (HAM). The features like low cost, better coverage area, high speed data, strong security controls make this option a strong candidate in the environment of smart grid.

### 1.1.3 Powerline Communication (PLC)

Among the wired technologies PLC is highly acceptable by utility companies around the world for remote sensing and load control applications due to its direct connection with the meter. It helps to implement AMI successfully in rural/urban areas where other technologies fail to meet the expectations of utilities. In typical PLC network, smart meter

is connected to data concentrator through power lines which further connects with a data center using cellular technologies. The transmission of data is broadcasted which makes it less secure as compared to others. Additionally, due to harsh and noisy environment, channel modulation also becomes difficult.

## 1.2 Components of Smart Grids

### 1.2.1 Advanced Metering Infrastructure (AMI)

AMI is the most important component of the SG which includes mainly operational gateway, meter data management system and smart meters, helps the customers to keep track of energy usage in more efficient way with low billing cost. It is a computer based system connecting homes or offices to the utilities using communications like the internet or public switched telephone network (PSTN). This infrastructure assists consumers to have better control on their power usage by looking into real-time prices from different tariff plans and almost every plan has higher power cost more in peak time as compared to off peak hours, so customers are always motivated to reduce their electricity bills by shifting their tasks in off peak hours. Using this technique power companies are giving more control to users as they can change to different plans according to their requirements for the coming month. Because of real time exchange of data and necessary two way communication, it is helpful for the grid to manage energy demand in more efficient way. Smart meter plays an important role by monitoring demands, creating logs of events like power outage, and sending control messages to appliances in case of emergency. Smart meters uses technology called Automatic Meter Reading (AMR) which is effective in collecting data for analysis or troubleshooting as it sends different types of data packets to the central database and using this data electricity provider can solve the issue without physically visiting to the customer's place. The transmission of data using these meters is simple and secure. Smart meters transmits data using Wi-Fi technology to the nearby

router which is placed on the electric pole, which further sends the data to the utility using cellular communication. The tremendous growth of smart meters in the world is taking power technology to the new heights but it also introduces serious security challenges which need to be test for the safe transportation of electricity.

AMI consists of millions of low cost devices, built without any security objectives in mind and also placed in physically Unsure location. These devices are the prime target for the attackers as tampering of data is easy. Even different classes of attacks can be launched due to presence of common security bugs and insecure coding of the software. Among different types of cyber-attacks, energy theft in AMI [4] is the most common attack in which the customer sends the manipulated data to the utility. Most of the AMI components are software based so it is easy for malicious users or customers to launch different types of attacks depending upon if the data is in rest in meter or transmitting through the network.

### 1.2.2 Control Center

It is the essential part of the smart grid which helps to monitor, analyze, visualize and control the power system. In traditional power grids, power operators were assigned tasks in the control center to watch the smooth flow of electricity using limited devices. If any fault occurs in the line they need to spend hours on it to retain the power but with the smart control center job become easy and effective with the new monitoring devices. We can go to the root cause of the fault by analyzing the data collected from sensors and there is less need to visit the place physically every single time. Control Center always requires new functions as the power system is getting more critical every day and we need set of tools to monitor these systems. The monitoring in the SG depends on the state estimators which works on data provided by SCADA systems, RTU and nowadays with phasor measurement units (PMU) as estimation in this case is more accurate due to availability of the voltage angles. Monitoring devices helps to collect data which is use for analyzing

the heath of power system. The more number of devices or sensors we install the amount of data will rapidly increase which makes tough for the operator to find useful information, so we need information according to specific fault type. It helps the operator to identify the fault quickly and save time for other tasks. Along with monitoring, visualization is also key component of the control center where the operator can see the working of power systems using the one line diagram on human machine interface (HMI) to see connections of buses with each other without any control of customization of these diagrams. The data collected from the monitoring and visualization phase helps to check the analytical capabilities of the SG which further develop the security assessment techniques. Analysis is done using predefined simulation models which depends upon the state estimators, if the state estimators fail then it's hard for simulation to detect the problem. Once the analysis is done security assessments comes into action which again depends on the simulation models and performance state estimator.

Besides the upgrading of smart grid it is essential to have a smart control center which not only helps the operator to make a better decision in case a fault occurs but also keep checks on the health of each component. In order to make the control center smarter plenty of research has been done and still it is one of the top priorities of SG. The researchers in [5] and [6] gave some useful ideas about how the future smart control center should look like. Using their vision, monitoring is better if we use synchro phasor as rather than depending on state estimators as it is better in state measurement. The state measurement helps to build the foundation of real time stability assessment. Visualization becomes more effective if we add Geographical Information System (GIS) technology into it. It helps the operator to monitor the system conditions in real time and clear the faults quickly. Integrating simulation models with measurement based analysis helps to predict the future system conditions as results from measurement can be fed into simulation models. The smart control center concentrating more on real time analysis and solving faults. Before the analysis phase it is important to check the integrity of data coming from

monitoring devices like sensors and PMU's. It was shown in [7] attackers can manipulate state estimators using stealth attack and bypassed the bad data alarms in the control center.

### 1.2.3 Smart Substation

In smart grid it is essential for the substation to be smart based upon advanced automation technologies. The interdependency of cyber and power components make substation more vulnerable and we can often see failure in one's component process affected the output of the other. In order to ensure smooth working smart substation consists of robust monitoring and alarming systems which helps operators to get informed if any equipment behave abnormally. The alarming systems provide an immediate warning message to authorized users using different communication means like phone, internet or intranet. The monitoring system helps to gather information about the fault occurrence which is sent to the control center for further analysis in order to update the rules for the alarm system and to stop the catastrophic failure. In smart substation communication is crucial element as signals are based upon time stamped with high accuracy but at the same time they need to deal with components of different kinds from various vendors. It is hard for substation components to communicate with each other until there is availability of any single communication protocol like IEC61850 which provides interface among IED's in the substation and also between two substations. Smart substations uses IEC 61850 standard with the goal to define digital communication within a substation. Based upon the IEC 61850 standards substation is divided into three levels: Process level, Bay level, and Station level. The process level contains devices like circuit breakers, actuator, indicator, and data acquisition to measure current, voltage and other parameters in the substation. The Bay level consists of IEDs that monitor data from different equipment's and can issue commands such as tripping circuit breaker if there is any instability in voltage, current or frequency to ensure reliable operation in the substation. Some examples of

IEDs are voltage regulator, circuit breaker controller, and protective relays. The Station level comprise of HMIs, router, gateway, and SCADA servers. Since IEC 61850 standard is open, any vendor can use this to make the product according to project demand and client specification to work in the substation. Using common standard is one step forward towards substation automation. Substation Automation (SA) refers to state of the art of providing control and automation functions to build a smarter and more reliable power grid over a wide range of operating conditions. In SA, communication is key role as data transmission at high rate with maximum delay of about 4ms is recommended and to fulfill this demand Ethernet [8] is the best communication technology that can be use as standard option. Switched Ethernet along with UDP is preferable in substation because of its characteristics of No collisions, Full duplex, and Store-Forward. The companies like ABB, SEL, and SIEMES provides Substation Automation System [SAS] packages [9] to enhance the substation performance and reliability index for robust operations.

Smart substation contains intelligent decentralized controllers or IED which are capable of taking any action to increase the optimization based on the data they receive from the sensors or if any anomaly occurs. One common example of IED is protective relay which is a computer based program use to detect fault in the electricity line. In traditional substation, grid instability was one of the major issues which is resolved in smart substation using IED and phasor measurement unit (PMU). PMU helps to measure grid health with more accuracy and faster than SCADA systems using magnitude and phase angle of sine waves found in the electricity. As the SG is expanding, the number of components from different vendors is also increasing rapidly which give attackers a large surface area to launch vast categories of cyber-attacks, for example IED can be a target of DOS attack by traffic flooding or spoofing attack where attacker can message IED to open/close the switch to create power imbalance in the substation. Generally, network gateway is a prime target of DOS attack so it is mandatory to implement strong firewall rules and access control to avoid basic types of attacks.

## 1.3 Standards

The large pool of applications and technologies in smart grid make it tough to create standards which meet the expectation of every vendor. The interoperability of smart grid devices and systems is the prerequisite for any standard. Any new standard for SG should be open, stable, secure and adaptable to industrial equipments. It should be developed for the international acceptance, and developers make changes regularly for the next version to meet the requirements. The wide acceptance of the standards help advanced devices like smart meters to integrate with other components of the SG for the better productivity and safe environment. Many efforts have been done in America by different organization like NIST, ANSI to get the standards which are fairly open, logically strong and built on non-discrimination policy. Some of the standards are discussed below.

### 1.3.1 ANSI C12.1

The primary focus of this standard is design and construction of the meter so that they can handle failure and increase the accuracy to meet the performance criteria. It doesn't deal with any kind of cybersecurity issue since the performance and testing is important part of it. It checks the physical parts of the meter also. The devices like ac watt meters, demand meters, pulse and auxiliary devices establish under this standard to meet the acceptable performance.

### 1.3.2 ANSI C12.19

This standard helps to send utility data such as energy usage from meter between end device and computer using table structure. The end device can be electricity meter and computer is any device like hand held meter which is able to communicate with end device. The information model contains procedure and table classes whose attributes can be modeled using XML based table language. The instance of this model can be used to communicate with end devices of different vendors. PAP05, which is standard meter data

profiles has been setup to help the utilities for the smart grid functions such as demand usage and real time information regarding usage. It didn't define anything regarding designing of end device or protocols use for communication.

### 1.3.3 ANSI C12.18

This standard is used to define protocol for the communication between the smart meters and C12.18 client using the optical port. The client can be a handheld meter, any computer or electronic device which support communication with the electricity meter. It uses the point to point connection between the client and device with type2 optical port.

### 1.3.4 IEC 61850

This standard is used as communication protocol for the components in distribution and transmission substation. It was basically introduced for the substation automation where communication is done over TCP/IP networks or LAN along with high speed Ethernet to get the response time for protective relay. Smart substations consist of wide variety of intelligent electronic devices which always communicate with each other but this communication is not smooth everytime. Sometimes there is an issue of interoperability which is handled by Priority Action Plans (PAP). PAPs is determined by standard setting organizations (SSO) which makes a decision whether standard extension is required and if they extend then steps to implement new standard should be available publicly with guidelines. PAPs are always built with the involvement of stake holders in smart grid in order to resolve a wide scope of problems. IEC 61850 consist of many parts which contains details regarding the standard. These parts demonstrate details like system requirements for communication between IEDs, basic communication structures which includes principles and models along with common data classes, communication for monitoring and control, communication between substations, and communication between substation and control centers. The complete detail of every part is given in the NIST guide [10]. IEC61850 includes features of data modeling, fast transfer of events,

setting groups and many others with aim to increase the scope of standard and meet the expectation of efficient working in substation.

### 1.3.5 IEC 1815(DNP3)

This standard is used as a communication protocol between the substation and control center and also helps with the substation automation. It is really popular in the power industries and critical infrastructures like oil and gas, water supply which uses SCADA systems along with DNP3 as a communication protocol. It was built to be first open source protocol for the utility industry with the desire to increase the bandwidth from 1200 bits per second to fairly high amount which was not common in power industry. The standard contains many features which helped utility to faster the communication with better security level. It is having broadcast ability where we can send message to multiple devices and this protocol also gives option of "select before operate" where master sends the control command which is responded by the outstation, later if outstation doesn't receive operate command within certain amount of time then it will not execute any action. DNP3 is mature protocol for time stamped data as it works on almost all data while some protocols like Modbus who doesn't have any way for time stamp data and some works only on binary data. This protocol contain method which helps with accurate time synchronization and flags provide a mechanism to check whether the data is valid. The architecture of DNP3 is quite simple as it consist of three layers, Data Link, Pseudo Transport and Application layer. The data link layer manage the data frames between the devices. A frame is having header part of 10 bytes and maximum length of data section is 292 bytes including 16 bit CRC fields for every 16 bytes of data. The pseudo layer control of message fragmentation and then reassembly of those messages. It adds one bye for the FIR and FIN flags and a sequence number. The FIR represents the first frame, FIN is for last frame and sequence number is use to reassembly of frames, it also helps to detect the lost frames in communication. The application handles DNP request

and reply messages from the master and outstation devices. A master sends request to outstation to perform task, collect and provide data or synchronization of internal clock. The application layer fragments message which exceeds the limit and size of fragments is between 2048 and 4096 bytes.

### 1.3.6 IEC 62531

This standard emphasize the cyber security of communication protocols. It defines the requirement of security for power system management and associated information exchange. It also includes communication network and security issues for Transmission Control Protocol (TCP), Inter Control Center Protocol (ICCP) and Manufacturing Message Specification (MMS) profiles. It comprise of 8 parts where each of the part speak about cyber security. Part 1 primary focus is information security and how it can be implement to power system operations. Part2 illustrate terms or definition of cyber security and communication. Part3 explains the technical details on how to secure confidentiality, data tampering and message level authentication for TCP/IP based protocols. Part4 provides specifications on how to transfer information securely while using MMS based application by specifying methods, algorithms and protocol extension to use. Part5 focus on the application layer authentication, here confidentiality is not important but authentication of sources and receivers is essential while encryption can be achieve by combing this standard with other security standards. Part6 works for the security of IEC 61850 profiles as different profiles required different security levels while authentication of source of data, receiver of data and data integrity remain basic requirement. Part7 mainly concentrate on the intrusion detection and intrusion prevention. It strengthen the communication network management which supports the power operations by monitoring and controlling the network. Part8 implements the role based access control (RBAC) which states that no subject is given more rights than required to perform the task.

# Chapter 2: Background

## 2.1 Cyber Physical System

Cyber Physical Systems (CPS) refers to integrating of new generation systems having computational capability with physical systems of different application domains. In other words, CPS bridges the cyber world of computation, networking and communication with the physical processes of the real world. It is helping humans to interact with the physical world around us. Some of the examples for CPS are medical devices, transportation systems, airplanes and space vehicles, robotic systems, hybrid gas-electric vehicles, and factory automation. The designing and development of these systems always posed tons of technical challenges for the researchers, Lee [11] discussed some of the design challenges of CPS. In CPS a bunch of things happens at the same time, unlike software which run processes sequentially. Physical processes are composition of many processes running at the same time and the correct measurement of these processes is essential as they are inter-dependent on each other. In general software, completing a task with longer time period is not a big issue and can be optimized but in CPS it makes a difference in correct functioning of the system. For example if we interface a computer with physical plant of automobile or power than the computation time matters. The safety and reliability of physical systems is challenging as compared to general computing system. Moreover, standard abstraction rules don't work for the physical systems, so it is mandatory to modify these rules and add some computation and networking abstraction rules. CPS research is always trending, advances in this field depends upon the identification of industrial needs and collaboration between academia and industry. Earlier researches in CPS had great impact on the industries like power, health and transportation and advantages for developing next generation system are wide ranging.

### 2.1.1 Applications

1. Healthcare Systems: - CPS in the medical field plays an important role and at the same time it is challenging to build system which can be highly reliable, intelligent enough to deal with patient in special circumstances, highly efficient and interoperable. Now a days hospitals are dependable on medical devices for providing high quality diagnosis to patients so these devices need to be capable to process different types of data coming from various number of devices in the network. The integration of distributed networking, storage, computing and sensing makes the medical systems more intelligent and critical to operate in a secure way. With the constantly changes of data we need CPS which can deal with large scale complex data and compute fast with high accuracy to generate final reports for the patient. As CPS is getting an essential part of medical field, integrating it with the cloud technology is one of the option to explore. Y Zhang [12] introduced a smart health system which uses Cloud and Big Data technology to manage large sets of medical data sets and parallel computing. CPS is also getting involve in the research for the human system function. A few examples are brain machine interface, orthotics and exoskeletons, and prosthetics

2. Smart Grid: - With the increase in demand of using renewable energy, the research and technological advancement in the power grid is at the highest priority. The smart grid is the option which can help to meet the expectation of increasing energy usage by expanding the grid generation, transmission and distribution capabilities. The main goal of the smart grid is to improve energy efficiency by investing into modern infrastructure of the grid. For example advances in Phasor Measurement Units (PMU) hardware is worth looking at for a better future of electricity. Smart grid makes the production and distribution of electricity more powerful through real time sensing and analysis. The sensors sends data to the control center which helps

to manage real time energy demand and decision making. Furthermore, smart grid encourage customers not to use more energy in peak time and provide real time price information to the customers. Finally, bidirectional flow of information helps customers to send electricity produced from renewable sources to power station.

3. Transportation Systems: - This sector is the back bone of any country so research in CPS transportation helps to grow modern economy infrastructure of any nation rapidly. The transportation system usually consist of physical components and objects which can interact with each other for the smooth and efficient flow of traffic. These objects can be vehicles, traffic infrastructure, drivers etc. Smart vehicle is equipped with intelligent device which helps the vehicle to exchange information using wireless technology between vehicle to vehicle or vehicle to infrastructure. It helps vehicles to assist driver or autonomous driving about the traffic condition, which is useful for planning ahead and drivers get more time to take actions like speed control, brake, and steering control. Modern transport CPS have a complex network as it contains a lot of subsystems which are connected with each other and software components. While designing CPS we need methods and techniques to assure real time sending of data in this complex network. Hence, computer algorithm in the vehicle can make better decision to avoid car collision in autonomous vehicle. Air Transportation Systems also require research which can directly impact on the design of the aircraft, air traffic management system and safety. In order to achieve the safe and secure operation, a key challenge is verification and validation of complex system. As with the increase in complexity of the system, the cost also increases so we need cost effective secure systems. As aircraft systems are more complex so there are definitely some control engineering challenges like distributed system architecture, health monitoring systems.

### 2.1.2 Challenges in Cyber Physical System

1. Architecture: - CPS architecture is getting complex with the enormous increase in the number of devices of different functionality added to the network. In order to handle this complex network, standardized architecture is always in demand that can help to integrate control, communication and computation in deploying CPS. Software platform with well defined architecture are require for the reliable and scalable CPS. It should allow other devices to interact with new devices to achieve the common goals but at the same time working on its own goals to complete them on time. In modern CPS, the network should be capable to learn about the potential of the new devices in case of utilizing new sources. Detecting and preventing malicious devices to connect with the network is challenging. Hence,a network requires rules, protocols to restrict malicious devices to join the network and even if they are inside the domain, rules should be follow to lock down malicious devices. The devices should be aware of the impact of their own actions on the environment and be aware about other devices actions, whether or not they are beneficial to achieve the goal. CPS architecture should be consistent and reliable which helps to capture information from various physical devices.

2. Abstraction: - The scale of CPS is getting large everyday with the addition of new components in the network. However, it is hard to find standard abstraction which permit modular design and development of CPS. Every component in the network interacts with other entities in a complex manner which makes implementation of CPS more challenging and difficult. To conquer this issue we need to build software using high level programming language with high abstraction for such complex systems. Real time CPS can be implemented using programming language which is platform independent, and abstraction can be used for sensor reading, updates of actuator and mode switching of control systems. In order to handle the complex-

ity of CPS we need to raise the level of abstraction in software development and this can be done using model driven development. If we can design models in the application domain rather than writing individual programs, and transform that model into real implementation. It helps to increase the productivity of software development. Models are used for the control logic which need to be implemented in software. Most of the physical properties like real time power constraints, and laws of physics should be captured inside the model. The real time embedded system abstraction is also important factor here. Using the new routing and queuing schemes can help to reduce network delay in the network.

3. Security and Privacy :- Securing advanced CPS is more challenging than traditional computer security of CPS. We need to deal with cyber components like computation and communication and physical components like sensors and actuators at the same time to ensure that data and operational capabilities of the system are running to fulfill their mission. Due to complex and heterogeneous behavior of CPS, it is difficult to deal with its security and privacy. The cyber physical interaction makes it difficult to trace threats and vulnerabilities which may attack multiple CPS components. In the case of SG, common protocols like DNP3 and Modbus used for communication already have numerous number of vulnerabilities which makes it easy for attacker to launch the attack. In addition, software being used are not build with security in mind. For example, remote smart meters are inviting attackers to use this feature to have full control of meter. After getting control of smart meter, a malicious attacker can try to attack other smart meters in AMI which can lead to blackout or price modification in the bills.

## 2.2 Modeling Cyber Physical Systems

CPS are integration of computation, networking and physical processes. In order to design such systems, deep knowledge of computing, network monitoring and working of

physical processes with feedback loop is required. The computing in CPS is different from general software, time taken by the CPS defines the correct functioning of the system but not efficiency issue. CPS have a mission critical nature so any compromise in physical or cyber security can have extreme consequences. To avoid any kind of disturbance in the complex process of CPS, working with models has major advantage. Using modeling we can say definite things. For example, setting the models parameters according to the requirement, asserting model is deterministic which means that with the same input it will always give the same output. Before implementing directly any changes in the physical processes, it is always recommended to try it with the model and analyze the output if it is same as expected. To build a homogenous model for SG, the abstraction level of model should be high. In that case, it give us confidence in implementing the model in the physical world. Otherwise it is dangerous to implement any model directly to SG as even a problem in subset can lead to blackout or put human lives in danger. For building and designing a heterogeneous model in CPS, Ptolemy II [13] is a good framework to consider. It is an open source framework built in UC Berkeley which supports actor oriented design approach. In this framework, actors are software components which interact with each other using messages through interconnected ports. In Ptolemy framework, an actor control the semantics of the model called director and it implements model of computation. All actors are connected with each other in hierarchal fashion. Modeling CPS pose several challenges [14]. It is difficult to judge the behavior of model as even after using determinate input it may exhibit non determinate behavior which can be shocking for designers. The next challenge is keeping the model consistent. If we are building test model then it shouldn't be only for regression test as it is tough to build final design of model from it. In the complex model it gets harder to evolve number of models with multiple variants and ensuring consistency among models. The bigger model comes with new challenge, preventing the model components to be misconnected. However, there is always possibility of misconnection which can leads to errors: unit errors, semantic errors,

and transposition errors. While modeling CPS, it is preferable to build implementation model along with functional model as we can't ignore implementation details like underlying platform and the communication network. The complexity level reached to next level while modeling CPS with components having distributed behavior. Examples of this kind of issue are network delay, difference in time measurements, imperfect communication between components and many more. Lastly, heterogeneous nature of components make it more complex in modeling CPS.

## 2.3 Need of Simulation

The communication infrastructure of SG is getting large and complex with the addition of enormous number of components. In recent years, lot of research has been done to completely secure the communication in SG but deployment of new technologies make the secure network vulnerable to attack. To reduce the risk factor of getting attacked, simulation is powerful approach to take into consideration. It helps to design and evaluate smart grid communication network, protocols, architecture, etc. Simulation is always safer and ethical way of implementing new experiments as it removes the possibility of loss of service in any device which is taking part in the communication. Using simulation we can configure environment parameters according to required scenarios and no additional cost involved even if changes or upgrades are needed for the experiments.

Simulation provides the ability to study the interaction between heterogeneous process and their components in the early phase of analysis. In addition, we can create environment which helps in controlling and monitoring different control devices. Using simulation is cheaper and safer as constructing the SG environment involves real equipment's which are expensive and highly sensitive in nature. Therefore, it is recommended to use simulation for the testing purpose which reduces the changes of damages to equipment's and loss of services. It not only help in removing the risk of doing experiments but enhancement in models also become easy which results in optimization of performance.

While representing SG functioning using simulation, it is challenging to build simulation model which represents most features and integrate with other components. Hence, model should have capability to interact with physical components which we called Hardware in the Loop (HIL). In HIL, some parts of the control loop components are real hardware and other parts are simulated which is use to enhance the quality of testing. Usually SG uses two types of simulation for the power and communication network.

- Continuous System Simulation:- In continuous system simulation, system state variable changes continuously with respect to time. Typically, simulation depends upon differential equations which represent system and equation includes parameters associated with the system which we called system state variables.

- Discrete Event Simulation:- Discrete Event Simulation is suitable for the systems where state of system is subject to change due to occurrence of discrete sequence of events. Any event which take place at particular instant of time change the state of system. Otherwise, there is no change in system between two consecutive time steps. In time driven simulation, instead of doing integration of time, the time bound to events. Thus, simulation hops from one event to another

  Both type of simulation uses different types of approaches for modeling but they are helpful for SG to build environment for testing. While building environment both simulation are useful as one helps to build power systems model and other for communication network model. However, in SG communication network simulation, fixed interval is selected for event synchronization. Scheduler is placed to maintain and synchronized time-order list for every event, this is useful for the simulation of event. Due to dynamic nature of power systems, continuous time-synchronized simulation is used to build models where variables are defined in continuous time functions. Hence, power system elements are represented using the differential equation. On the other hand, communication network is modeled using event driven simula-

tion. The termination of simulation is based on: Special termination of event, for example: drop of 50 packets, Specified simulation time, for example: run simulation for 1000 secs, and until future event list end. As Discrete event simulation doesn't require to run in every time slice, therefore it can run faster than continuous event simulation.

Although power simulators or network simulators are being used in their domains from many years, it is combined effort of both type simulator called which is getting attention from last few years. It can be achieved using various approached, two of them are discussed in [15]: co-simulation and comprehensive or integrated simulation. We are more interested in co-simulation approach as it uses existing simulators capabilities, less expensive and not time consuming. In co-simulation approach two simulators are used, each of them have their own interface for configuration, data outputs etc. Hence, main challenge is to connect, handle and synchronize data and interactions between two simulators. The two well know approaches in co-simulation are EPOCHS [16] and DEVS [17]. The EPOCH approach is based on federated simulation which used simulators NS2, PSLF, and PSCAD/EMTD. The intermediate software called RTI act as interface between all components. RTI is responsible for simulation synchronization and for routing communication between components. The DEVS approach integrates power system continuous models and discrete event communication network model. This technique basically converts the continuous power dynamics into discrete events using state event detection mechanism.

The above discussed schemes were the initial efforts to integrate power systems simulation and communication network simulation but it contains some errors. The EPOCH scheme is having synchronization time issue between two independent simulators. The synchronization mechanism introduces accumulating errors which make it tough to select synchronization boundary. In order to remove this error, H.Lin [18] proposed a new framework for co-simulation. This new method proposes a global

scheduler for co-simulation and using this scheduler both simulators which were running independently, now shares same timeline. Using this framework whenever there is need of power system and network simulator, request is processed quickly without any unnecessary wait. Similarly, one more method has been proposed in [19] where authors demonstrated real time co-simulation to analyze performance of smart grid. This research introduces real time co-simulation using OPNET and OPAL-RT. For synchronization in real time simulation, interface is required which act as data buffer which allow real time packet exchange using protocols like TCP or UDP. Although we have discussed about co-simulation in detail but in this research we are interested only in the network communication model. This network model has built using NS3 simulator.

# Chapter 3: Smart Grid Threats

Power system operations have always been critical to handle as power availability is the prime focus. However, in last decade with the development of smart grid the other two cyber security objective i.e. confidentiality and integrity are also became equitably essential. In general, confidentiality prevents unauthorized user to access private information. Integrity prevents an unauthorized user to modify private information. Availability ensure access of information in reliable and timely manner. In cybersecurity there is no single set of information which covers every threat category of SG. Although with addition of computer systems, monitoring and controlling of process becomes more feasible. Power industry has been upgrading their systems for continuous power supply to customers and business industry but with the integration of computer systems, the task become more challenging and sophisticated. With the addition of cyber system, the power industry increases the overall efficiency but also vulnerable to attack. In this chapter we will discuss some of the potential threats to SG taking simulation model into consideration.

## 3.1 Availablity

Availability is the primary security objective of SG. In SG, among traditional cyber security properties of availability, confidentiality, and integrity, availability gets the highest priority. This is because cyber infrastructure in SG deals with continuous power flow so it is mandatory high availability. For most users, the availability of power is more important than confidentiality or integrity of information about power flow. Since power have 24/7 availability requirement, upgrading or correcting any equipment in the SG is challenging as it may lead power loss. Loss of availability can cause inability to access operations which can further undermine power distribution and delivery. In terms of communication, network unavailability may affect the real-time monitoring of critical power infrastructure and if attack occur it may lead to blackout. One of the main attack

which target availability in SG is DOS attack. It can have immediate impact on the communication network which is backbone of SG

### 3.1.1 DOS

It is a form of attack where attacker or adversary makes the resources unavailable in the network for the legitimate users by disrupting services. The DOS can be launched in two ways:

1. Special crafted data: - Attacker sends the special crafted data which victim is unable to handle and results in a crash of system or component. It involves manipulating fields in the protocol network protocol like TCP.

2. Flooding: - This attack is launched by sending too much data to the server or component in the communication network so that all of its resources get busy with attacker data and fail to serve the legitimate data.

In SG, DOS attack can be accomplished by flooding the network with data packets, jamming the communication channels, and compromising the devices like smart meters to render the data to be transfer to control center. The types of DOS attacks are:

- UDP Flooding: - In this attack UDP packets are sent to open ports of server or appliances which reply back with ICMP packet after checking the service for a particular port. When large number of packets are sent, most of the resources of server are busy in replying back. As a result, it is unable to answer the legitimate requests.

- SYN Flooding: - It uses reliable TCP connection to exchange data between sender and receiver. A three way handshake (SYN, SYN-ACK, and ACK) is follow for sending the data. In SYN flooding, attacker sends SYN packet and server replies with SYN-ACK which is acknowledge for the packet received. In next step attacker needs to reply with ACK packet but it didn't reply and server waits until time out. Hence, server resources got used while waiting for answer.

- Teardrop Attack: - In order to transmit data, packets are broken down into smaller packets called fragment, and when these fragments reach the destination they re-assemble to form original data. In teardrop attack, attacker crafted few packets to overlap so that at destination, they can't reassemble themself.

It is a resource consumption attack and can be launched in bigger form by utilizing distributed attack sources such as compromised meters and appliances in the network. Now the attack is called Distributed Denial of Service (DDOS). An attacker can compromise various components including networking devices, communication links, smart meters and utility servers to launch the DDOS attack. If the attack is successful then it is hard to control the power supply and various other functions in the control center and Advanced Metering Infrastructure (AMI).

As we know availability of information in SG is really important especially the price of information for the customers which can affect the power demand supply. The main concern for the SG is the message delay than data throughput, due to time constraint for messages transmitted in the network. A DOS attack targets the control center or smart meter with the aim of unavailability of sensor data, control data or both. Either way, operations get affected which makes power grid unstable. SG uses the IP based protocols which are vulnerable to DOS attacks, and it is very easy for a malicious user to launch attack on the communication network due to its susceptibility of being compromised. For example, any node in the network which is acting as a server or access control device uses authentication protocol for authentication and authorization can be the victim of DOS attack. If the attacker has control on a bunch of nodes in the network, then he can flood the network anytime with data, and running the simple processes under these circumstances can be dangerous sometimes.

Although the flooding attacks are quite common for the SG but special crafted attacks are more effective and can result into quite large destruction for SG. For example, if the attacker sends DNP3 message to master with code 14, which indicates that service is not

working on the outstation device, it will prevent the outstation from communicating with master or HMI. This attack is called Warm restart attack. A continuous streaming of this message can result into a DOS attack. A well targeted DOS can lead to important systems down in the network which can result in a shutdown of the SG. Another type of attack that can interrupt smooth working of SG is jamming attack. IEEE 802.11, which is standard for wireless local area networks, is commonly used for communication in the SG which is vulnerable to Physical and MAC layer jamming attack [20] [21]. The physical layer attack is the most common jamming attack for wireless communication. Since attacker just needs to connect with communication channel rather than authenticate itself which makes it easy for him to launch DOS attack. A MAC layer is responsible for point to point communication where adversary can use compromised device to modify its MAC parameters at the cost of performance degradation of other devices using same communication channel. In SG, spoofing is a big threat for confidentiality and integrity of data. A spoofed device by taking advantage of MAC frame, can send fake information to other devices. For example, malicious node in the network can broadcast fake address resolution packet to shut down all IEDs. Although these attacks have already been seen a long time ago and various defense strategies [22] [23] discussed, still they are worth examining in the context of SG wireless network.

Usually automation systems are used in cyber physical systems to take control of physical processes like converting steam into electricity. If these systems failed to serve for the mission then their action is called Loss of Control, which results in the shutdown of the physical process. A small disturbance in the physical process can affect the working of the whole SG and control center equipment, like HMI will exhibit unexpected results. The operator using HMI can see system overloading and try to launch to back up plan but flooding of data can prevent the execution of any command. In that case system overloading causes equipment failures which can result into physical damage. In CPS, feedback loops are important and also in the case of SG. They help to monitor and

control the physical processes of SG. Hence, breaking the feedback loop by attacking on the network or flooding the device with data, make it unresponsive which can lead to serious failure in the SG. In this case, Sensors may fail to give latest reading and RTU will not process commands which leads to failure in network communication and all other devices are unware with the system state.

The countermeasure for the DOS attack can be isolation of the compromised nodes but it may lead to severe stability issues. Thus, understanding the working of physical systems is a key to defend SG. On the other hand, building the simulation model and implementing DOS attack inside the model is also a good way to start learning about the impact of this attack on the network.

DOS attack in the SG can be small or large depending upon the attacker's goals and physical factors, but in either case operator will lose control over the physical processes. In a small attack, subset of devices from the network fail to take part in the communication. This type of attack targets devices with specific vulnerability. For example, any device using Zigbee [24] as communication technology is vulnerable to attacks like eavesdropping, DOS, message tampering, selective forwarding, sinkhole attacks, warmhole attacks, and Sybil attacks. In a large attack, significant number of devices get affected which results in the loss of control data, sensor data and billing data. For example, instead of one sensor being attacked, all of the sensors in the network suffer from DOS attack, and the communication between control and AMI is lost. Furthermore, redundant devices using the same network is useless.

## 3.2 Confidentiality

In SG, confidentiality is equally important as availablity and integrity. To protect the privacy of customer data or status of power systems, it is necessary to preserve authorized restrictions on information access and prevent disclosure of information to the public which can reveal anything about individuals. Smart meter data is usually of two types: High

Frequency and Low frequency [25]. High frequency data is sent in every few minutes from smart meter to utility which contain information about specific power usage pattern of customer. Low frequency metering data is sent on weekly or monthly basis to utility for power management or billing purpose. The former type of data contains detailed information which can be used to gain insights of user behavior. Therefore, it is required to secure the communication channel which sends users sensitive information. Otherwise attacker can eavesdrop anytime to get information about customer's activity.

Smart grid is getting more modern every day, and new components of SG, like smart meters are helping customers and electricity companies to keep track of power usage and requirements for the future. Nowadays, customer can see his/her electricity consumption by just login into the web page, and this information is also used by electricity providers to predict the future usage of electricity for a particular user or group. Everything sounds good as this approach is customer friendly but unfortunately it also threaten the customer's privacy. Assuming that data is sent from smart meters, which is installed at user home by utility company using secure channel, but still companies are getting personal data for the customers. Using this data, it is possible to track down the user's activities. For example, if on a particular day power usage is low in a time slot as compare to normal days, then we can infer that the user is not at home. As a result, if attacker can get access to this information, then robbery can be possible in home. Another example of compromising customer privacy is when energy companies might be interested in collecting the user's data to infer habits and type of appliances used. Later, this information can be used for advertisement purposes without the knowledge of customers. To save the personal identifiable information about individual customers, lot of work has been done. In [26], the author proposed a solution which hides the customer information individually and gives access of aggregated data to electricity supplier. Each smart meter encrypts its electricity consumption value and sends to the electricity company. Once the company collects information from smart meters, it aggregate individual values to derive the unique

value which represents the encryption key of aggregated value. In this method, electricity company received value of group meters for example, value of energy consumption of one building. Using this mechanism, company can predict energy consumption without looking into individual value of customers. In [25], author a proposed method for privacy by anonymizing the meter data. In this method each smart meter is associated with two types of IDs, i.e High Frequency data transmission [HFID] and Low Frequency data transmission [LFID]. A third party, known as escrow, knows the link between two IDs and also has public/private for these IDs. The objective here is to send data from each smart meter in two steps. First step, send LFID and its associated public key to utility directly which helps to pass the gateway. In the second stop, HFID and its public key is sent to escrow and it forwards to control center.

In general, privacy in SG is concerned with the security of data which is related to individual's life. This type of attack usually occurs at Application layer as attacker is interested in getting access to customer information or device information to analyze running status. In this type of attack, malicious user has no interest in modifying the information transmitted over the power network. Attacker eavesdrop on the communication channels in the network to get customer information, for example account number, account balance, electricity consumption. Such attacks doesn't affect the working of the smart grid, but it can have an impact on customer personal life. It is the responsibility of electricity providers or smart meters manufactures to secure the customer data, but it can be possible that attacker is the customer who is interested in changing its meter reading which lowers it electricity bill. In recent years there have been lot of data breaches which made customer's privacy a sensitive discussion and more challenging. In Addition, complex working of SG makes it worse to deal with this type of attack. The consequences of confidentiality attack depend upon the amount of information getting extracted from the data. To analyze the data and get knowledge about the personal behavior of user, [27] has proposed method which is based on empirical probability distribution. In order to protect

the smart grid privacy, many solutions have been given, and one of them is data aggregation and encryption but this can also be reverse using NIALM (Nonintrusive Appliances Load Monitoring). This technology is used to detect changes in current and voltage going to the house and infer which appliances are used along with their energy consumption. In [28] authors propose a privacy preserve protocol which uses simple cryptography for the meter for billing and general calculations on the meter reading data .Addressing privacy issue in SG is critical. In order to improve the privacy level, joint efforts of electricity providers and customers are required. Research is going on this sensitive topic, but smart meter users will need to reassure that their data is secure.

## 3.3 Integrity

In data integrity attack, adversary aims to deliberately alter, insert, or delete sensor data or control signals in the network so as to mislead the smart grid to take wrong decisions. However, for the attack to be successful, malicious data should be within acceptable range of inputs. Hence, attacker requires knowledge of system functionality and networking for the attack to be effective. One common example of this type of attack is when customer try to tamper a smart meter to reduce its electricity bill. Another example is that when compromised RTU gets signal from fault circuit indicator (FCI) but it refuses to pass this signal to control center which results in increasing the fault time. In SG, integrity of metering data and commands is important, but in most of the cases result of their data shows revenue loss. While attack on any software can be bigger threat as compromised software or malware can control other devices in the network. The originality of the data depends upon whether data is collected or generated [29]. If the data is collected data than it is application oriented, and its data integrity can be checked using semantic check, source of the data is authentic user or sensor device, and certificates from trusted authorities in communication. In case of generated data, its originality depends upon the process and input to the process while input depends upon the input device. If a

malicious user able to pass the data integrity check then he/she can successfully launch the spoofing attack. A spoofing attack is when compromised IED impersonates another device in a network to launch attacks against other devices or sensors or just to bypass the access control. For example, switches in SG are capable of disconnecting the substation from the transmission grid once they received signal from the IED. If the attacker masquerades successfully as sensor IED, it can send open/close message to switches, resulting in loss of power for customers. This type of attack can be ceased by implementing strong point to point authentication. Data integrity can also be compromised, if there is adversary attack on the communication between power devices in local area network and control center. In the context of this scenario, a prime example is man in the middle attack (MIM) where adversary relays or alters the message secretly between two devices who believes they are directly communicating with each other. MIM attack exploits a weak end to end authentication in the communication which allow adversary to act as legitimate user. A successful implementation of attack helps to gain access of RTU which makes it possible for adversary to replace original data packets with malicious packets and impersonate as a valid data source. MIM attack can have severe consequences on the SG. For example, once getting control on sensor devices adversary can send forged data packets to control center appear to be normal while grid operating in stress condition.

### 3.3.1 False Data Injection (FDI)

In false data injection attack, an attacker injects malicious inputs in the sensors reading which is used for state estimation of SG using self-constructed attack vectors to bypass the bad measurement detection algorithm. This attack was first introduced in [7] where researchers exposed vulnerability of existing bad measurement detection algorithm by introducing new class of attack against state estimation in smart grid. FDI was executed under the assumption that attackers have access to configuration information and can manipulate measurements of meters installed at physically safe place. A successful FDI

attack can cause state estimators to generate wrong values of state estimation. Since some applications in power grid depends upon the output of state estimators, wrong values can mislead the operations of these applications which can effect overall working of SG.

System monitoring is the basic principle of SG to ensure the optimum performance without any disturbance. It collects data about operations using sensors installed at physically safe places such as substations, which helps in predicting condition of power grid. The meter measurement includes bus voltages, bus real and reactive power injections,and branch reactive power flows in every substation of power grid [7]. These measurements are typically stored in SCADA and sent to control center for analysis which helps to infer state estimation. State estimation refers to process of estimating unknown state variables in operations to infer the operational state of power system. It uses power flow models which are sets of equations used for numerical analysis to calculate power flow in each transmission line. There are two types of models Alternating Current (AC) model and Direct current (DC) model. AC model is more accurate but sometimes it is not feasible to do calculations using this model due to its nonlinear nature, in that case DC model is used. Once state estimation process is completed, data is being analyzed in control center to check if SG is working in normal or divergent state. If there is sign of any abnormal issues then required steps are taken to return it to normal state.

In FDI, attacker's interest is to inject malicious input by any means. For example attacker may get access to substation using physical attack or comprise smart meter in the network. Even there is a possibility that attacker may hack into the computer of control center which stored data from various sensors. In order to avoid any danger to power operations, bad measurement detection algorithm was introduced. It aims to detect, identify and eliminate measurement errors throughout the system. However, this algorithm have loopholes which allow attackers to bypass malicious data detection. According to the research in [7], if attacker knows current configuration of the power system then it is easy for attacker to bypass safeguards for bad measurement as all of DC power models

suffer from same vulnerability. However, later it was proven that it is possible to launch attack with incomplete information where attacker can collect information from different sources. For example utilizing company employee for information, using market data to deduce information, and using power flow measurements. FDI can be of following types:

- Load Distribution (LR) :- It is special type of false data injection studied in [30] where attack is executed on load bus injection measurements and line power flow measurements. As this attack bypasses the bad data detection algorithm, outcome of state estimate calculation is incorrect which further influences the output of security constrained economic dispatch (SCED). The goal of SCED is to minimize the operation cost while meeting the system load. The fallacious SCED report may lead the system to an uneconomical operating state which can have devastating impact like immediate load shedding. Based on the adversary intentions of attacking it can be immediate attack or delayed attack. In immediate attack, attacker goal is to maximize the operation cost immediately after successful attack. While in delayed attack, operation cost is maximize after the outage of overloaded lines.

- Energy Deceiving Attack:- This attack proposed in [31] where authors studied the energy distribution routing scheme and introduce false data injection for the scheme. In this attack type, authors consider general attacks like manipulating quantity of energy supply, quantity of energy demand, and link state of energy transmission to execute false data injection attack. Once FDI is injected successfully, it cause load imbalance in power demand and supply. In addition, energy distribution cost increases and distribution supply gets disturbed. In energy routing scheme, which is used for distributing energy to customers, each node represents energy demander or supplier. If the node consumes more energy than it generates, node is called energy demand node. If the node consumes less energy than it generates, node is called energy supplier node. Here node represents the users of energy. The

measuring components in the grid determine whether it is consumer or supplier. In the routing scheme, malicious user is capable of injecting forge energy information or link state information which allow attacker to generate erroneous values of energy demand and supply. This can lead to disparity in the power grid which disrupt the effectiveness of the energy distribution.

# Chapter 4: NS3 MODEL AND ANALYSIS

## 4.1 About NS3

NS3 is discrete event network simulator built for research and education purposes to learn or perform experiments in network protocols and communication methods. However, the objective of NS3 has been changed by research community according to their requirement of performing experiments in different fields. For example NS3 is becoming a prominent member in the power industry due to its ability to collaborate with power world simulators like GridLAB-D. NS3 is open source, extensible network simulation platform and provides various number of in-built models to analyze data packets in the network works. One of the fundamental goals of building this network simulator is to provide realism in research experiments i.e. to make models which are close to actual software implementation. NS3 chose C++ as the programming to build models as it helps to achieve realism with high level of abstraction which makes an impact on the results of simulation in a positive way. In addition, reuse of models is also one of the benefits using this simulator. Using C++ as programming language, debugging and integration with other models which are built using different language becomes an easy task. Python based API allow ns3 to integrate with another model. NS3 was built to prioritize the use of single programming language, but now it has capabilities of python bindings.

NS3 contains network elements which help to build the computer network. A node element represents end systems in the network such as computers, hubs, switches, and routers. Another element is network devices which represent physical devices like network interface used to connect nodes with the communication channel. A third element is communication channel which is a medium to send data between network devices. It uses two types of media: cable and broadcast, while cable can be fiber-optic and broadcast can be done using wireless communication. The next element is communications protocols

which is used to implement standard protocols or experiment protocols which are under construction. One more element is protocol headers which are the subsets of data found in data packet, and every protocol has different layout for it. The last element is network packets which is the fundamental unit of data in network. Every packet contains one or more header which describe the information required for protocol implementation, and it also contains payload which is the actual data needed to be exchanged between end systems. In order to construct any simulation model in ns3, user builds a C++ main program using network elements and describes the functioning for which network is built. The next step is to compile the program which connects simulation program with libraries of in-built models that come with ns3 when we installed. To write simulation program in ns3, we need to follow few steps. First step is to create the network topology which can be done by instantiating the objects of network elements like nodes, channels, devices, and network channel. The second step is to create models of network applications which send and receive the packet. The third step is to execute the simulation program which repeats itself until either event list becomes empty or preset execution time is reached. The last step is to analyze the results from the trace file. Using the trace file we can compute average link utilization on the communication channel, drop rate, source and destination of packet and many more. We can set the format of trace file, for example: pcap file which can be analyzed using wireshark tool.

Most of the available simulators written in C++ had memory leakage problem which reduce the efficiency of simulation, but this issue has been handled by the authors of ns3. Memory leakage occur when new memory is located dynamically and it never deallocates. In C++ program, new memory is allocated using new operator and deallocated using delete operator. The main issue with memory leaks is, they keep accumulating and if left unchecked can abort or crash the program. NS3 uses smart pointers to deal with memory leak, which don't require program to call "new" and "delete" functions directly. Rather simulation models can call a "create" method which allocates the requested memory

and increment "reference count" value associated with allocated memory. When the reference count value decrements to zero, all the allocated memory is destroyed and the underlying memory returns with the delete operator. Using this approach handling of dynamic memory becomes easy in ns3. Another fundamental requirement for any network simulator is presentation of packet. NS3 network packet contains headers and payload. It is designed in a way that it supports any number of protocol header of any size, fragmentation and reassembly by network. The object aggregation in ns3 can be solved using Microsoft component object model (COM). In COM object, access of object data is achieved by one or more related functions. As NS3 is discrete event simulator, it maintains a list of future events based on event timestamp in ascending order. It keeps on updating the list time to time and calls the event handler for appropriate event. In NS3, event handler can be any static or public function for an object. It doesn't define new subclass for each event type rather required information is passed as an argument to function which creates and schedules new events.

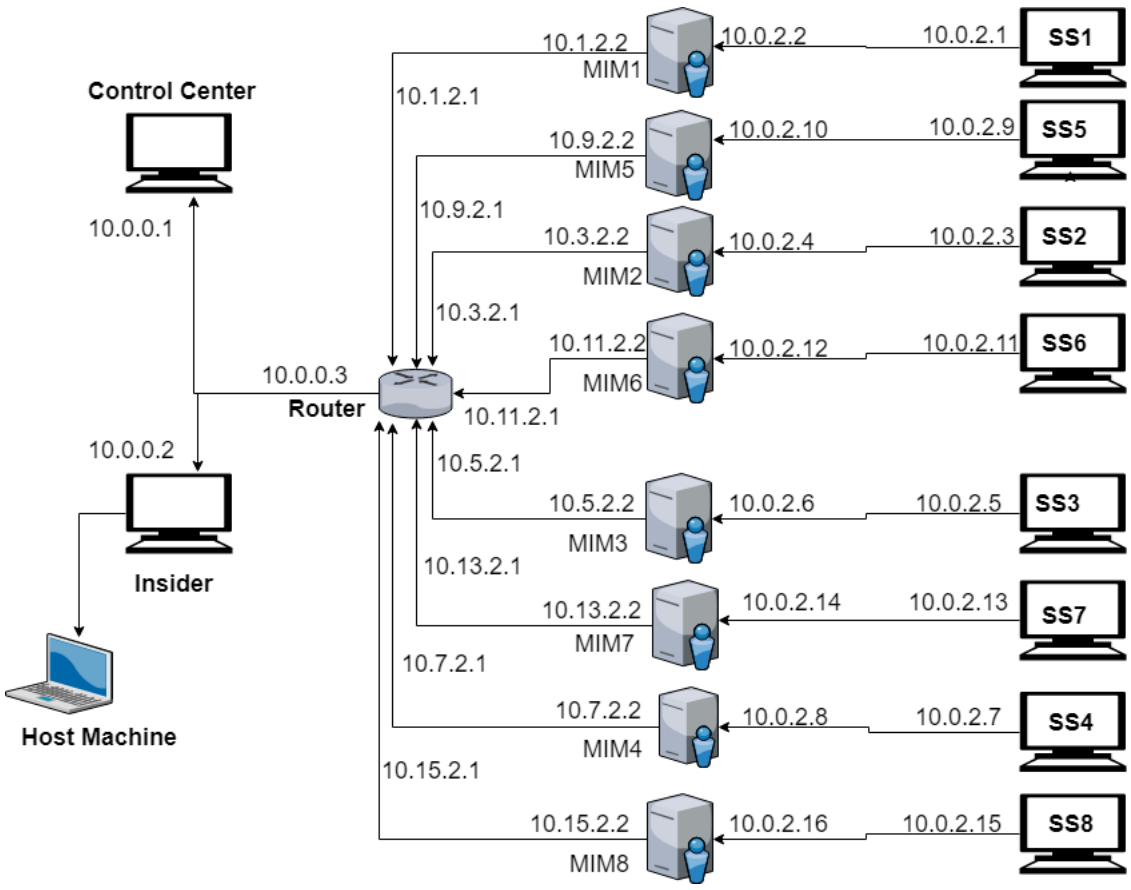
To perform research experiments with larger network, ns3 provides capabilities of distributed simulation. In bigger network, it is challenging for single instance of simulation to handle all events, so it is recommended to use distributed simulation approach which runs simulation on multiple platforms. This helps to increase the efficiency and overall scalability. In distributed simulation, each simulator is responsible for the subset it belongs to and for remaining subset in the network topology ghost node is created. Ghost node is use to link with other subnets and no protocol stacks or application is created for ghost node. In the past decade, a lot of research has been done in improving SG communication and still it never ending process. Researchers from all around the world created testbeds and virtualization environment to provide realism in experiments, but still simulation is one of the favorable option for research. Taking realism into consideration, NS3 is competent simulator to provide features of emulation, virtualization, hardware in the loop, and running of real implementation code. All these features help to provide stability to

experiments, and even few techniques can be combined together to get better productivity of experiments. After successful experiments, analysis of data comes into action. NS3 provides tracing subsystem to capture data during simulation. It exports simulation data from trace source to trace sink. Here trace source and trace sink denoted data generation and data consumption. NS3 provides ability for users to write their own trace sink, and get the desire output. The in-built models in NS3 already define various trace sources, for example: you can change the variable value in the congestion control. However, there is always option to trace selected behavior by attaching your own sink with the model. After exploring various network simulators, NS3 is best suitable option in the current scenario of research due to its features and compatibility with power simulators.

## 4.2 Model

NS3 model provides the basis for analysis of attacks that can be possible within the control center or in Advanced Metering Infrastructure when attacker is insider. Insider can be legitimate employee or authorized user who is having access to system resources to perform actions which is difficult to detect and prevent. Insider have knowledge of network architecture, system policies, and defense mechanism which help them to bypass the security. The accessibility to smart grid components increases the possibility to launch power attack which is difficult to track down as compared to outside attacker. In our model, insider is represented by node whose one side is connected with router node using CSMA link and other side is attached to host machine i.e. Ubuntu operating system, to launch various types of attacks. Model contains total of 15 nodes where each node interface is assigned IP address. The network diagram for the model is shown below in Figure 4.1, and Figure 4.2 exhibit simulation diagram.

Figure 4.1: NS3 model Network diagram




### 4.2.1 Elements of Model

1. Control Center (CC):- The CC node is the first node in network which is used to send seocon poll request to substation node. This node is connected to the router node using CSMA link. To send request, DNP3 master application is installed on the CC node. There are eight DNP3 master applications installed on CC to interact with its corresponding DNP3 slave application installed on substation node. The attributes of DNP3 application like master device address, station device address, jitter minimum and maximum value etc. are set using helper class.

2. Insider: - This Node is responsible for all types of attacks within control center or to the substation. It uses CSMA interface to connect with the router node. Insider

node is connected with the host machine, in this case Ubuntu operating system, using Tap Bridge model of NS3. The Tap Bridge model is designed to integrate real host into ns3 simulation environment. The goal of this model is to make it appear ns3 device as a local device to real host node. Tools like nmap can be installed on the host machine for information gathering about substation node. It can also be used for powerful attacks like DOS, false data injection etc.

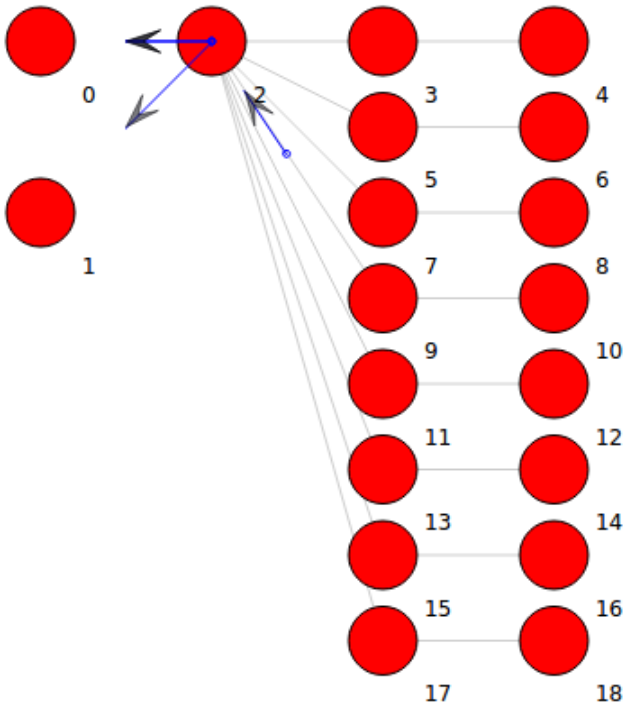
3. Router: - Router node is use to connect control center with the advanced metering infrastructure. The CC, Insider, and Router nodes are connected with CSMA while router is connected via P2P link to all of the MIM nodes. The CC and Insider route everything through this node and substation node which sends meter data to control center also route using this node. There is no application installed on this node so the main goal is to route data between nodes. This node is assigned multiple IP addresses for each interface.

4. Man in the model (MIM): - This node represents the man in the middle attack. It can be used for just tapping the network and can be used for various scenarios. For example: MIM can act as substation node, and it can be done by installing DNP3 slave application on this node. Similarly, MIM can also be spoof as control center, and it can be implemented in the model by installing DNP3 master application on the MIM node and setting the attributes according to the scenario.

5. Substation (SS):- SS Node is use to send sensor data like power reading, breaker settings to the control center (CC) node. In total, there are eight SS nodes and each node is connected with same numbered MIM node via P2P link. Each node contains DNP3 slave applications installed on it, corresponding to the master application which is installed on CC node. The seocon poll request-reply mechanism occur between same numbered master-slave DNP3 applications. SS node is always under risk to be attacked by insider. In order to protect it, each branch connecting with

MIM node is replicated. It provides extra defense layer to the model.

Figure 4.2: Simulated Network




## 4.3 Analysis of Attack

The Analysis of attack discussed in table 4.1 is done based upon the targets under category of availability, confidentiality and integrity. We consider limited targets for each category by taking the NS3 model into consideration. There is possibility of more targets which need to be analyze but that may be out of the scope of simulation model. Before analyzing there is need to define impact levels, and in our case definition is based upon NISTIR 7628 guide. These impact levels can be used for the selection of security requirements for each categories.

In terms of availability, if the impact is low then disruption to access or use information is expected to have limited adverse effect on organization operation, assets, and

individuals. Whereas if impact is moderate then effect is expected to be serious and in case of high impact, effect can be severe or catastrophic.

In terms of confidentiality, if the impact is low then unauthorized disclosure of information is expected to have limited adverse effect on organization operation, assets, and individuals. Whereas if impact is moderate then effect is expected to be serious and in case of high impact, effect can be severe or catastrophic.

In terms of integrity, if the impact is low then unauthorized modification or destruction of information is expected to have limited adverse effect on organization operation, assets, and individuals. Whereas if impact is moderate then effect is expected to be serious and in case of high impact, effect can be severe or catastrophic.

Table 4.1: Anaysis of Attack

| Category | Threats | Target | Impact on AMI | Impact on Control Center | Impact on Customers |
|---|---|---|---|---|---|
| Availability | DOS | Control Data | High | Moderate | Low |
| | | Sensor Data | High | Low | Low |
| | | Billing Data | Low | Low | Moderate |
| Confidentiality | Privacy | Customer Data | Moderate | Moderate | High |
| | | Management Data | High | High | High |
| | | Network Data | Low | Low | High |
| Integrity | False Data Injection | Electricity Pricing | Low | Moderate | High |
| | | State Estimation | High | High | High |
| | | Load Distribution | High | High | Moderate |

### 4.3.1 Targets

- Control Data :- SG sometimes remotely correct the problem by sending commands to equipments which are connected to control center to adjust the conditions, but DOS attack can delay or stop these commands. There is a high Impact on AMI as it's unable to send relevant information to CC. Some devices in AMI need commands from control center to perform certain actions like ON/OFF or to upgrade itself, but if DOS attack occur then these devices are unable to execute expected commands. It can affect the network performance which can result in voltage instability in the network. Even in worst situation blackout can be possible. Interaction with the electricity market is also cut off which affects the users electricity usage. Impact on CC will be moderate or low as commands are lost in the communication and not able to reach the desired component of the SG. Impact on customers will be low as they aren't able to see real time pricing, but the availability of power is more important for customer.

- Sensor Data:- In SG, lot of sensors or monitoring devices like PMU has been installed in order to send data to control center which helps operators to monitor power condition in real time. For example, protection system at substations can record disturbance events and send it to control center to analyze more about fault. As sensor data is time sensitive, even small delay can lead to accident in SG. If DOS attack launched by attacker, sensor data isn't able to reach the control center which can affect the real time monitoring. It can have high impact on AMI as even one fault can disturb the communication, while impact on CC will be low as it only increase the waiting period for data. Similarly, impact on customers will also be low as sensor data doesn't affect the life of customers directly.

- Billing Data:- The impact of billing data, in case of DOS attack, on AMI and Control Center will be low as it doesn't influence the working of both. However,

the impact on customers will be moderate as they aren't able to see their billing for short amount of time. Unavailability of billing data can stop them from using the required appliances, or there are chances that power usage by customers increases rapidly which can affect energy estimation for the area.

- Customer Data:- Nowadays, power companies are getting data in every few minutes from smart meters installed in customers houses. It enhance the capability of monitoring, controlling and predicting power usage for the particular area. However, this data is exploiting the customer's privacy. The analysis of this data can reveal customer's habits and behavior, even it can divulge which appliances are used in the house in a particular time period. If the privacy of this data is not maintained then it can have bad impact on customer's life, for example: analysis of data can disclose when customer is not at home which can result in robbery. Hence, if privacy is not maintained, impact on customers will be high whereas impact on CC and AMI will be moderate as monitoring and controlling also depends upon this data.

- Management Data:- The monitoring and analysis of operational data provides useful information which helps to improve SG operations, efficiency, security, and reduce cost. This kind of information is suitable for adversary if confidentiality is not maintained. It can be accessed using HMI or data historian client. Managing changes in SG is challenging as small change in architecture or working can lead to failure of components. Management data includes market policies which should be transparent and provide liberty for customers to choose from different plans. Now a days selling power is challenging for business. Companies and stakeholders are adopting new marketing strategies to know behavior of rivals and costumers. If the data breach occurs, it will have high impact on AMI, Control Center and customers as adversary can find vulnerability in the functioning of SG.

- Network Data:- In this type of attack, attacker eavesdrop on communication chan-

nels in SG network to steal desired information which can be further useful in detecting loopholes in the network. It can be done with wiretapping or network analyzer. Attacks targeting confidentiality don't have any intentions in modifying data. However, privacy of customers like account number, electricity usage per day etc. can be stolen and sold on dark web, which can have high impact on customers. Confidentiality attack doesn't affect the functioning of power grid, so impact on AMI and CC will be low.

- Electricity Pricing :- In this type of data attack, main goal is financial misconduct. The adversary manipulates the smart meter data, transmitting to control center for future power estimation and real time pricing. Local Marginal Prices (LMP) are commonly used for predicting power and real time pricing by the power companies. An attacker can affect the real time pricing by manipulating the quantity of electricity usage in meter reading or injecting malicious data in the meter reading which affect the LMP calculations. In SG, monitoring and control data is sent to control center where Energy Management System (EMS) role is to detect bad data. If attacker bypass the EMS then successful attack can create imbalance in working of SG. This attack is having high impact on customers as it is directly related to smart meter reading. However, the impact of control center will be moderate as it can be challenging for security of EMS and which can result in incorrect power estimation. The impact on AMI will be low if it is bypassing only single smart meter.

- State Estimation :- State Estimation is calculated using meter measurement data which includes bus voltages, branch reactive power flow in subsystem etc. transmitted to control center, where it is stored in SCADA system. Using this collected data and power models, state of the power grid is calculated to check whether everything is working fine. It is the process of estimating state variables in a power based on

meter reading collected using sensors installed in AMI. If attacker can determine current power system configuration then he/she can inject malicious data in the meter reading which can bypass the bad data measurement algorithm. This can lead to incorrect state estimation in the power grid. If the attacker is successful in this type of attack then the impact of AMI, control center and customers are high as smart meters are comprised, detection techniques are bypassed and everything can lead to blackout in worst situation.

- Load Redistribution :- It is special type of False Data Injection attack which bypasses bad data detection techniques used in the control center. Load Redistribution means increasing load on some buses and reducing load on other buses, but the total load is unchanged. If the load measurement and power flow measurements for transmission line are attackable then load redistribution attack is feasible. If attack is successful then it can harm the power system in two ways. First, it can lead the system to load shedding stage, i.e. distributing the power supply across multiple supply source to reduce stress on the primary source. Second, it can lead power system to uncertain stage where power flow in transmission line is exceeds its capacity. The impact on CC and AMI will be high as power operations are not running as expected which may lead to physical damage in the power lines. While impact on customer will be moderate as power will not disappear soon.

## 4.4 Experimental Proof of Concept and Results

- Denial of Service (DOS) Attack :- Using our NS3 model we have implemented denial of service (DOS) attack, and result is shown in figure 4.2. The figure represents an output of pcap file which is generated when insider launch the DOS attack to first substation node (SS1). In the model, DNP3 master applications installed on control center (CC) node request for meter data from every substation node (SS) where DNP3 slave applications are installed. If the DOS attack occurs then there is delay

in the message transmitting from substation node. In figure 4.2, it is clearly shown that attack has been launched from insider node having IP 10.0.0.2 to the substation node with IP 10.0.2.1. DOS attack presented here floods the substation node with ICMP packets which results in delay of DNP3 response. In order to sucessfully implement the experiment we installed the tool hping3 on the host machine which is a useful tool to flood the network. The time differences between DNP3 messages with and without DOS attack have been shown in table 4.2, which clearly verify the differences in time stamps with each request number. Using the time stamps of both cases, the graph has been plotted which is shown in figure 4.3. The graph proves that with every request number, there is increase in time taken by DNP3 message to reach the control center node.

Figure 4.3: DOS attack implementation

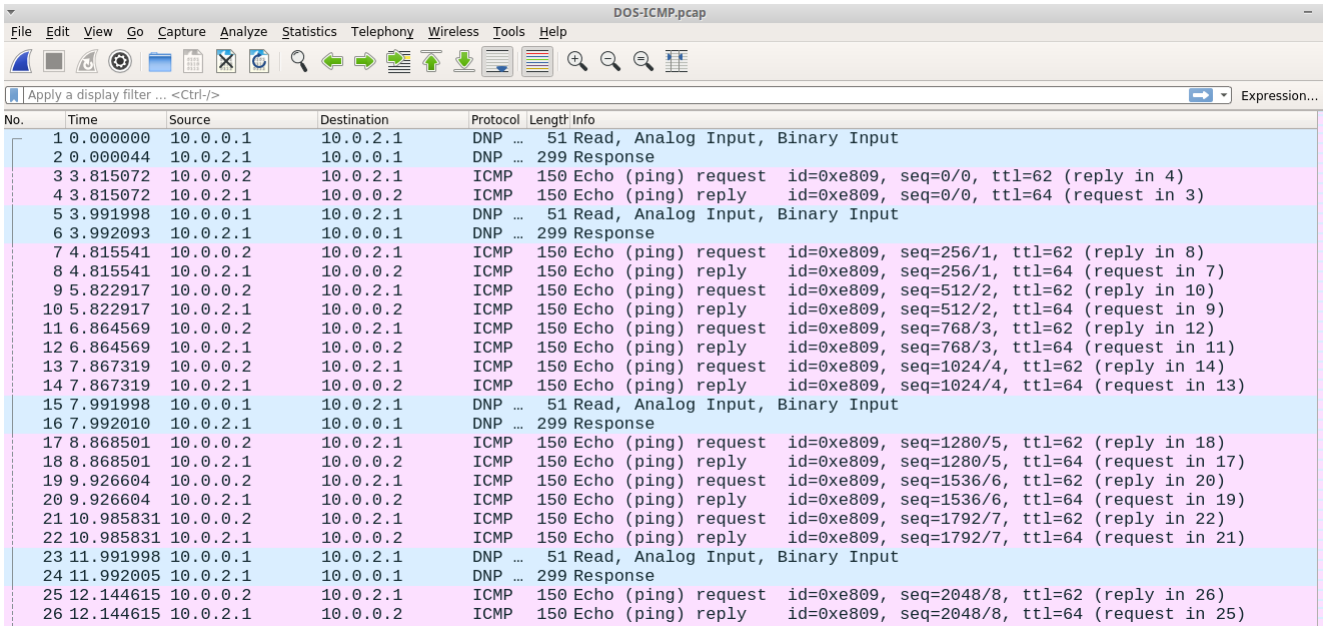


Table 4.2: Time Difference in DNP3 Messages

| **DNP3 MESSAGE** | | |
|---|---|---|
| Request Number | Time without DOS Attack | Time with DOS Attack |
| 1 | 0 | 1.390822 |
| 2 | 3.991998 | 5.38282 |
| 3 | 7.991998 | 9.38282 |
| 4 | 11.991998 | 13.38282 |
| 5 | 15.991998 | 17.38282 |
| 6 | 19.991998 | 21.38282 |
| 7 | 23.991998 | 25.38282 |
| 8 | 27.991998 | 29.38282 |
| 9 | 31.991998 | 33.38282 |
| 10 | 35.991998 | 37.38282 |

- Data Injection :- In the model, normal traffic between control center node and substation node is a request-response mechanism using DNP3 protocol. The figure 4.4 exhibit the normal traffic between control center and substation nodes. However, if attacker able to inject any type of malicious data in the network then it can affect the overall well-being of the network communication. In our case, attacker spoof the IP of control center and inject the random data inside the network with target as SS1 node. The SS1 node is not capable of processing mainly DNP3 data packets but as shown in figure 4.5, attacker sends different type of data using protocols like HTTP, TCP etc. It may results in delay of normal traffic or attacker can get control on first substation node. If adversary compromised any one of the substation node then the stability of entire network is under his control. The attacker can change the meter reading transmitting to control center node or other types of attacks can also be launched to get control on remaining substation nodes. This attack can be neutralized by isolating the first substation node as our NS3 model have capability of running network communication under normally condition using replicate node.

Figure 4.4: DOS attack

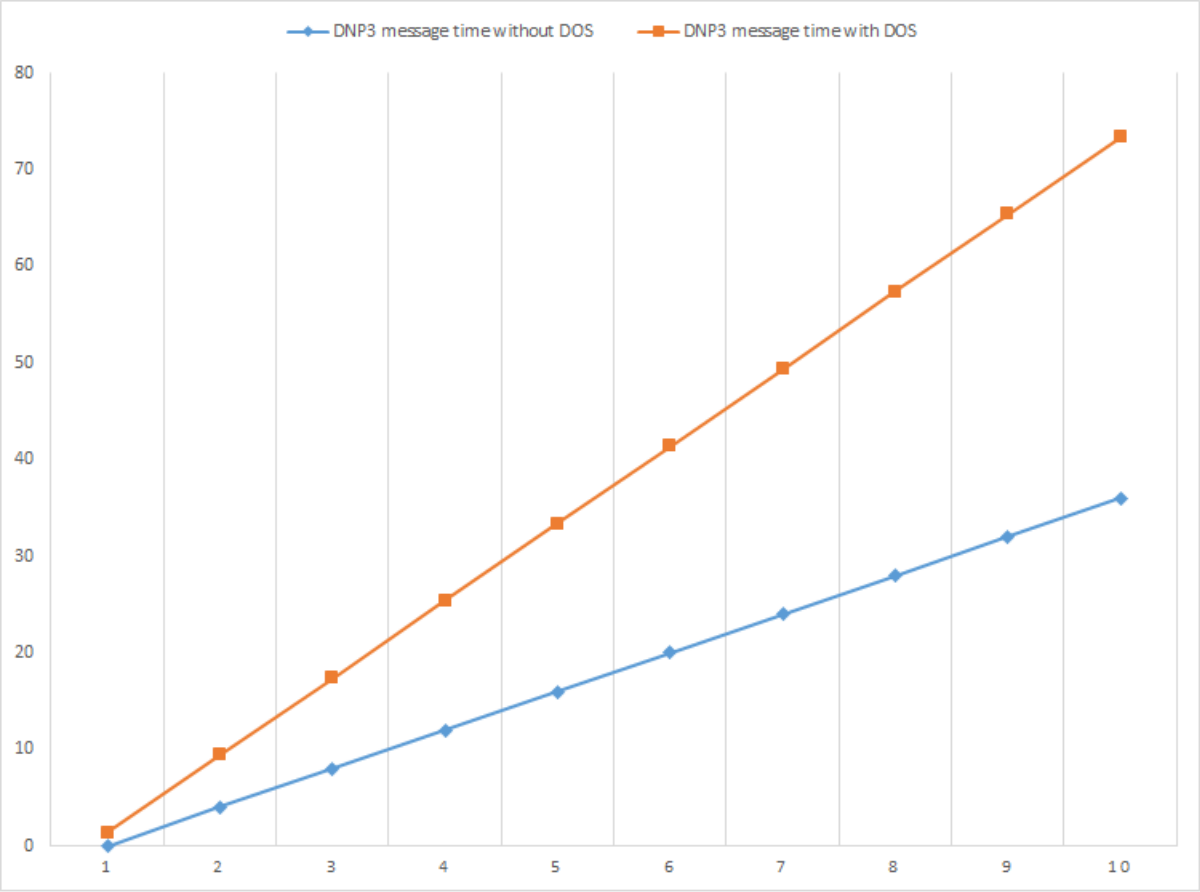


Figure 4.5: Normal Traffic

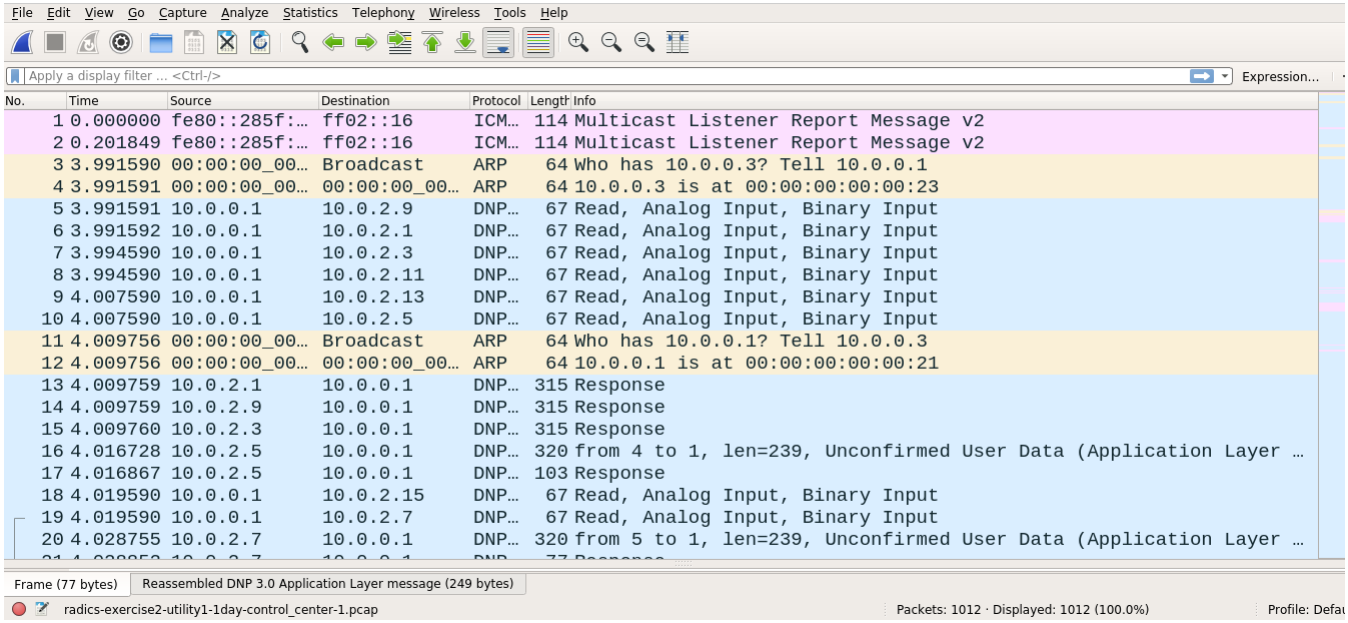
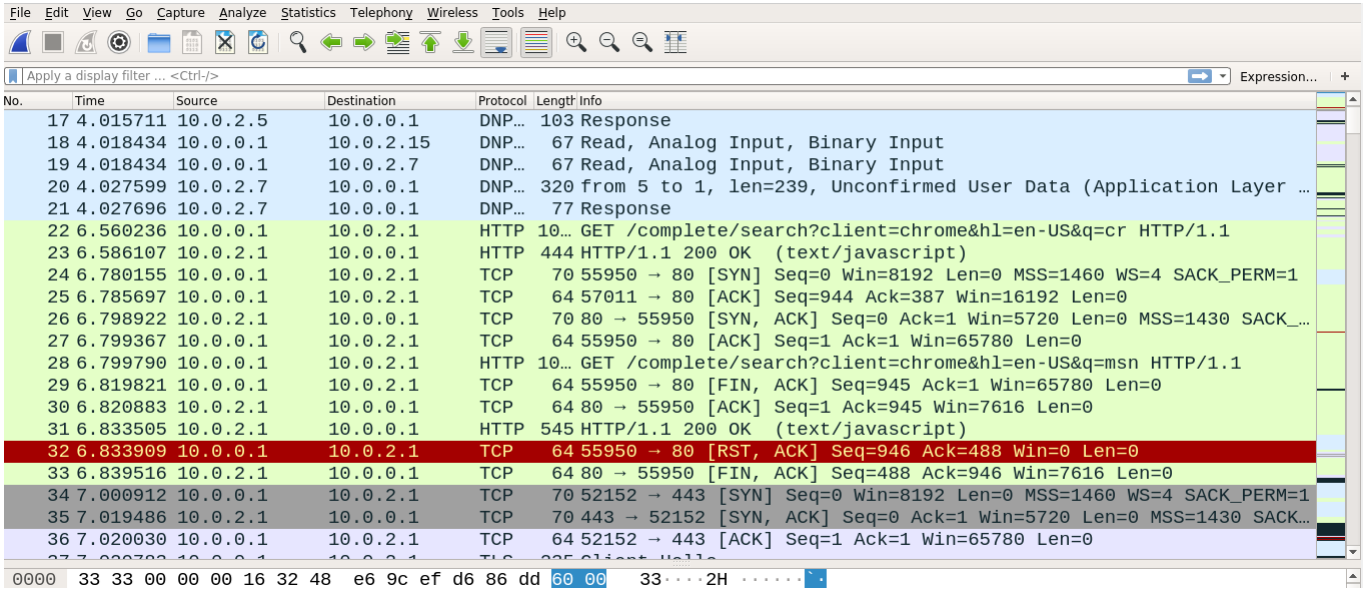



Figure 4.6: Data Injection Traffic



# Chapter 5: Conclusion

In this research, we analyze smart grid threats and their impact on control center, Advanced Metering Infrastructure and customers. Cyber security of smart grid is challenging because of heterogeneity and complexity of components connected in communication network where vulnerability in any component has immediate impact on the reliability of power infrastructure. Due to demand of continuous availability in power systems, testing is practically infeasible and out of budget in SG. The need arises for simulation model which is helpful in defining new architectures and testing threats by setting parameters according to required scenarios.The three main objectives: availability, integrity and confidentiality of cyber security are important for smart grid also. We define various threats under these categories which are important to smart grid and can be implemented to NS3 model. Along with securing the communication network, physical security of components like substation and smart meters at home are equally important. Since the research in cyber security is continuous process, our objective is to analyze some of these threats using simulation model. NS3 model presented here contain 19 nodes, out of these nodes DNP3 master applications are installed on control center node, and their corresponding DNP3 slave applications are installed on substation nodes. These substation nodes transmits meter data to the control center. This process can be traced and analyzed using pcap files.

# Bibliography

[1] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid – The new and improved power grid: A survey," *IEEE communications surveys & tutorials*, vol. 14, no. 4, pp. 944–980, 2012.

[2] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "Smart grid technologies: Communication technologies and standards," *IEEE transactions on Industrial informatics*, vol. 7, no. 4, pp. 529–539, 2011.

[3] B. E. Bilgin and V. C. Gungor, "Performance evaluations of ZigBee in different smart grid environments," *Computer Networks*, vol. 56, no. 8, pp. 2196–2205, 2012.

[4] S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy theft in the advanced metering infrastructure," in *International Workshop on Critical Information Infrastructures Security*. Springer, 2009, pp. 176–187.

[5] P. Zhang, F. Li, and N. Bhatt, "Next-generation monitoring, analysis, and control for the future smart control center," *IEEE Transactions on Smart Grid*, vol. 1, no. 2, pp. 186–192, 2010.

[6] F. Li, W. Qiao, H. Sun, H. Wan, J. Wang, Y. Xia, Z. Xu, and P. Zhang, "Smart transmission grid: Vision and framework," *IEEE transactions on Smart Grid*, vol. 1, no. 2, pp. 168–177, 2010.

[7] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[8] T. Skeie, S. Johannessen, and C. Brunner, "Ethernet in substation automation," *IEEE Control Systems*, vol. 22, no. 3, pp. 43–51, 2002.

[9] H. Zeynal, M. Eidiani, and D. Yazdanpanah, "Intelligent substation automation systems for robust operation of smart grids," in *Innovative Smart Grid Technologies-Asia (ISGT Asia), 2014 IEEE*. IEEE, 2014, pp. 786–790.

[10] C. Greer, D. A. Wollman, D. E. Prochaska, P. A. Boynton, J. A. Mazer, C. T. Nguyen, G. J. FitzPatrick, T. L. Nelson, G. H. Koepke, and A. R. Hefner Jr, "NIST framework and roadmap for smart grid interoperability standards, release 3.0," Tech. Rep., 2014.

[11] E. A. Lee, "Cyber physical systems: Design challenges," in *11th IEEE Symposium on Object Oriented Real-Time Distributed Computing (ISORC)*. IEEE, 2008, pp. 363–369.

[12] Y. Zhang, M. Qiu, C.-W. Tsai, M. M. Hassan, and A. Alamri, "Health-CPS: Healthcare cyber-physical system assisted by cloud and big data," *IEEE Systems Journal*, vol. 11, no. 1, pp. 88–95, 2017.

[13] C. Ptolemaeus, *System design, modeling, and simulation: using Ptolemy II*. Ptolemy. org Berkeley, 2014, vol. 1.

[14] P. Derler, E. A. Lee, and A. S. Vincentelli, "Modeling cyber – physical systems," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 13–28, 2012.

[15] K. Mets, J. A. Ojea, and C. Develder, "Combining power and communication network simulation for cost-effective smart grid analysis," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1771–1796, 2014.

[16] K. Hopkinson, X. Wang, R. Giovanini, J. Thorp, K. Birman, and D. Coury, "EPOCHS: a platform for agent-based electric power and communication simulation built from commercial off-the-shelf components," *IEEE Transactions on Power Systems*, vol. 21, no. 2, pp. 548–558, 2006.

[17] J. Nutaro, P. T. Kuruganti, L. Miller, S. Mullen, and M. Shankar, "Integrated hybrid-simulation of electric power and communications systems," in *IEEE Power Engineering Society General Meeting*, 2007, pp. 1–8.

[18] H. Lin, S. Sambamoorthy, S. Shukla, J. Thorp, and L. Mili, "Power system and communication network co-simulation for smart grid applications," *Innovative Smart Grid Technologies (ISGT)*, pp. 1–6, 2011.

[19] D. Bian, M. Kuzlu, M. Pipattanasomporn, S. Rahman, and Y. Wu, "Real-time co-simulation platform using OPAL-RT and OPNET for analyzing smart grid performance," in *Power & Energy Society General Meeting, 2015 IEEE.* IEEE, 2015, pp. 1–5.

[20] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *computer*, vol. 35, no. 10, pp. 54–62, 2002.

[21] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing.* ACM, 2005, pp. 46–57.

[22] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE network*, vol. 20, no. 3, pp. 41–47, 2006.

[23] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, 2009.

[24] P. Baronti, P. Pillai, V. W. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards," *Computer communications*, vol. 30, no. 7, pp. 1655–1695, 2007.

[25] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on.* IEEE, 2010, pp. 238–243.

[26] F. G. Marmol, C. Sorge, O. Ugus, and G. M. PÃ©rez, "Do not snoop my habits: preserving privacy in the smart grid," *IEEE Communications Magazine*, vol. 50, no. 5, 2012.

[27] G. Kalogridis and S. Z. Denic, "Data mining and privacy of personal behaviour types in smart grid," in *Data Mining Workshops (ICDMW), 2011 IEEE 11th International Conference on.* IEEE, 2011, pp. 636–642.

[28] A. Rial and G. Danezis, "Privacy-preserving smart metering," in *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society.* ACM, 2011, pp. 49–60.

[29] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communications Surveys and tutorials*, vol. 14, no. 4, pp. 998–1010, 2012.

[30] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382–390, 2011.

[31] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao, "On false data injection attacks against distributed energy routing in smart grid," in *Proceedings of the 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems.* IEEE Computer Society, 2012, pp. 183–192.