8-2021

# The Cyber Security Evaluation of a Wireless and Wired Smart Electric Meter

Patrick Nnaji
*The University of Texas Rio Grande Valley*

# THE CYBER SECURITY EVALUATION OF A WIRELESS AND WIRED SMART ELECTRIC METER

A Thesis

by

PATRICK NNAJI

Submitted to the Graduate College of
The University of Texas Rio Grande Valley
In partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE IN ENGINEERING

August 2021

Major Subject: Electrical Engineering

# THE CYBER SECURITY EVALUATION OF A WIRELESS AND WIRED SMART ELECTRIC METER

A Thesis
by
PATRICK NNAJI

COMMITTEE MEMBERS

Dr. Sanjeev Kumar
Chair of Committee

Dr. Jun Peng
Committee Member

Dr. Mark Chu
Committee Member

August 2021

# ABSTRACT

Patrick Nnaji, The Cyber Security Evaluation of Wireless and Wired Smart Electric Meter. Master of Science in Engineering (MSE). August, 2021, 118 pp., 11 table, 82 figures, 55 references.

In this thesis, Experimental cyber security evaluation of Wireless Smart Electric Meter has been performed under cyber security attacks. The security integrity of data collection from EPM 6100 Power Quality Wireless Smart Electric Meter under a wireless cyber-attack was evaluated. After which the security integrity of data collection from the same Wireless Smart Electric Meter was evaluated under a different configuration. In this thesis we tested three different smart meters for their connectivity under different cybersecurity attacks. We compared the security integrity of the three different smart meters to measure their response under different cybersecurity attacks.

# DEDICATION

I thank the almighty God Jehovah for everything I have achieved in life. The completion of my master's studies would not have been possible without the love and support of my family. I would like to thank my girlfriend Precious Bisong for her encouragement and emotional support especially during the pandemic. I would also like thank my Christian brothers and sisters who gave me the spiritual and moral support I needed to cope with my new environment. I would like to dedicate my thesis to all well-meaning researchers who strive to make an impact in the scientific community. To my IT mentors Bro Shegun and Debo, I understand what you both have done for me, I will never forget.

# ACKNOWLEDGMENTS

I will always be grateful to Dr. Sanjeev Kumar, chair of my dissertation committee, for all his mentoring and advice. He encouraged me to complete this process through his infinite patience and guidance. My thanks go to my dissertation committee members: Dr. Mark Chu, and Dr. Jun Peng. I could not have done this research if not for the knowledge I acquired while attended their classes. I would also like to thank my colleagues at the UTRGV library who helped me locate supporting documents for my research. I would like to thank all my friends at Network Research Laboratory in UTRGV.

Work in this thesis is based upon the grant awarded to Dr. Sanjeev Kumar by the national Science Foundation (NSF) under Grant No. 0521585, Houston Endowment Chair in Science, Math and Technology Fellowship and Presidential Graduate Research Assistantship Scholarship.

TABLE OF CONTENTS

Page

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

# CHAPTER I

## INTRODUCTION

The dangers posed to life and properties whenever cyber-attacks are perpetrated provide a highly compelling explanation on why it is necessary to understand and know how to respond to cyber threats. A predominant cyber-attack is one which is targeted towards the Advanced Metering Infrastructure (AMI) which is intended to upset some of a nation's critical infrastructure. This makes it an attractive target to hackers regardless of their skill level. Meanwhile, it is important to know that another thing that makes AMI a potential target is that hacked smart grids can be used as a host for other attacks due to the number of devices involved and the fact that these devices can be used to carry out attacks and hide malicious data using multiple nodal points [1].

In research by Ponemon [2], it was revealed that the organizations which were responsible for the United States' critical and infrastructure facilities are ill-prepared in the event of a cyber-attack and this is not even exclusive to the U.S. alone as many more countries are just as vulnerable. This makes Smart meters primed for attacks by hackers [3]. These AMI network attacks usually come in form of Denial of Service (Overloading the system for it to shut down) or theft of power and these can be detected when there are unapproved web pages posted on data-collecting web servers, outbound data transmissions using obscure ports and protocols, heavily compressed files transmitted over AMI networks and anomalous data load between data

collectors and smart meters. In a survey carried out by McAfee in 2014 [4], it was reported that 80% of electric utilities have all, on a wide scale, faced a Denial of Service (DoS) attack on their communication networks and unauthorized network penetrations. This report further showed that if the rate stayed the same, at the end of the year, one in four people would have been victims of a cyber-attack or a cyber-threat. Also, approximately two-third of the respondents to this survey had found malware in their systems at one point or the other.

The mode and impact of a DoS attack and how data traffic can be disrupted on an AMI network are explained in [5]. A cyber-attack on smart meters, one that allows hackers to compromise data obtained from meter measurement is discussed in [6] and in [7], there is a simulation of a hypothetical scenario where a hacker hacks an AMI communication network and performs a DoS.

According to the Institute for Electric Efficiency smart meter deployment projection, figures showed that an estimate of 65 million smart meters would have been deployed in the U.S. by 2015 [9]. It should be noted that the cost of AMI is huge and any regular replacement with safer units is cost prohibitive. The value of this research is that the understanding gotten from it would aid utilities become more informed regarding AMI and its security issues.

### 1.1 Smart Grid

Smart grids are a network of transmission lines, substations, transformers, and power generators which allow a two-way flow of electricity from electric power plants to residential houses or industrial buildings. The Smart grid is a highly intricate cyber-physical system (CPS) which incorporates and harnesses several distributed systems like actuators, controllers, and sensors and is expected to grow more and more on a global scale as time progresses. “Smart” in

this context refers to digitalization of this system which allows it to self-detect, react and be proactive to any sudden or unexpected changes in the system.

Smart grids benefit both customers and utilities in a lot of ways and the biggest selling point of this technology is the fact that it offers internet-based communication. It is easier to know the amount of energy wasted when one knows the amount of energy which has been consumed and this in turn helps to guard against further wastages in energy. Smart grids help to transmit electricity more efficiently, restore electricity faster when there is power interruption, and reduce operation cost for utility companies which in turn reduce cost on the part of consumers. It also helps to reduce peak demand in order to drop down electricity rates and integrate customer-owner power generation systems which is better for security purposes [10].

Smart grid technology modernizes the old method of manually reading electrical systems. It comes with an option of remotely handling and monitoring usage predictions for both the customers and the utility companies. With smart grids, the performance of electric networks is more dependable, easier to be regulated and definitely more cost effective.

## 1.2 Advanced Metering Infrastructure

To develop a smart grid, the Advanced Metering Infrastructure (AMI) is a critical feature that cannot be overlooked. AMI is an integrated system of smart meters, communications networks and data management systems that allow a two-way communication between utilities and consumers. It is primarily used by meter manufacturers and utility companies. Additionally, AMI is also a system that allows for communication between a client and a service supplier, and a collection of data management systems that provide information to the entity providing the service. AMI was introduced to replace the Automatic Meter Reading which was basically used

to read data from the meter. However, the main distinction between an AMI and AMR is in the fact that AMI has two-way communication.

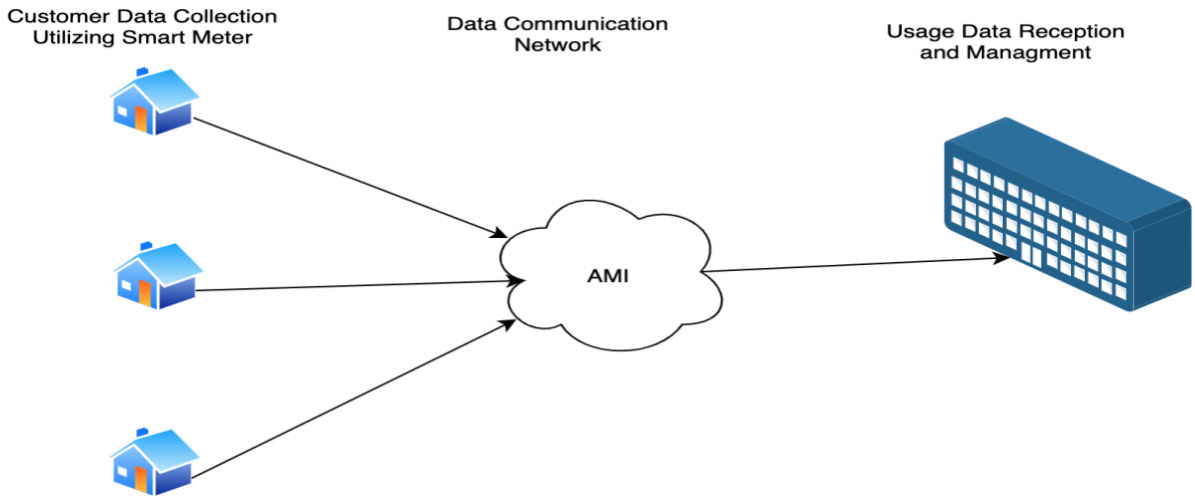


Figure 1.1: Advanced Metering Infrastructure.

The increased use of AMI is aided by the fact that it allows consumers remotely to read their meters and remotely control operations on their meters. AMI is the foundation for the digitalization of electric power grids, and it provides the architecture of two-way communication between smart meters and utility companies.

As is seen in the diagram above, the infrastructure of the AMI includes customer locations, access points, data communication networks (wireless or wired) between customers and utility companies and a data management system for the gathering, processing, analysis, and management of data. At intervals, smart meters send the information they have gathered to utility companies for the purpose of billing and monitoring of loads. An extra benefit of smart meters is that their readings allow the control center to come up with a Demand/Response mechanism. Therefore, customers can decide how much power they want to use, particularly managing their peak load. Generally, the AMI network includes thousands of smart meters, routers using

Ethernet cables or optical cables (in the case of wired systems), power line communications and wireless communications using WI-FI, Wireless Local Area Networks (WLANs), Radio Frequency (RF), which are all created to route data traffic from the customer to the utility [7] .

Two classes of AMIs are currently in use in modern technology – Wireless based AMIs and Wire line based AMIs. The kind of environment where the AMI is to be used determines the class of AMI which would be used. Because interference increases in densely populated areas, wireless AMIs are not very suitable in these kinds of environments which makes wire line based AMIs (using Ethernet cables) the go-to infrastructure. Ethernet based AMIs use switches and routers for data communication from smart meters at the consumer location to utility companies for billing and control. The AMI majorly incorporates the communication network, smart meters, and meter data management systems (MDMS).

The communication network consists of three key components which include Home Area Network (HAN), Wide Area Network (WAN) and the utility system. Smart meters are majorly on the part of the customer as they are installed in their locations. Then, they send the customers' electricity consumption information to the utility company which then uses this received information to determine how much the customer has to pay in electricity bills, enable demand response, predict user electricity consumption patterns and update pricing in real time.

### 1.3 Smart Electric Meter

This is an important component of smart grid technology, and its use has seen a meteoric rise in the last few years to the point that more than 50% of the U.S. population are now using it [11]. This is a milestone that would not have been met until 2019 based on pre-ARRA plans and proposals [9].

As are AMIs, smart electric meters can also be connected over wire lines or wirelessly. This helps the service providers remotely monitor the customer's power consumption. The smart meters installed at the customer's location can be used to remotely control smart appliances like smart lights, smart speakers, smart cameras, smart smoke detectors etc. This is done by interfacing those smart appliances to the smart meters. This system uses a technology called Internet of Things (IoT) for automatic meter reading and for remotely gathering data. This is essentially a modernization of the old data reading system which was done manually and that is how it got the name "Automatic metering infrastructure".

Critically, smart meters are essential to the electric power network which is being used significantly both for residential and industrial purposes. Smart meters when connected to an IoT network provide access to elaborate, real-time data which helps utilities provide better services while dropping down costs to consequently increase profit. With the use of smart meters, it is also more convenient to manage electric loads and reduce the occurrence of power outages although the downside to all this is that they are vulnerable to cyber-attacks which affect the reliability of all the data gathered about power usage.

### 1.4 Smart Meter Communication Technologies

Over the years, smart metering has attracted much attention because of its flexibility. Utility companies are shifting from mechanical meters to smart ones. With this shift comes the choice of communication technology. The communication technology adopted by a company mostly depends on the infrastructure already in place before a transition to smart metering. The choice of communication technology is carefully considered because it plays a role in the speed and

reliability of information relayed to the utility. In this section, we will briefly discuss some of the communication technologies used in smart meters.

### 1.4.1 WIFI

Wi-Fi communication is a family of wireless network protocols, based on the IEEE 802.11 family of standards, which are commonly used for local area networking of devices Internet access, enabling nearby digital devices to exchange data by radio waves. WIFI is a major part of the most widely used computer networks in the world, used globally in homes and small office networks to link desktop and laptop computers, tablets, computers, smartphones and smart speakers together and to a wireless router to connect them to the Internet, and in wireless access points in public places like coffee shops, hotels, libraries and airports to provide the public Internet access for mobile devices [17]. Wi-Fi uses multiple parts of the IEEE 802 protocol family and is designed to interwork seamlessly with its wired sibling Ethernet. Compatible devices can network through wireless access points to each other as well as to wired devices and the Internet. The different versions of Wi-Fi are specified by various IEEE 802.11 protocol standards, with the different radio technologies determining radio bands, and the maximum ranges, and speeds that may be achieved. Wi-Fi most commonly uses the 2.4 gigahertz (120 mm) UHF and 5 gigahertz (60 mm) SHF radio bands; these bands are subdivided into multiple channels. Channels can be shared between networks but only one transmitter can locally transmit on a channel at any moment in time [12]. WIFI is used in smart meter applications today because of its numerous advantages. The advantages of WIFI communication includes convenience, mobility, productivity, ease of deployment, cost, and expandability. Its disadvantages include limited security, low coverage range, low reliability, and low speed [13].

### 1.4.2 ETHERNET

Ethernet is a family of wired communication technologies commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN). This method of communication has since been refined to support a greater number of nodes, higher bit rates and longer link distances, but retains much backward compatibility. Over time, It completely replaced competing wired LAN technologies such as Token Ring, FDDI and ARCNET. The original 10BASE5 Ethernet uses coaxial cable as a shared medium, while the newer Ethernet variants use twisted pair and fiber optic links in conjunction with switches. Over the course of its history, Ethernet data transfer rates have been increased from the original 2.94 megabits per second (Mbit/s) to the latest 400 gigabits per second (Gbit/s). The Ethernet standards comprise several wiring and signaling variants of the OSI physical layer in use with Ethernet. Systems communicating over Ethernet divide a stream of data into shorter pieces called frames. Each frame contains source and destination addresses, and error-checking data so that damaged frames can be detected and discarded; most often, higher-layer protocols trigger retransmission of lost frames. Per the OSI model, Ethernet provides services up to and including the data link layer. The 48-bit MAC address was adopted by other IEEE 802 networking standards, including IEEE 802.11 (Wi-Fi), as well as by FDDI. Ether Type values are also used in Subnetwork Access Protocol (SNAP) headers [13]. Ethernet communication is utilized in so many smart meter applications. The pros of Ethernet communication in smart meters include high speed, security, reliability, and efficiency. Its cons include lack of mobility, not easily expandable, high installation overhead and untidy connections [14].

### 1.4.3 BLUETOOTH

Bluetooth is a short-range wireless technology standard used for exchanging data between fixed and mobile devices over short distances using ultra high frequency in the Industrial Scientific Medical band ranging from 2.402 GHz to 2.480 GHz, it is also used in implementing personal Area Networks (PANs). It was originally conceived as a wireless alternative to Recommended standard 232 data cables. It serves as a standard wire-replacement communications protocol primarily designed for low power consumption on low-cost transceiver microchips in each device. Because it uses a radio communications system, they do not have to be in visual line of sight of each other. However, a wireless path must be viable. A master Bluetooth device can communicate with a maximum of seven devices in a piconet, though not all devices reach this maximum. The devices can switch roles, by agreement, and the slave can become the master [16]. The Bluetooth Core Specification provides for the connection of two or more piconets to form a scatternet, in which certain devices simultaneously play the master role in one piconet and the slave role in another. At any given time, data can be transferred between the master and one other device. The master chooses which slave device to address, it then switches rapidly from one device to another in a round robin fashion. Since it is the master that chooses which slave to address, whereas a slave is (in theory) supposed to listen in each receive slot, being a master is a lighter burden than being a slave. Being a master of seven slaves is possible; being a slave of more than one master is possible. The pros of Bluetooth communication include low power consumption, lower setup time, less RF interference, and unlimited node star network topology [16]. Its cons include low coverage area, very low bandwidth and interference from Home RF technologies operating on the same frequency

### 1.4.4 IrDA

The Infrared Data Association (IrDA) is an industry-driven interest group that was founded in 1993 by around 50 companies. IrDA provides specifications for a complete set of protocols for wireless infrared communications, and the name "IrDA" also refers to that set of protocols [17]. The main reason for using the IrDA protocols had been wireless data transfer over the "last one meter" using point-and-shoot principles. Thus, it has been implemented in portable devices such as mobile telephones, laptops, cameras, printers, and smart meters. Main characteristics of IrDA are physically secure data transfer, line-of-sight (LOS) and very low bit error rate (BER) that makes it very efficient. It has frequency range between 300 GHz and 400 THz and wavelength range between 1 mm and 750 nm [18]. The pros of IrDA include low price, compactness, less power, less RF interference and it is more secure compared to RF technologies. The cons are that it requires both transmitter and receiver to be in the line of sight, it cannot move around while transmission is in progress, and it is used for very short distance applications.

### 1.4.5 ZIGBEE

IEEE802.15.4 communication standard, known as ZigBee, is a low-cost, low-power, wireless mesh network standard. It is widely deployed in wireless control and monitoring applications. ZigBee operates in the industrial, scientific, and medical (ISM) radio bands, which are unlicensed - 868 MHz in Europe, 915 MHz in the USA and Australia and 2,4 GHz in almost all over the world. Data transmission rates vary from 20 kb/s in the 868 MHz frequency band to 250 kb/s in the 2,4 GHz frequency band. (ZigBee Alliance, 2013). As Wireless M-Bus is the most popular protocol for wireless sensor networks (WSN) in Europe, ZigBee is the most popular in the U.S.A. Thanks to ZigBee Smart Energy standard, ZigBee is now an integral part of the smart

metering AMI system. ZigBee Smart Energy is standard for interoperable products that monitor, control, inform and automate the delivery and use of energy [22]. The newest version, Zigbee Smart Energy version 1.1, adds several important features including dynamic pricing enhancements, tunneling of other protocols, prepayment features, over-the-air updates and guaranteed backwards compatibility. Generally, ZigBee is more popular in the 2.4 GHz frequency band, but these frequencies are not so penetrating through the walls as 868MHz or 915MHz, especially walls made of concrete reinforced with steel grids. Therefore, it is recommended to use lower bands to create wireless sensor networks. Choosing Zigbee over RF Mesh highly depends on the use case. The former is a preferred option for lighter use cases in the consumer market such as home automation or smart lighting while RF Mesh is a more reliable alternative for industrial applications. Its pros include multiple frequency band operation, supports up to 65,000 devices, low power consumption and low cost. The cons is that there is interference from applications using the same bandwidth, high licensing fees and limited support [20].

### 1.4.6 WiMAX

WiMAX is an industry trade organization formed by leading communications, component, and equipment companies to promote and certify compatibility and interoperability of broadband wireless access equipment that conforms to the IEEE 802.16 and ETSI HIPERMAN standards. WiMAX was formed in April 2001, in anticipation of the publication of the original 10-66 GHz IEEE 802.16 specifications [19]. WiMAX is to 802.16 as the WIFI Alliance is to 802.11. WiMAX operates like WIFI, but at higher speeds over greater distances and for a greater number of users. WiMAX can provide service even in areas that are difficult for wired infrastructure to reach and the ability to overcome the physical limitations of traditional wired infrastructure. It is expected

to offer initially up to about 40 Mbps capacity per wireless channel for both fixed and portable applications, depending on the technical configuration chosen, enough to support hundreds of businesses with T-1 speed connectivity and thousands of residences with DSL speed connectivity. WiMAX can support voice and video as well as Internet data. WiMAX evolved to provide wireless broadband access to buildings, either in competition to existing wired networks or alone in currently unserved rural or thinly populated areas. It can also be used to connect WLAN hotspots to the Internet [21]. WiMAX is also intended to provide broadband connectivity to mobile devices. It would not be as fast as in these fixed applications, but expectations are for about 15 Mbps capacity in a 3 km cell coverage area. The pros is that there is a connection of multiple meters in a single station, much faster deployment, high speed on line-of-site and it is standardized. Its cons are interference weather conditions and high installation cost [18].

### 1.5 Distributed Denial of Service (DDOS) Attacks

Distributed denial of service is slightly different from a denial-of-service attack. In a distributed denial of service attack, multiple attackers attack one single target device. The leading or first attacker creates a daemon or a zombie which is a malicious software designed to carry out an attack on the target at a specific time. After this, the attacker increases the number of attackers by virtually installing the zombie on the internet-connected devices of other users which may be located at another external network [26]. Together, all these devices combine to form a giant network which is also called a “Botnet”. Finally, the parent attacker sends commands to the other multiple devices which have already been infected by the zombie and consequently, they attack the target. In a typical DDoS, the target can either suffer a direct or an indirect hit. If the attack is indirect, the attacker multiplies the number of zombies to attack a single target [26].

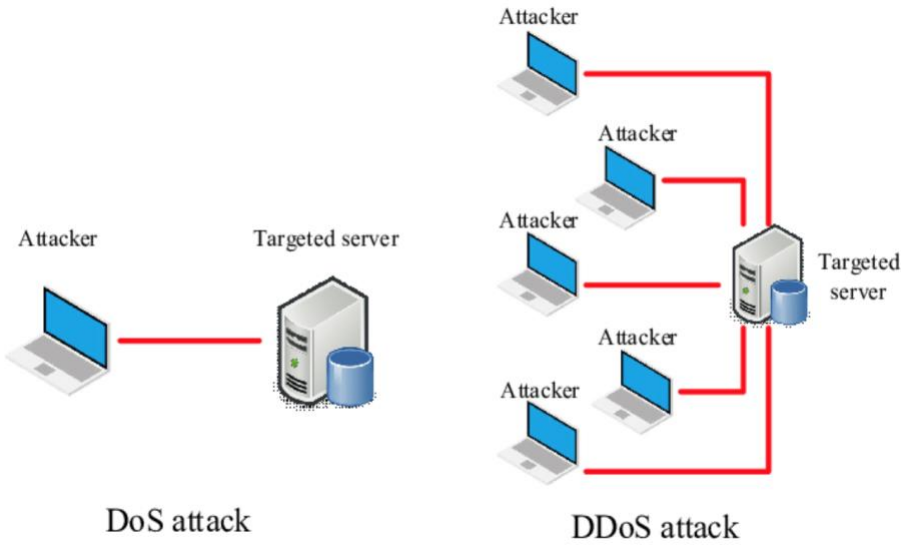


Figure 1.2: Denial of Service and Distributed Denial of Service Attack

### 1.5.1 ARP Flood Attack

The ARP protocol was designed to translate addresses between the second and third layers of the OSI model. Essentially, the Data link layer uses MAC addresses to create a communication link between different hardware devices directly on a small scale. The network layer makes use of Internet Protocol (IP) addresses to form large networks which can be expanded across the globe. In this instance, the attack used is called ARP cache poisoning, a type of man-in-the-middle of attack. This attack puts the hacker on the same subnet as the victim which allows the attacker to listen in on network traffic between the victim and the communication network. Usually, devices which use ARP protocol accept updates unlike devices which make use of Domain Name System. Devices that use DNS accept only secure dynamic updates. Hence, any device can send an ARP reply packet to another host and the host will have no choice but to update its ARP cache with the new value in the ARP packet that was sent to the host. If an ARP reply is sent when no request has been generated, such ARP is called

a gratuitous ARP. With an attacking intent, gratuitous ARP packets can be well positioned such that a host can think it's communicating with another host but in fact, communicating with a listening attacker.

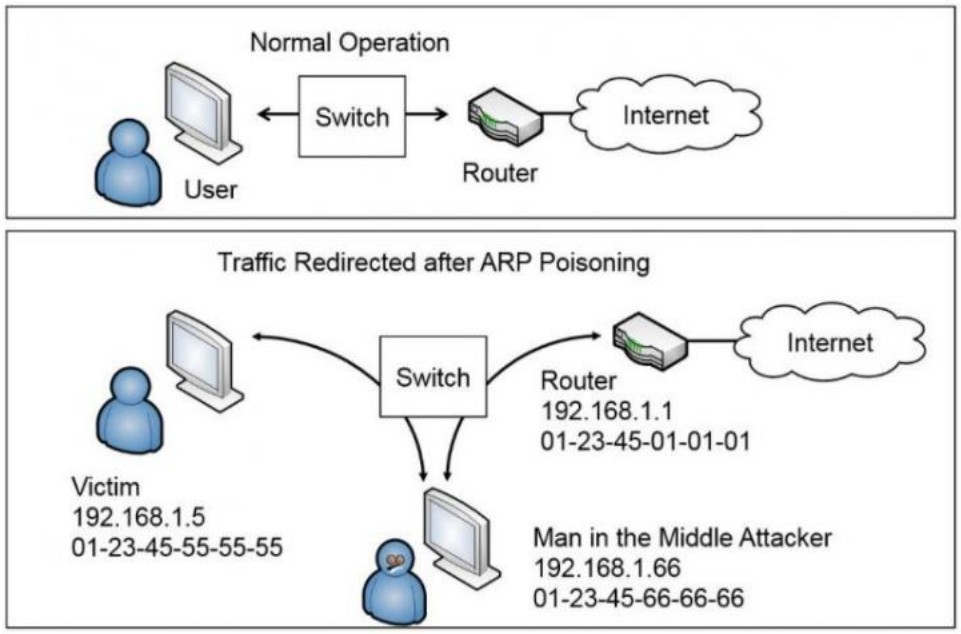


Figure 1.3 ARP Flood Attack Operation [27]

Ideally, normal operation involves communication between the user and the router. However, with the ARP deception, the user and the router are both deceived to send data to a listening attacker.

### 1.5.2 Ping Flood Based DDoS Attack

This is one of the oldest attacks known. It works by flooding the network with a protocol called the Internet Control Message Protocol (ICMP). The ICMP authenticates end-to-end path operation, where an ICMP echo request packet is sent to the target machine and an ICMP echo reply packet confirms the confirmation.

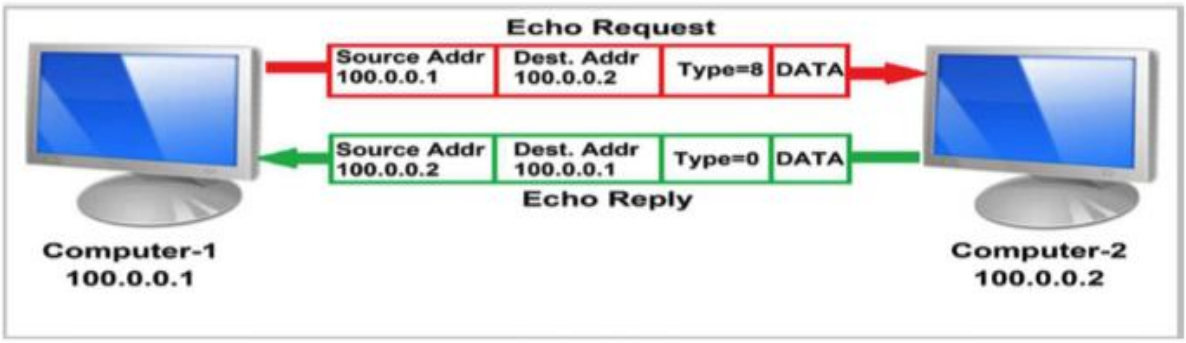


Figure 1.4: Ping Utility [28]

In the diagram above, the host echoes a ping request to a destination to see if that destination can be reached. The computer that receives the message responds with its own echo reply message. The ICMP echo request and reply messages are identified by the value in the type field. As seen above, the value indicated by the red arrow is '8' which indicates an echo request. Similarly, the value indicated by the green arrow is '0' which indicates an echo reply [29]. Usually these attacks are a deluge of ping messages which can be very destructive especially to the availability of the web-based services because what those attacks aim to do is to overload the target server's bandwidth making it unable to address all the ping requests sent to it.

### 1.5.3 Smurf Attack

This is a type of DDoS attack which is more complicated than using pings. This attack makes use of a lot of ICMP packets of altered IP addresses which targets the network to be attacked. To do this, the attacker alters the echo request sent to the botnet using an IP broadcast address [28-29]. A large botnet creates faster and bigger floods of echo replies [30]. This increased traffic makes it hard for the server to respond and if this attack persists, the system completely shuts down [31-32]. In this attack, both the ICMP echo request and ICMP echo reply are used.

While the attacker sends an ICMP echo request to a vulnerable broadcast domain in order to increase the magnitude of the attack, the victim computer receives the amplified attack traffic which is majorly a plethora of echo reply messages. Generally, if the broadcast domain has N number of computers, then for each echo request made, there is N number of echo replies which attacks the victim's network.

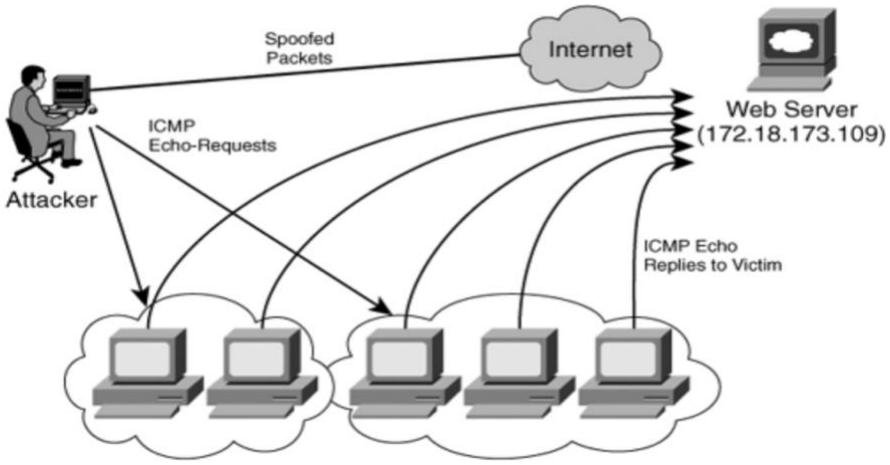


Figure 1.5: SMURF Attack [33]

### 1.5.4 TCP-SYN Flood Attack

The Transmission Control Protocol (TCP) is a transport-layer protocol which prioritizes reliable data transmission between two hosts on a network over the speed of the transmission. It uses a concept called the three-way handshake. Here, the client to connect with a server sends a SYN (Synchronize) packet to the server. The client sets the segment's sequence number to a random value, A. If the server is open for connection, it acknowledges the request made by the client and sends back a SYN-ACK (Synchronize-Acknowledge) packet to the client [34] . The acknowledgement number sets to one more than the received sequence number which in this case is +1 and the sequence number that the server chooses for the packet sets to another random

number, B. Lastly, the client sends an ACK (Acknowledgement) packet to the server to confirm the connection and establish communication between the two of them. The sequence number is set to the received acknowledgement value which is A + 1 and the acknowledgment number is set to one more than the received sequence which is B + 1.

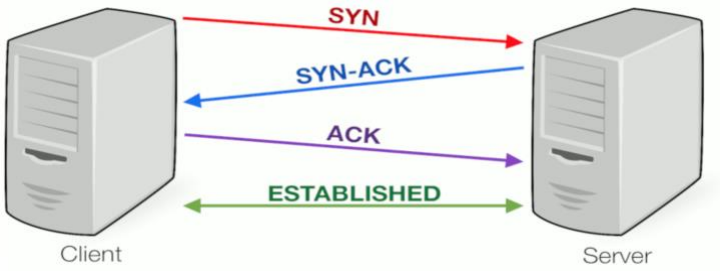


Figure 1.6 Normal 3-way handshake [31]

In this TCP-SYN attack, what the attacker does is to send a SYN to the server. When the server sends a SYN-ACK back to the attacker, he doesn't acknowledge back to the server, instead, he keeps resending SYN packets to the server. Eventually, this process would crash the server and make it unresponsive to legitimate users.

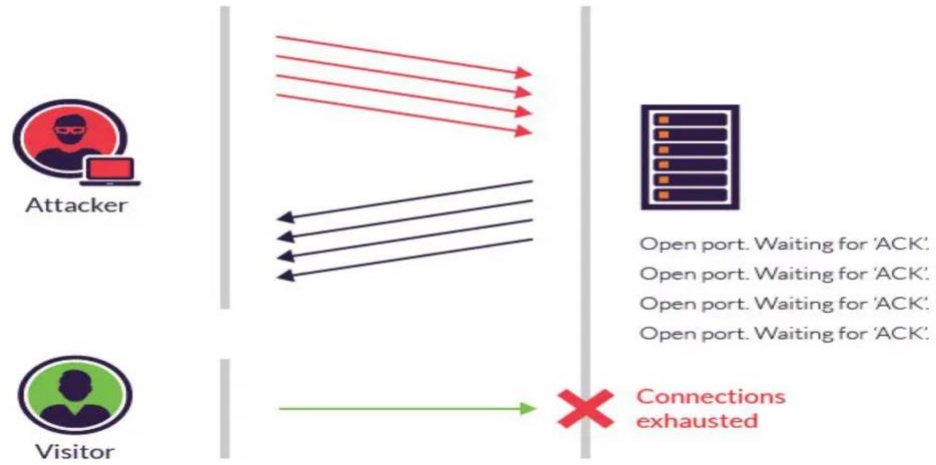


Figure 1.7: TCP/SYN Flood Attack [31]

## 1.6 Prior Works on Smart Electric Meters

Prior research work have been done about the operations and functionality of a smart electric meter. In the paper “Smart Metering and Smart Electricity Consumption” [35], the authors highlighted how to track the daily power usage in houses, the aim of the paper is to change the behaviors of customers by encouraging them switch consumption to off-peak periods, they got their data by conducting case studies in various house hold by measuring and analyzing power consumption patterns. The paper does not discuss anything about cyber security attacks on smart meters. In the paper titled “Analysis of Smart Meter Data for Electricity Consumers” [36] the authors analyzed smart meter data collected from 1000 households in Poland at a 15-minute interval over a period of one year, they analyzed data based on daily load profiles. At the end, they provided a distribution plot of time series decomposition. They concluded that, at household and building levels, the consumption data are much more random and volatile than those at aggregate levels. For paper [36] researcher did not analyze or test the performance of smart meter under security attack. In the paper titled “Cyber-Attacks on Smart Meters in Household Nano-grid [37]”, the authors simulated an unidentified cyber-attack on a smart meter, the attacks were injected into the smart meter in other to monitor their effect. However, the authors did not specify the type of attack, nor the type of smart meter used for the attack. Also, they did not compare the impact of the attack on different smart meters. The research that came very close to what is presented in this Thesis was conducted by previous researchers Harsh Kumar, Ganesh Gunnam and Sanjeev Kumar  and the work was presented in the research paper titled “Security Integrity of Data Collection from Smart Electric Meter Under a Cyber-attack” [38]. In the paper [38], the authors evaluated the impact of a cybersecurity attacks on a General Electric smart meter EPM 6100. However, this smart meter was configured as wireline Ethernet based smart

meter. No wireless configuration was used in this paper [38], no form of wireless or hybrid configurations were carried out in the experiment.

In this Thesis we are presenting configurations that are different from previous studies mentioned above. In most smart meter application today, remote monitoring using wireless connection is the preferred method of communication between smart meters and advance metering infrastructure (AMI) devices. Therefore, in this Thesis, we evaluated the impact of different wireless cybersecurity attacks on different types of smart meters under hybrid and wireless configurations. We also compared the different degrees of impact a wireless configuration can have when compared to a wired configuration.

### 1.7 Statement of Purpose

AMI are used to connect customer smart meters to the utility companies' central office. The increasing use of Advanced Metering Infrastructure (AMI) means the security concerns that come with it needs to be addressed. The fact that utility companies need real-time power usage data means there should be no room for compromise to the security integrity of this data. Mitigating security vulnerabilities allows utility companies to continue to provide dynamic pricing services, demand response and better power grid management. Much like other inceptive systems, AMIs are still behind on the security measures which have already been established to combat cyber intrusions. Although there are basic security protocols on ground, like network encryptions, they are clearly not enough.

While it is true that utility companies already have security measures in place to prevent attacks on AMI systems, those solutions are not inherent to the meters. Different research shows that there are so my ways internet connected devices can be attacked [42-55]. There have been

cases where security measures have been compromised, leaving the smart meters without any defense mechanism. Therefore, AMI's should be designed to inherently detect and prevent cybersecurity attacks. When it comes to cyber-attacks, it is important to know that they differ in intricacy, immensity, and impact [42-55]. Usually, before attackers perpetuate their hacks, they start by gathering information, scanning the systems before running exploits on the target AMI network [23-24].

Despite the obvious positives of smart grid technology and smart electric meters, the extent to which cyber-attacks can hamper the operation of smart meters is not yet very clear, this means that efforts to make sure security is not compromised must be taken. This research shows several experiments which were carried out on smart meters. However, the type of configurations used in this research is wireless using WIFI, as compared to the previous research [41] done in dash using Ethernet based wired connection. The experiments were carried out in a controlled laboratory at the Network Research Laboratory at the University of Texas Rio Grande Valley. The commercial grade smart meters which were used were the EPM 6100, E650 and EPM 7100 from General Electric. This thesis presents different results of the research done using different cybersecurity attacks.

## 1.8 Hypothesis.

Wireless Cyber security attacks have an impact on the consumption integrity of EPM6100 smart meters and other smart meters that share similar Network Interface Card (NIC). Also, wireless cyber security attacks can completely disconnect a smart meter from a remote monitoring device.

## 1.9 Thesis Outline

In this thesis, performances of Smart Metering Communication against a varying number of DDoS attacks were analyzed and the security of Smart Electric Meters were discussed. In chapter 1, Introduction to Smart Grids, Smart Electric Meters, Advanced Metering Infrastructure, Distributed Denial of Service attacks and security challenges of Advanced Metering Infrastructure were all discussed. In chapter II, the effects of wireless cybersecurity attacks on the readings of EPM6100 was evaluated. In Chapter III, the effect of a hybrid of wired and wireless cybersecurity attacks on EMP6100 was evaluated. Chapter IV is all about the connectivity test; different types of cybersecurity attacks (PING, SMURF, and TCP/SYN) were used to determine the connectivity of EPM6100, EPM7000 and E650 smart meters. In Chapter V, all the results obtained from Chapters II to IV were compared. Finally, the research paper was concluded in Chapter VI.

# CHAPTER II

# EXPERIMENTAL EVALUATION OF DATA COLLECTION INTEGRITY OF GENERAL ELECTRIC EPM 6100 POWER QUALITY SMART METER UNDER WIRELESS CYBER ATTACK

As already established in the previous chapter, a major issue that electric power companies must deal with is Cyber Security because of the fact that they make use of smart grid technology. Besides this, there is also the problem of identifying how and how much havoc is wrecked against smart meter operations by cyber-attacks and also the effect this has on gathering power usage data from customers. In a bid to understand this, we have conducted several experiments in a controlled cyber security laboratory to test an EMP 6100 commercial grade smart meter and present results of this investigation which measures the operational integrity of the smart meter when connected wirelessly using a WIFI connection through an access point.

## 2.1 EPM 6100 Power Quality Smart Electric Meter from GE

The EPM 6100 shown below us is a smart meter which is produced by General Electric (GE). Basically, it allows service providers to oversee and manage the rate at which they use energy in factories, businesses and residents. EPM 6100 is a smart multifunctional meter that has several interfaces like the RS485, RJ45 Ethernet and IEEE 802.11 for Wi-Fi connection. It also features ANSI C12.20 (0.2% class) accuracy. The benefit of all these is that even when there is already an existing communication system, it is still easy to deploy this smart meter. It also has

an alarm system which enables it to detect early enough when there is a power problem in order to rectify the problem early enough. This unit uses a standard 5 or 1-amp CTs.

Additional benefits of the EPM 6100 smart meter are that it is easy to program or configure in a way that is tailored to exactly what the manual states and it has a plethora of voltage, current and energy measurements. In buildings that have multiple occupants, this smart meter can be used to appropriate energy usage to each of them.


Figure 2.1: Smart Meter (EPM 6100) with EnerVista Software for remote power recording [35].

The EnerVista software shown in the diagram above gives the service providers the platform to access all the necessary tools remotely for the configuration of the smart meter in use. This is done in real-time and it can monitor the status of the smart meters and power usage statistics.

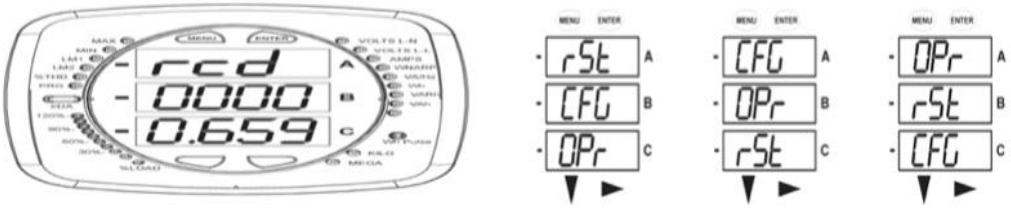


Figure 2.2: Manual Reading Parameters setting from Smart Meters [35] .

From the figure above, we see that it is easy to read several parameters like voltage between any two phases, between a phase and the neutral, the energy (in Watt-hours), active, reactive, and apparent power, baud rate etc. It is also possible to configure the parameters from the front panel buttons like the menu and the left or right arrows. This configuration can still be done remotely if the person has the software installed on a computer at that remote location. In this thesis, the goal was to configure and read data from the meter from its front panel while configuring it manually for the recording. The front panel has four arrow buttons and a menu button for configuration options. Things that can be configured from the front panel include Potential transformer ratio, current transformer ratio, meter reset, baud rate, voltage, current, watt-hour etc.

## 2.2 Experimental Setup

This section evaluates the security performance of the EPM 6100 from General Electric using a Wi-Fi connected system. The EPM 6100 is connected to a remote computer and also to another network designated for the attack (See diagram below). This experiment used a “3 EL WYE” in the Meter Programming Setup and a 200-Watt (Two light bulbs) load is connected to the smart meter at the load end.

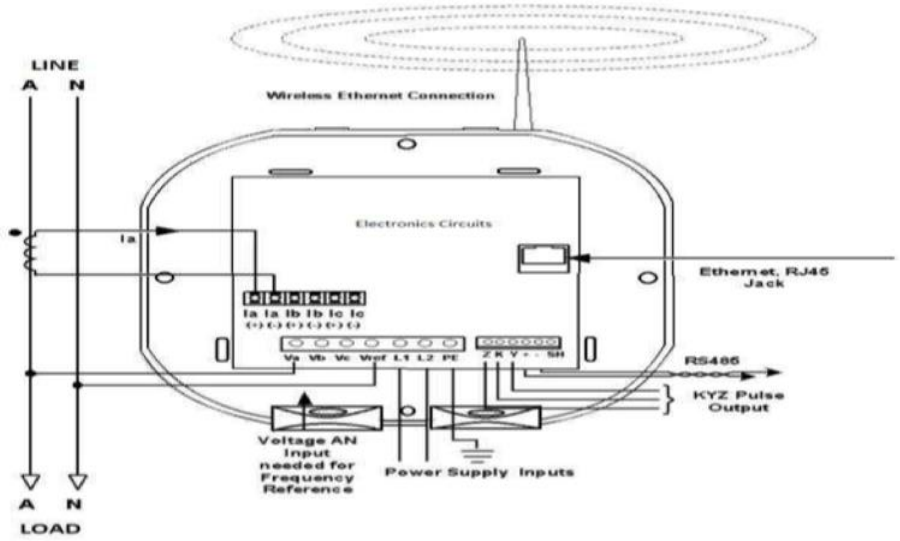


Figure 2.3: "3 EL WYE" in Meter Programming Setup

When using a monitoring computer, we obtained the power usage data remotely from the smart meter. We also simulated a ping based security attack traffic which was then sent to the smart meter. The schematics of this set up (Which was done at the Network Research Laboratory at UTRGV) is shown below:

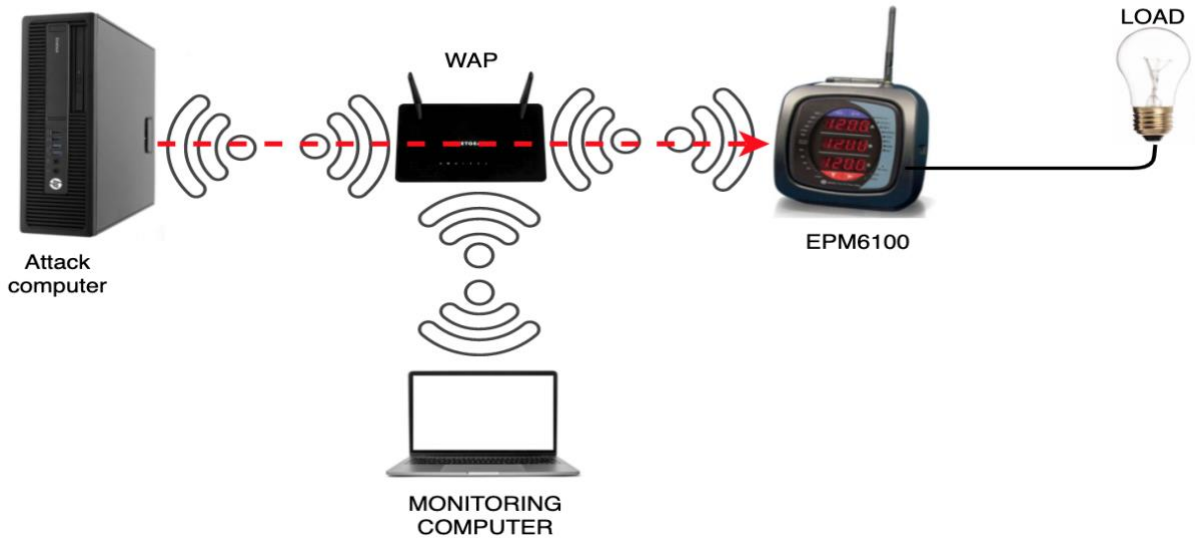


Figure 2.4: Experimental setup for cyber-attack.

The smart meter was remotely accessed for power reading over the Wi-Fi connection which made use of the EnerVista software installed on the remote monitoring computer.


Figure 2.5: Lab setup used in experiment showing Load, Smart meter and remote monitoring computer.

Four separate experiments were conducted, and the aim was to observe the impact of cyber-attacks on the Watt-Hour data over a couple of days and compare this impact to the Watt-Hour data recorded over a couple of days but with no attack.

### 2.2.1 Performance Parameters for Evaluation Experiment I under wireless Attack for 4 days

In this experiment, we made use of two 200-Watt incandescent light bulbs for the smart meter. This load was the baseline load i.e. the recorded load without any attack. This baseline load was used for the smart meter operation for four days.

We collected the baseline power usage data (in the absence of a cyber-attack) which can be seen in column 2 of Table 2.1. We then repeated this procedure but this time, we introduced a wireless ping-based cyber-attack. The power usage data we recorded this time (over a period of four days) can be seen in column 3 of Table 2.1. The ping attack traffic was recorded to be a continuous 50 Mbps which is actually low in intensity.

### 2.2.2 Experiment II Under wireless Attack for 7 Days

Similar to the first experiment, we used two 200-Watt incandescent bulbs for the smart meter which was the baseline load (no attack). This baseline load was used for 7 days during which we collected power usage data remotely. This data is shown in column 2 of Table 2.2. This procedure was performed again with the presence of a ping based indirect cyber-attack. Again, the power usage data was recorded and shown in column 3 of Table 2.2. The Ping attack traffic was also measured to be 50 Mbps which is low in intensity.

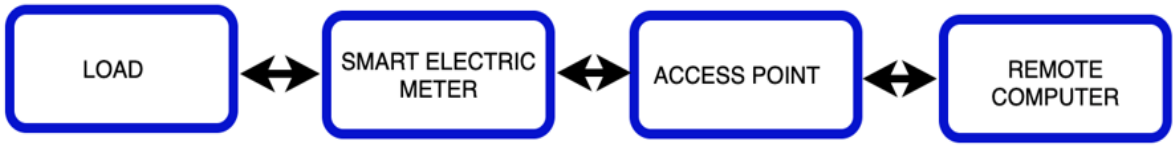


Figure 2.6: Experimental setup

### 2.2.3 Experiment III Under wireless Attack for 15 Days

Again, we used 200-Watt incandescent light bulbs for the smart meter. This was the baseline load (No attack). This baseline load was used for 15 days (360 hours) during which we collected power usage data remotely. This data is shown in column 2 of Table 2.3. This procedure was performed again with the presence of a ping based indirect cyber-attack. Again,

the power usage data was recorded and shown in column 3 of Table 2.3. The Ping attack traffic was measured to be 50 Mbps which is also low in intensity.

### 2.2.4 Experiment IV Under wireless Attack for 30 Days

Two 200-Watt incandescent light bulbs were used for the smart meter. This was the baseline load (No attack). This baseline load was used for 30 days (720 hours) during which we collected power usage data remotely. This data is shown in column 2 of Table 2.4. This procedure was performed again with the presence of a ping based indirect cyber-attack. Again, the power usage data was recorded and shown in column 3 of Table 2.4. The Ping attack traffic was measured to be 50 Mbps which is also low in intensity.

## 2.3 Experimental Results and Discussion

### 2.3.1 Results from Experiment I

It was observed that during the first 24 hours of the attack, there was no meaningful effect on the power usage data. However, post 24 hours, an obvious decline in the power usage data could be seen. In table 2.1, we see the average power consumption data for 96 hours which is shown as a running average power consumption after the first, second, third and fourth days in the third column of table 2.1.

**Average power consumption with and without the cyber-attack on the Smart Meter measured for 4 days.**

| No of Days | Baseline-Average power consumption (In Watt-Hour) | Average Power consumption under attack (In Watt-Hour) | Percentage Power Loss |
|---|---|---|---|
| 1 | 203.32 | 203.21 | 0.0541 |
| 2 | 203.33 | 203.15 | 0.0885 |
| 3 | 203.23 | 202.53 | 0.3444 |
| 4 | 203.25 | 202.34 | 0.4477 |

Table 2.1

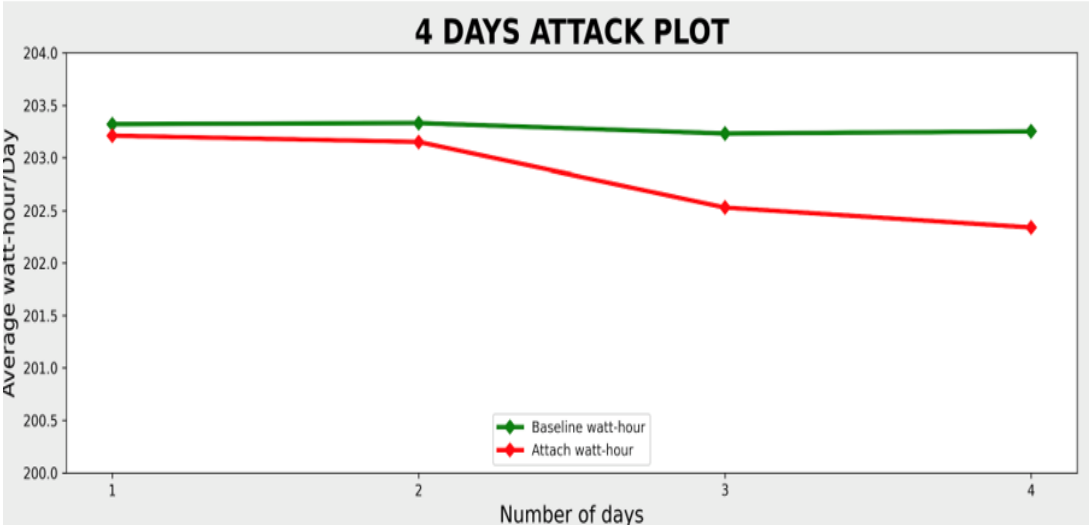


Figure 2.7: Attack Plot for 4 days.

The average power consumption measured in Watt-Hours for Experiment I without any cyber-attack is shown in green and the power consumption with cyber-attack is measured in red.

% Power Loss (After 4 days) =

$$\frac{Power\ consumption\ (Baseline) - Power\ consumption\ (Under\ Cyber-attack)}{Power\ consumption\ (Baseline)} \text{ x } 100$$

$$= \frac{203.25-202.34}{203.32}\ x\ 100$$

= 0.4477%

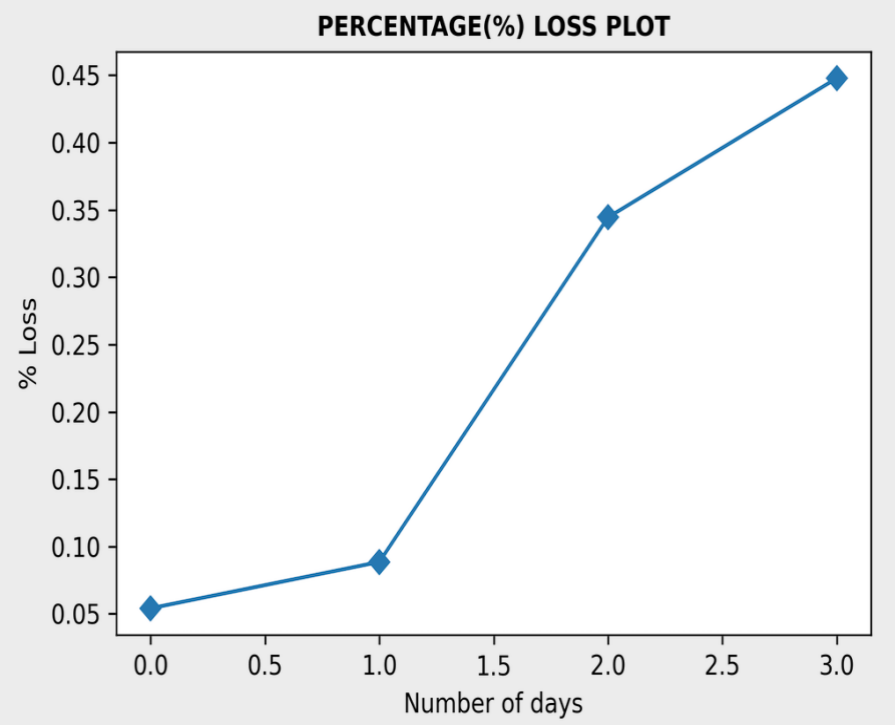


Figure 2.8: Percentage Power Loss Plot for Experiment I

From the power loss plot seen above, as the number of days increases, the percentage power loss increases which indicates that the loss suffered by electric power companies increases in magnitude if a cyber-attack is left unchecked.

In Experiment I, it could be seen that by the end of Day 4, the smart meter had recorded an overall power loss of 0.4477%. This was due to the attack on the smart meter. Also, when observing the power consumption for the baseline and the power consumption during the cyber-attack, a trend was noticeable and it showed a decline in the average power consumption recorded by the smart meter and sent to the remote monitoring computer. It is easy to think that the 0.4477% loss is negligible however that is not true as it would make a huge difference when it comes to deploying smart meters by a large electric company to large commercial organizations. An example to demonstrate this is shown below:

**Financial loss estimation due to the cyber-attack for a large electric company's deployment under experiment I setup.**

The point of this is to estimate how much a cyber-attack on smart meters affects the revenue of a large electric company if they use the type of smart meter suggested above.

It should be noted that some of the data used were Pacific Gas & Electric data obtained from [36] and the data can be seen below.

- Company Name: Pacific Gas & Electric
- Number of customers (Residential and Commercial): 5,069,189
- Overall monthly power consumption: 6,040,152,083 kWh
- Average price from [36] = 17.41 cents/kWh
- Loss of power due to security attack on Smart Meter = 2,704,176,088 kWh/month (using our 0.4477% power loss)
- Overall revenue loss because of cyber-attacks on smart-meter = $470,797,056 Million/month.

### 2.3.2 Result from Experiment II

From figure 2.9, we saw that during the first 24 hours of the attack, there was no particularly meaningful impact on the power usage reading but after the first 24 hours, the smart meter showed that power consumption was declining. The table 2.2 below shows the power consumption data for 7 days (From the 1st day to the 7th day).

**Average power consumption with and without the cyber-attack on the Smart Meter measured for 7 days.**

| No of Days | Baseline Average Power consumption (In Watt-Hour) | Average Power consumption under attack (In Watt-Hour) | Percentage Power loss |
|---|---|---|---|
| 1 | 203.32 | 203.21 | 0.0541 |
| 2 | 203.33 | 203.15 | 0.0885 |
| 3 | 203.23 | 202.53 | 0.3444 |
| 4 | 203.25 | 202.34 | 0.4477 |
| 5 | 203.24 | 202.23 | 0.4969 |
| 6 | 203.28 | 202.19 | 0.5362 |
| 7 | 203.26 | 202.17 | 0.5363 |

Table 2.2

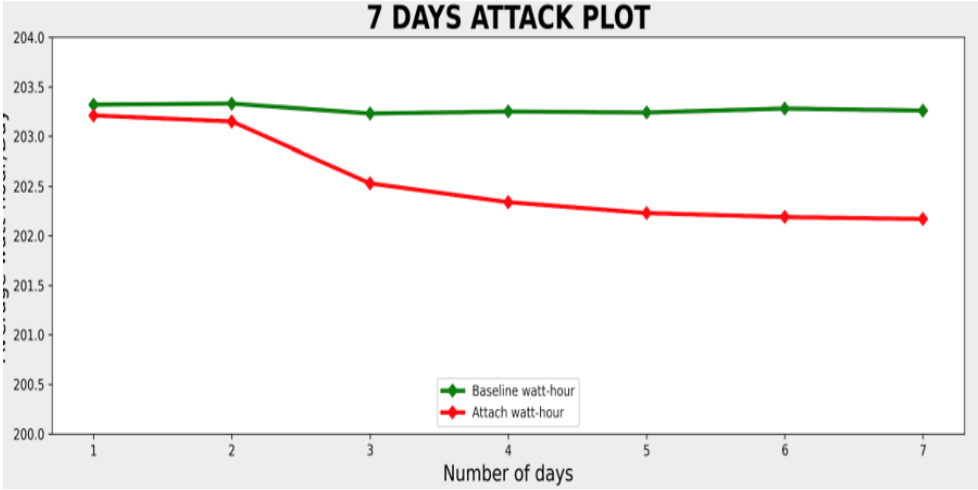


Figure 2.9: Attack Plot for 7 days

The average power consumption measured in Watt-Hours for Experiment II without any cyber-attack is shown in green and the power consumption with an indirect cyber-attack is measured in red.

**Loss of Power recorded (during the cyber-attack)**

$$\% \text{ Loss of Power after 7 days} = \frac{Power\ consumption\ (Baseline) - Power\ consumption\ (Under\ cyber\ attack)}{Power\ consumption\ (Baseline)}$$

$$= \frac{203.26 - 202.17}{203.26} x\ 100$$

$$= 0.5363\%$$

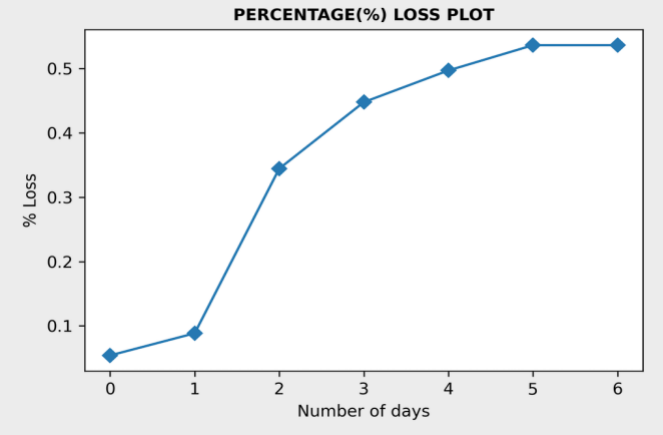


Figure 2.10: Percentage Loss Plot for Experiment II

In the Percentage loss plot shown above, the power consumption loss increased linearly in the first 24 hours although it was minimal. During the remaining six days, the power loss increased exponentially from 0.2% to 0.5%.

In Experiment II, it could be seen that by the end of Day 7, the smart meter had recorded an overall power loss of 0.53%. This was due to the attack on the smart meter. Also, when observing the power consumption for the baseline and the power consumption during the cyber-attack, a trend was noticeable and it showed a decline in the average power consumption recorded by the smart meter and sent to the remote monitoring computer. It is easy to think that the 0.53% loss is negligible however that is not true as it would make a huge difference when it comes to deploying smart meters by a large electric company to large commercial organizations. An example to demonstrate this is shown below:

**Financial loss estimation due to the cyber-attack for a large electric company's deployment under experiment II setup.**

The point of this is to estimate how much a cyber-attack on smart meters affects the revenue of a large electric company if they use the type of smart meter suggested above.

It should be noted that some of the data used were Pacific Gas & Electric data obtained from [36] and the data can be seen below.

- Company Name: Pacific Gas & Electric
- Number of customers (Residential and Commercial): 5,069,189
- Overall monthly power consumption: 6,040,152,083 kWh
- Average price from [53] = 17.41 cents/kWh
- Loss of power due to security attack on Smart Meter = 3,239,333,562 kWh/month (using our 0.53% power loss)
- Overall revenue loss because of cyber-attacks on smart meter = $563,967,973 Million/month.

### 2.3.3 Result for Experiment III

From figure 2.11, we saw that during the first 24 hours of the attack, there was no particularly meaningful impact on the power usage reading but after the first 24 hours, the smart meter showed that power consumption started rapidly declining. The table 2.3 below shows the power consumption data for 15 days (From the 1$^{st}$ day to the 15$^{th}$ day)

**Average power consumption with and without the cyber-attack on the Smart Meter measured for 7 days.**

| No of Days | Baseline Average Power consumption (In Watt-Hour) | Average Power consumption under attack (In Watt-Hour) | Percentage Power loss |
|---|---|---|---|
| 1 | 203.32 | 203.21 | 0.0541 |
| 2 | 203.33 | 203.15 | 0.0885 |
| 3 | 203.23 | 202.53 | 0.3444 |
| 4 | 203.25 | 202.34 | 0.4477 |
| 5 | 203.24 | 202.23 | 0.4969 |
| 6 | 203.28 | 202.19 | 0.5362 |
| 7 | 203.26 | 202.17 | 0.5363 |
| 8 | 203.23 | 202.08 | 0.5659 |
| 9 | 203.16 | 202.00 | 0.5710 |
| 10 | 203.35 | 201.99 | 0.6839 |
| 11 | 203.25 | 201.86 | 0.7380 |
| 12 | 203.26 | 201.75 | 0.7478 |
| 13 | 203.28 | 201.74 | 0.7723 |
| 14 | 203.29 | 201.67 | 0.7969 |
| 15 | 203.31 | 201.67 | 0.8066 |

Table 2.3

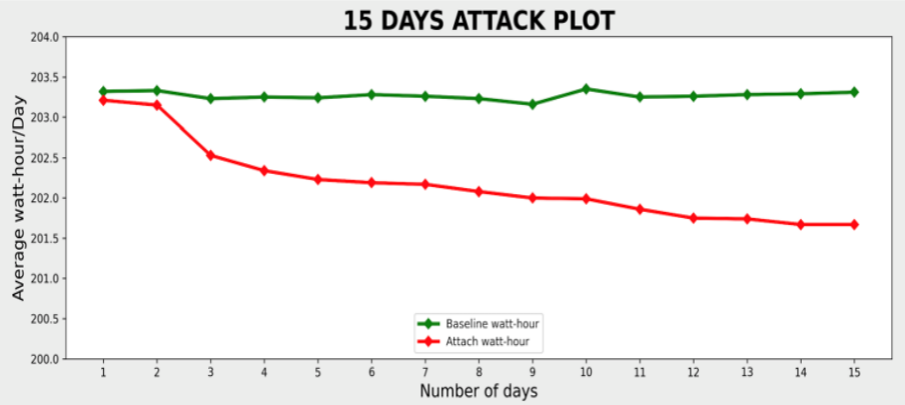


Figure 2.11: 15 Days Attack Plot

The average power consumption measured in Watt-Hours for Experiment III without any cyber-attack is shown in green and the power consumption with an indirect cyber-attack is measured in red.

**Loss of Power recorded (during the cyber-attack)**

$$\% \text{ Loss of Power after 7 days} = \frac{Power\ consumption\ (Baseline) - Power\ consumption\ (Under\ cyber\ attack)}{Power\ consumption\ (Baseline)}$$

$$= \frac{203.31 - 201.67}{203.31} x\ 100$$

$$= 0.81\%$$

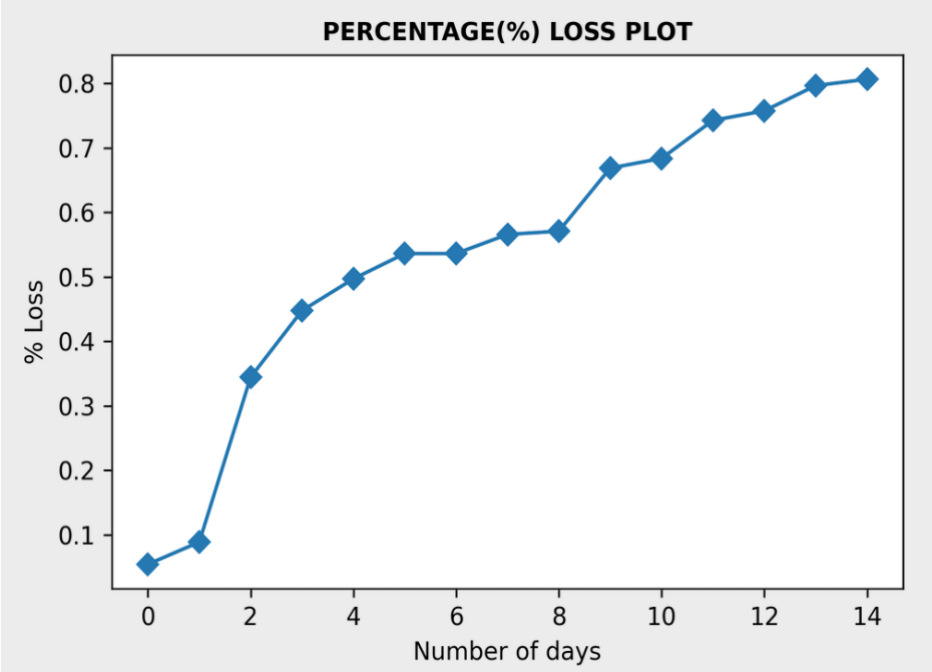


Figure 2.12: Percentage loss plot for Experiment III

In the Percentage loss plot shown above, the power consumption loss increased linearly in the first 24 hours although it was minimal. During the next six days, the power loss increased exponentially from 0.2% to approximately 1.1%. Over the remaining 8 days, the percentage loss kept increasing till it reached 0.8%

In Experiment III, it could be seen that by the end of Day 15, the smart meter had recorded an overall power loss of 0.81%. This was due to the attack on the smart meter. Also, when observing the power consumption for the baseline and the power consumption during the cyber-attack, a trend was noticeable and it showed a decline in the average power consumption recorded by the smart meter and sent to the remote monitoring computer. It is easy to think that the 0.81% loss is negligible however that is not true as it would make a huge difference when it comes to deploying smart meters by a large electric company to large commercial organizations. An example to demonstrate this is shown below:

**Financial loss estimation due to the cyber-attack for a large electric company's deployment under experiment III setup.**

The point of this is to estimate how much a cyber-attack on smart meters affects the revenue of a large electric company if they use the type of smart meter suggested above.

It should be noted that some of the data used were Pacific Gas & Electric data obtained from [36] and the data can be seen below.

- Company Name: Pacific Gas & Electric
- Number of customers (Residential and Commercial): 5,069,189
- Overall monthly power consumption: 6,040,152,083 kWh
- Average price from [36] = 17.41 cents/kWh
- Loss of power due to security attack on Smart Meter = 4,871,986,670 kWh/month (using our 0.81% power loss)
- Overall revenue loss because of cyber-attacks on smart meter = $848,212,879 Million/month.

### 2.3.4 Result for Experiment IV

From figure 2.13, we saw that during the first 24 hours of the attack, there was no particularly meaningful impact on the power usage reading but after the first 24 hours, the smart meter showed that power consumption started rapidly declining. The table 2.3 below shows the power consumption data for 30 days (From the 1$^{st}$ day to the 30$^{th}$ day).

**Average power consumption with and without the cyber-attack on the Smart Meter measured for 7 days.**

| No of Days | Baseline Average Power consumption (In Watt-Hour) | Average Power consumption under attack (In Watt-Hour) | Percentage Power loss |
|---|---|---|---|
| 1 | 203.32 | 203.21 | 0.0541 |
| 2 | 203.33 | 203.15 | 0.0885 |
| 3 | 203.23 | 202.53 | 0.3444 |
| 4 | 203.25 | 202.34 | 0.4477 |
| 5 | 203.24 | 202.23 | 0.4969 |
| 6 | 203.28 | 202.19 | 0.5362 |
| 7 | 203.26 | 202.17 | 0.5363 |
| 8 | 203.23 | 202.08 | 0.5659 |
| 9 | 203.16 | 202.00 | 0.5710 |
| 10 | 203.35 | 201.99 | 0.6839 |
| 11 | 203.25 | 201.86 | 0.7380 |
| 12 | 203.26 | 201.75 | 0.7478 |
| 13 | 203.28 | 201.74 | 0.7723 |
| 14 | 203.29 | 201.67 | 0.7969 |
| 15 | 203.31 | 201.67 | 0.8066 |
| 16 | 203.30 | 201.56 | 0.8541 |
| 17 | 203.29 | 201.48 | 0.8885 |
| 18 | 203.30 | 200.97 | 1.1444 |
| 19 | 203.22 | 200.68 | 1.2447 |
| 20 | 203.30 | 200.66 | 1.2969 |
| 21 | 203.28 | 200.56 | 1.3362 |
| 22 | 203.28 | 200.56 | 1.3363 |
| 23 | 203.25 | 200.47 | 1.3659 |
| 24 | 203.26 | 200.47 | 1.3710 |

| | | | |
|---|---|---|---|
| 25 | 203.27 | 200.28 | 1.4688 |
| 26 | 203.16 | 200.15 | 1.4839 |
| 27 | 203.15 | 200.02 | 1.5429 |
| 28 | 203.01 | 199.85 | 1.5576 |
| 29 | 203.00 | 199.76 | 1.5969 |
| 30 | 202.98 | 199.72 | 1.6066 |
| 31 | 202.90 | 202.70 | 0.0986 |

Table 2.4

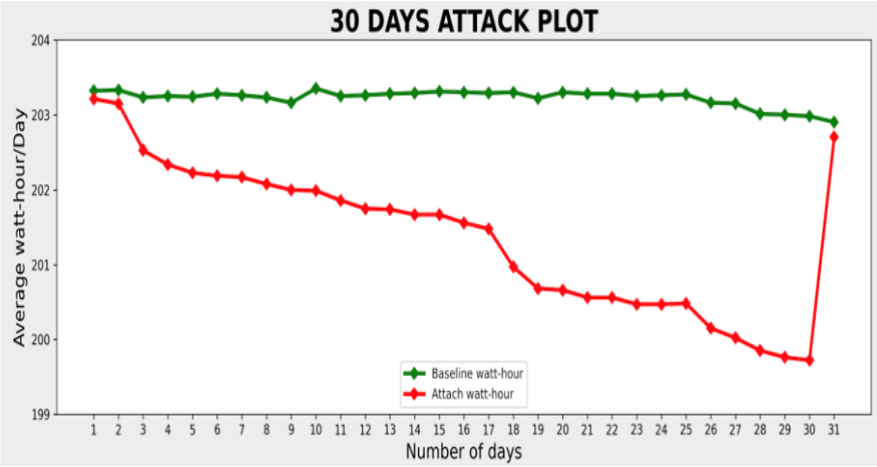


Figure 2.13: 30 Days Attack Plot

The average power consumption measured in Watt-Hours for Experiment IV without any cyber-attack is shown in green and the power consumption with an indirect cyber-attack is measured in red.

**Loss of Power recorded (during the cyber-attack)**

$$\% \text{ Loss of Power after 7 days} = \frac{Power\ consumption\ (Baseline) - Power\ consumption\ (Under\ cyber\ attack)}{Power\ consumption\ (Baseline)}$$

$$= \frac{202.90 - 202.70}{202.90} x\ 100$$

$$= 0.098\%$$

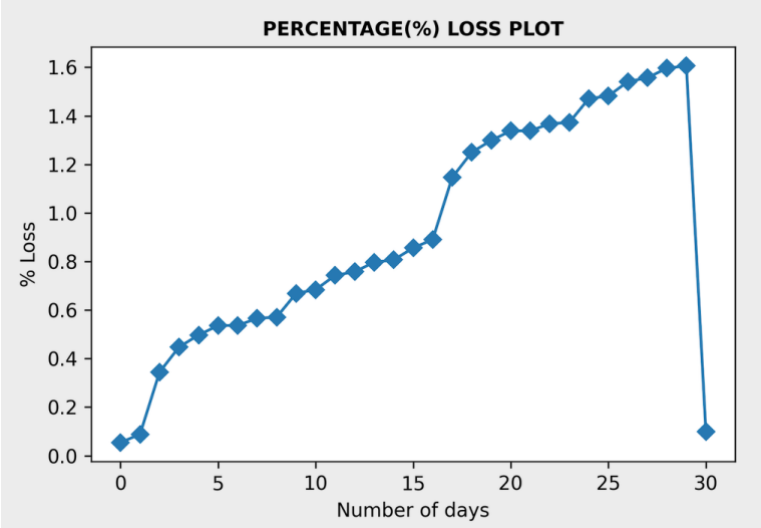


Figure 2.14: Percentage Loss Plot for Experiment IV

In the Percentage loss plot shown above, the power consumption loss increased linearly in the first 24 hours although it was minimal. During the next six days, the power loss increased exponentially from 0.2% to approximately 0.7%. Over the following 8 days, the percentage loss kept increasing till it reached 0.8% before it took another sharp increase over the 14 days to peak at approximately 1.6%. On the last day, this loss dropped sharply to 0.098% after the attack was removed.

In Experiment IV, it could be seen that by the end of Day 30, the smart meter had recorded an overall power loss of 1.6%. This was due to the attack on the smart meter. Also, when observing the power consumption for the baseline and the power consumption during the cyber-attack, a trend was noticeable and it showed a decline in the average power consumption recorded by the smart meter and sent to the remote monitoring computer. It is easy to think that the 1.6% loss is negligible however that is not true as it would make a huge difference when it comes to deploying smart meters by a large electric company to large commercial organizations. An example to demonstrate this is shown below:

**Financial loss estimation due to the cyber-attack for a large electric company's deployment under experiment IV setup.**

The point of this is to estimate how much a cyber-attack on smart meters affects the revenue of a large electric company if they use the type of smart meter suggested above.

It should be noted that some of the data used were Pacific Gas & Electric data obtained from [36] and the data can be seen below.

- Company Name: Pacific Gas & Electric
- Number of customers (Residential and Commercial): 5,069,189
- Overall monthly power consumption: 6,040,152,083 kWh
- Average price from [36] = 17.41 cents/kWh
- Loss of power due to security attack on Smart Meter = 595,558,995.38 kWh/month (using our 1.6% power loss)
- Overall revenue loss because of cyber-attacks on smart Meter = $103,686,821 Million/month.

What these experiments have demonstrated is that cyber-attacks can have a damaging effect on the operation of smart meters and this can have a ripple effect on the finances of large electric companies as they could suffer heavy losses due to cyber-attacks.

## 2.4 Chapter Summary

In this chapter, we performed a wireless cyber-attack on the EPM 6100 Smart electric meter from General Electric in a bid to understand and evaluate the effects of these attacks on the operation of the smart meter and how data traffic moves between the smart meter and a remote monitoring computer. It is known that smart meters are very useful for customers and especially utilities particularly when we consider how they implement their smart grid infrastructure and provide consistent power assessment and problem troubleshooting.

These experiments shades light on the effect of cybersecurity attacks which have been research extensively [42-55]. We found out that even a wireless ping-based attack can have a very large impact on a smart meter operation especially for large electric companies. When we did the wireless cyber-attack 30-Day experiment, we noticed that on the first day, the impact was minimal but at the end of the entire billing cycle, the impact had become significant. These type of attacks can lead to big financial losses in millions of dollars for electric companies especially the ones that focus in large scale smart grid infrastructure.

# CHAPTER III

# EXPERIMENTAL EVALUATION OF DATA COLLECTION INTEGRITY OF GENERAL ELECTRIC EPM 6100 POWER QUALITY SMART METER UNDER A HYBRID OF WIRELESS AND WIRED CYBER ATTACK

A major issue that electric power companies must deal with is Cyber Security because they make use of smart grid technology. Besides this, there is also the problem of identifying how and how much havoc is wrecked against smart meter operations by cyber-attacks and also the effect this has on gathering power usage data from customers. In a bid to understand this, we have conducted several experiments in a controlled cyber security laboratory to test an EPM 6100 commercial grade smart meter and present results of this investigation which measures the operational integrity of the smart meter using a hybrid of wired and wireless connection.

## 3.1 EPM 6100 Power Quality Smart Electric Meter from GE

The EPM 6100 shown below us is a smart meter which is produced by General Electric (GE). Basically, it allows service providers oversee and manage the rate at which they use energy in factories, businesses and residents. EPM 6100 is a smart multifunctional meter that has several interfaces like the RS485, RJ45 Ethernet and IEEE 802.11 for Wi-Fi connection. It also features ANSI C12.20 (0.2% class) accuracy. The benefit of all these is that even when there is already an existing communication system, it is still easy to deploy this smart meter. It also has an alarm

system which enables it detect early enough when there is a power problem in order to rectify the problem early enough. This unit uses a standard 5 or 1-amp CTs.

Additional benefits of the EPM 6100 smart meter are that it is easy to program or configure it in a way that is tailored to exactly what the manual states and it has a plethora of voltage, current and energy measurements. In buildings that have multiple occupants, this smart meter can be used to appropriate energy usage to each of them.

### 3.2 Experimental Setup

This section evaluates the security performance of the EPM 6100 from General Electric using a hybrid of wired and wireless connection. The EPM 6100 is connected to a remote computer and also to another network designated for the attack (See diagram below). This experiment used a "3 EL WYE" in the Meter Programming Setup and a 200-Watt load is connected to the smart meter at the load end.

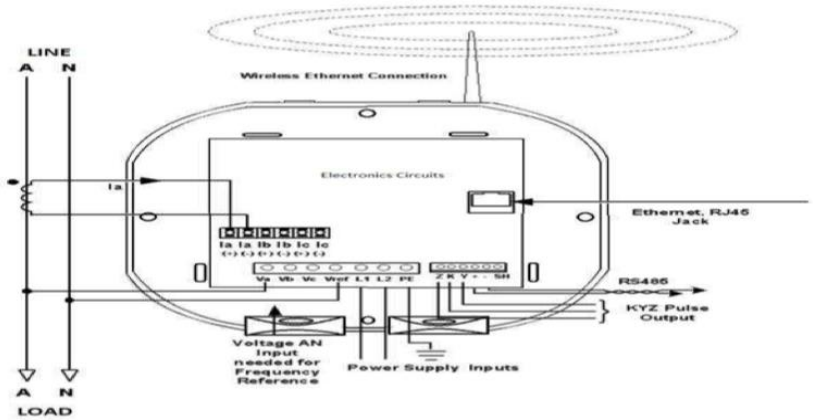


Figure 3.1: "3 EL WYE" in Meter Programming Setup

When using a monitoring computer, we obtained the power usage data remotely from the smart meter. We also simulated a ping based security attack traffic which was then sent to the smart meter. The schematics of this set up (Which was done at the Network Research Laboratory at UTRGV) is shown below:

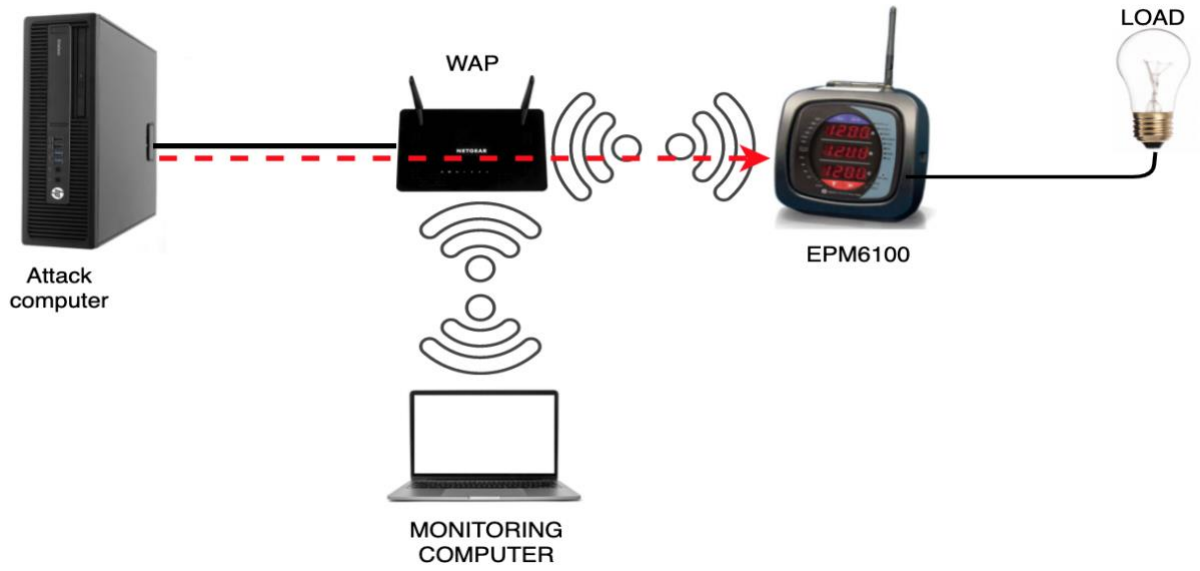


Figure 3.2: Experimental setup for cyber-attack.

The smart meter was remotely accessed for power reading over the Wi-Fi connection which made use of the EnerVista software installed on the remote monitoring computer.


Figure 3.3: Lab setup used in experiment showing Load, Smart meter and remote monitoring computer.

Four separate experiments were conducted, and the aim was to observe the impact of cyber-attacks on the Watt-Hour data over a couple of days and compare this impact to the Watt-Hour data recorded over a couple of days but with no attack.

## 3.3 Performance Parameters for Evaluation

### 3.3.1 Experiment I under Hybrid Attack for 4 days

In this experiment, we made use of a 200-Watt incandescent light bulbs for the smart meter. This load was the baseline load i.e. the recorded load without any attack. This baseline load was used for the smart meter operation for four days. We collected the baseline power usage data (in the absence of a cyber-attack) which can be seen in column 2 of Table 3.1. We then repeated this procedure but this time, we introduced a hybrid ping-based cyber-attack. The power usage data we recorded this time (over a period of four days) can be seen in column 3 of Table

3.1. The ping attack traffic was recorded to be a continuous 50Mbps which is actually low in intensity.

### 3.3.2 Experiment II Under Hybrid Attack for 7 Days

Similar to the first experiment, we used a 200-Watt incandescent bulbs for the smart meter which was the baseline load (no attack). This baseline load was used for 7 days during which we collected power usage data remotely. This data is shown in column 2 of Table 3.2. This procedure was performed again with the presence of a ping based indirect cyber-attack. Again, the power usage data was recorded and shown in column 3 of Table 3.2. The Ping attack traffic was also measured to be 50 Mbps which is low in intensity.

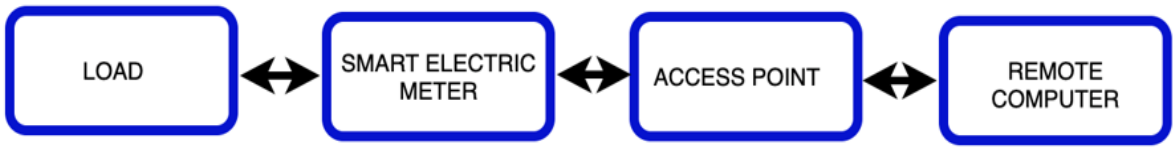


Figure 3.4: Experimental setup

### 3.3.3 Experiment III Under Regulated Attack for 15 Days

Again, we used two 200-Watt incandescent light bulbs for the smart meter. This was the baseline load (No attack). This baseline load was used for 15 days (360 hours) during which we collected power usage data remotely. This data is shown in column 2 of Table 3.3. This procedure was performed again with the presence of a ping based indirect cyber-attack. Again, the power usage data was recorded and shown in column 3 of Table 3.3. The Ping attack traffic was measured to be 50 Mbps which is also low in intensity.

### 3.3.4 Experiment IV Under Regulated Attack for 30 Days

Two 200-Watt incandescent light bulbs were used for the smart meter. This was the baseline load (No attack). This baseline load was used for 30 days (720 hours) during which we collected power usage data remotely. This data is shown in column 2 of Table 3.4. This procedure was performed again with the presence of a ping based indirect cyber-attack. Again, the power usage data was recorded and shown in column 3 of Table 3.4. The Ping attack traffic was measured to be 50 Mbps which is also low in intensity.

### 3.3.5 Experiment V Under Unregulated Attack

The next phase of our experiment on smart meters to use a direct cyber-attack on the smart meters. We first recorded data on a smart meter without an attack for an entire day. Then we recorded for another day, but this time, under the influence of a direct cyber-attack. Then we recorded for another day with the removal of the attack. The aim of this experiment was to check for connectivity issues the smart meter was experiencing while communicating data from the smart meter to the remote monitoring computer during the attack.

## 3.4 Experimental Results and Discussion

### 3.4.1 Results from Experiment I

It was observed that during the first 24 hours of the attack, there was no meaningful effect on the power usage data. However, post 24 hours, an obvious decline in the power usage data could be seen. In table 3.1, we see the average power consumption data for 96 hours which is shown as a running average power consumption after the first, second, third and fourth days in the third column of table 3.1.

| No of Days | Baseline-Average power consumption (In Watt-Hour) | Average Power consumption under attack (In Watt-Hour) | Percentage Power Loss |
|---|---|---|---|
| 1 | 203.32 | 203.09 | 0.1131 |
| 2 | 203.33 | 203.00 | 0.1623 |
| 3 | 203.23 | 202.70 | 0.2608 |
| 4 | 203.25 | 202.58 | 0.3296 |

Table 3.1

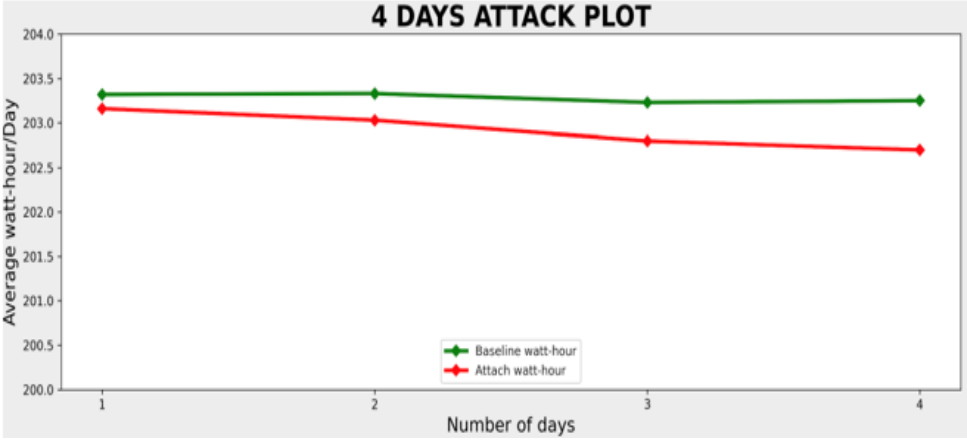


Figure 3.5: Attack Plot for 4 days.

The average power consumption measured in Watt-Hours for Experiment I without any cyber-attack is shown in green and the power consumption with cyber-attack is measured in red.

% Power Loss (After 4 days) =

$$\frac{Power\ consumption\ (Baseline) - Power\ consumption\ (Under\ Cyber-attack)}{Power\ consumption\ (Baseline)} \text{ x } 100$$

$$= \frac{203.25-202.58}{203.32}\ x\ 100$$

= 0.3296%

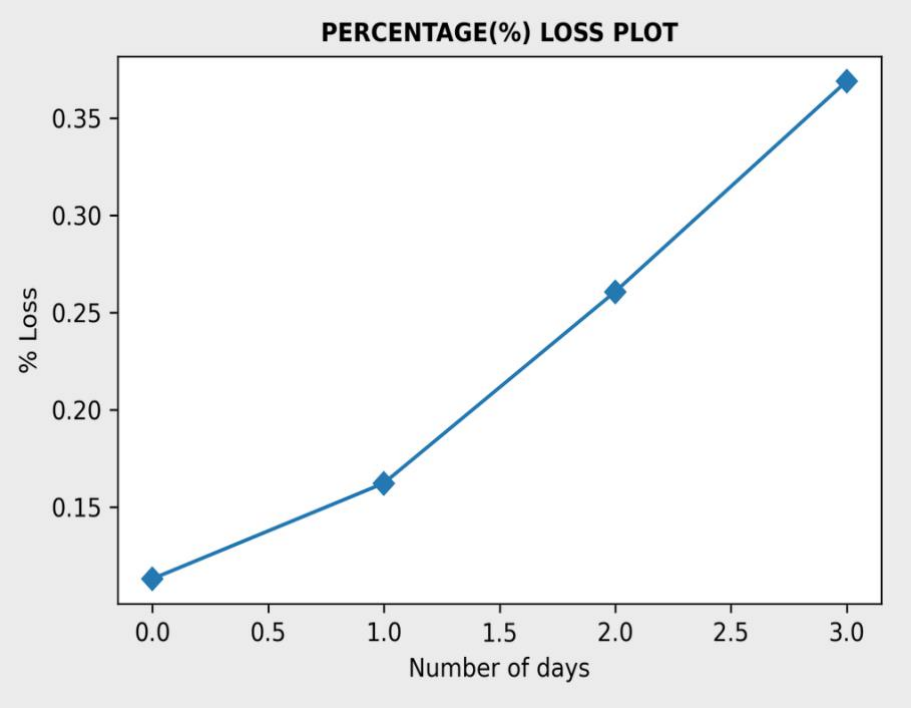


Figure 3.6: Percentage Power Loss Plot for Experiment I

From the power loss plot seen above, as the number of days increases, the percentage power loss increases which indicates that the loss suffered by electric power companies increases in magnitude if a cyber-attack is left unchecked.

In Experiment I, it could be seen that by the end of Day 4, the smart meter had recorded an overall power loss of 0.3296%. This was due to the attack on the smart meter. Also, when observing the power consumption for the baseline and the power consumption during the cyber-attack, a trend was noticeable and it showed a decline in the average power consumption recorded by the smart meter and sent to the remote monitoring computer. It is easy to think that the 0.3296% loss is negligible however that is not true as it would make a huge difference when it comes to deploying smart meters by a large electric company to large commercial organizations. An example to demonstrate this is shown below:

**Financial loss estimation due to the cyber-attack for a large electric company's deployment under experiment I setup.**

The point of this is to estimate how much a cyber-attack on smart meters affects the revenue of a large electric company if they use the type of smart meter suggested above.

It should be noted that some of the data used were Pacific Gas & Electric data obtained from [53] and the data can be seen below.

- Company Name: Pacific Gas & Electric
- Number of customers (Residential and Commercial): 5,069,189
- Overall monthly power consumption: 6,040,152,083 kWh
- Average price from [53] = 17.41 cents/kWh
- Loss of power due to security attack on Smart Meter = 1,990,834,126 kWh/month (using our 0.3296% power loss)
- Overall revenue loss because of cyber-attacks on smart meter = $346,604,221 Million/month.

### 3.4.2 Result from Experiment II

We saw that during the first 24 hours of the attack, there was no particularly meaningful impact on the power usage reading but after the first 24 hours, the smart meter showed that power consumption was declining. The table 3.2 below shows the power consumption data for 7 days (From the 1$^{st}$ day to the 7$^{th}$ day).

**Average power consumption with and without the cyber-attack on the Smart Meter measured for 7 days.**

| No of Days | Baseline Average Power consumption (In Watt-Hour) | Average Power consumption under attack (In Watt-Hour) | Percentage Power loss |
|---|---|---|---|
| 1 | 203.32 | 203.09 | 0.1131 |
| 2 | 203.33 | 203.00 | 0.1623 |
| 3 | 203.23 | 202.70 | 0.2608 |
| 4 | 203.25 | 202.58 | 0.3296 |
| 5 | 203.24 | 202.25 | 0.4871 |
| 6 | 203.28 | 202.04 | 0.6100 |
| 7 | 203.26 | 201.68 | 0.7773 |

Table 3.2

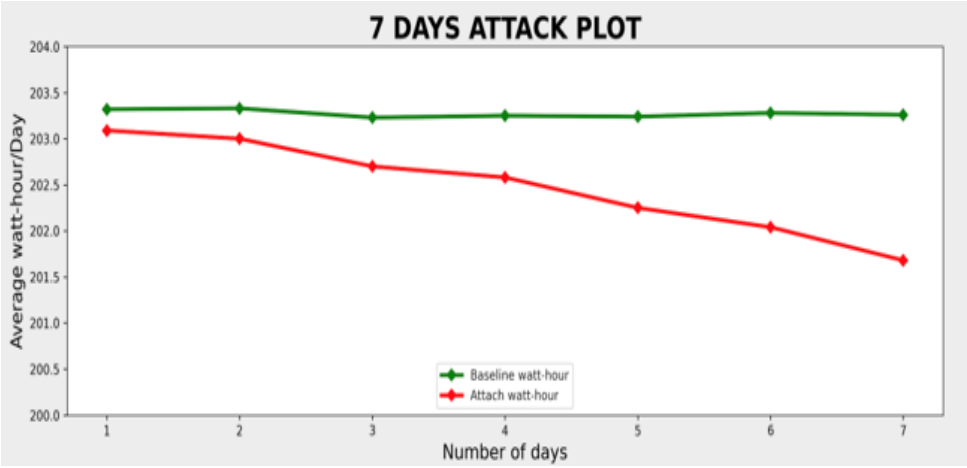


Figure 3.7: Attack Plot for 7 days

The average power consumption measured in Watt-Hours for Experiment II without any cyber-attack is shown in green and the power consumption with an indirect cyber-attack is measured in red.

**Loss of Power recorded (during the cyber-attack)**

$$\% \text{ Loss of Power after 7 days} = \frac{Power\ consumption\ (Baseline) - Power\ consumption\ (Under\ cyber\ attack)}{Power\ consumption\ (Baseline)}$$

$$= \frac{203.26 - 201.68}{203.26} x\ 100$$

$$= 0.7773\%$$

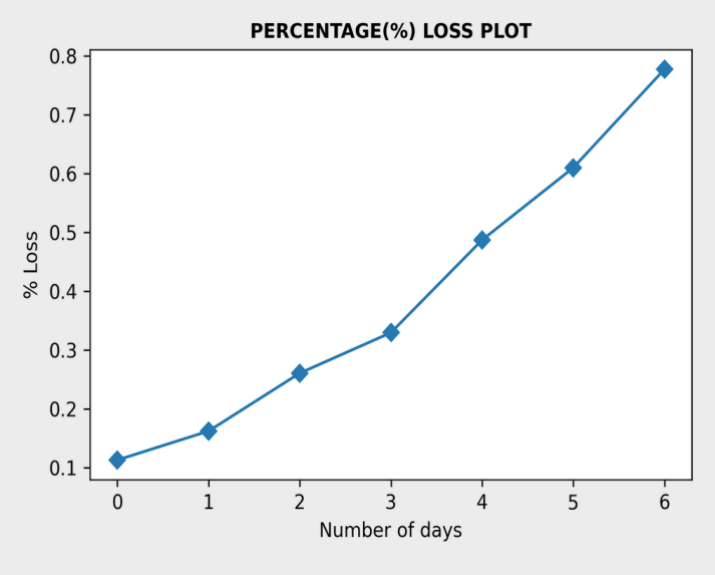


Figure 3.8: Percentage Loss Plot for Experiment II

In the Percentage loss plot shown above, the power consumption loss increased linearly in the first 24 hours although it was minimal. During the remaining six days, the power loss increased exponentially from 0.2% to 1.0%.

In Experiment II, it could be seen that by the end of Day 7, the smart meter had recorded an overall power loss of 0.77%. This was due to the attack on the smart meter. Also, when observing the power consumption for the baseline and the power consumption during the cyber-attack, a trend was noticeable and it showed a decline in the average power consumption recorded by the smart meter and sent to the remote monitoring computer. It is easy to think that the 0.77% loss is negligible however that is not true as it would make a huge difference when it comes to deploying smart meters by a large electric company to large commercial organizations. An example to demonstrate this is shown below:

**Financial loss estimation due to the cyber-attack for a large electric company's deployment under experiment II setup.**

The point of this is to estimate how much a cyber-attack on smart meters affects the revenue of a large electric company if they use the type of smart meter suggested above.

It should be noted that some of the data used were Pacific Gas & Electric data obtained from [53] and the data can be seen below.

- Company Name: Pacific Gas & Electric
- Number of customers (Residential and Commercial): 5,069,189
- Overall monthly power consumption: 6,040,152,083 kWh
- Average price from [53] = 17.41 cents/kWh
- Loss of power due to security attack on Smart Meter = 4,695,010,214 kWh/month (using our 0.77% power loss)
- Overall revenue loss because of cyber-attacks on smart meter = $817,401,278 Million/month.

### 3.4.3 Result for Experiment III

From figure 2.11, we saw that during the first 24 hours of the attack, there was no particularly meaningful impact on the power usage reading but after the first 24 hours, the smart meter showed that power consumption started rapidly declining. The table 3.3 below shows the power consumption data for 15 days (From the 1st day to the 15th day).

**Average power consumption with and without the cyber-attack on the Smart Meter measured for 7 days.**

| No of Days | Baseline Average Power consumption (In Watt-Hour) | Average Power consumption under attack (In Watt-Hour) | Percentage Power loss |
|---|---|---|---|
| 1 | 203.32 | 203.09 | 0.1131 |
| 2 | 203.33 | 203.00 | 0.1623 |
| 3 | 203.23 | 202.70 | 0.2608 |
| 4 | 203.25 | 202.58 | 0.3296 |
| 5 | 203.24 | 202.25 | 0.4871 |
| 6 | 203.28 | 202.04 | 0.6100 |
| 7 | 203.26 | 201.68 | 0.7773 |
| 8 | 203.23 | 201.20 | 0.9989 |
| 9 | 203.16 | 200.75 | 1.1863 |
| 10 | 203.35 | 200.45 | 1.4261 |
| 11 | 203.25 | 200.05 | 1.5744 |

| | | | |
|---|---|---|---|
| 12 | 203.26 | 199.80 | 1.7023 |
| 13 | 203.28 | 199.49 | 1.8644 |
| 14 | 203.29 | 199.42 | 1.9037 |
| 15 | 203.31 | 199.42 | 1.9133 |

Table 3.3

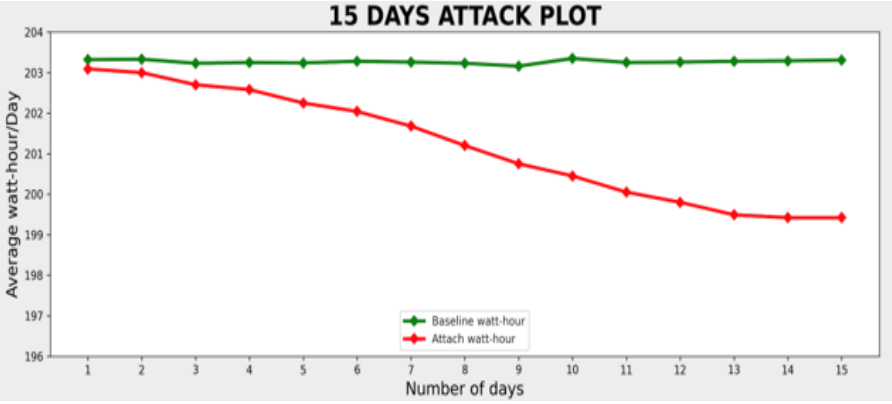


Figure 3.9: 15 Days Attack Plot

The average power consumption measured in Watt-Hours for Experiment III without any cyber-attack is shown in green and the power consumption with an indirect cyber-attack is measured in red.

**Loss of Power recorded (during the cyber-attack)**

% Loss of Power after 15 days =

$$\frac{Power\ consumption\ (Baseline) - Power\ consumption\ (Under\ cyber\ attack)}{Power\ consumption\ (Baseline)}$$

$$= \frac{203.31 - 199.42}{203.31} x\ 100$$

$$= 1.9133\%$$

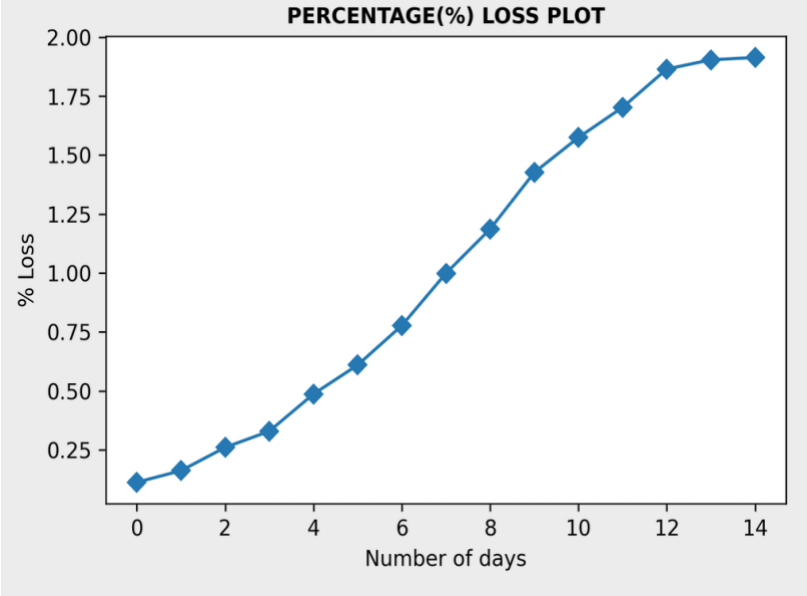


Figure 3.10: Percentage loss plot for Experiment III

In the Percentage loss plot shown above, the power consumption loss increased linearly in the first 24 hours although it was minimal. During the next six days, the power loss increased exponentially from 0.2% to approximately 1.1%. Over the remaining 8 days, the percentage loss kept increasing till it reached 1.6%

In Experiment III, it could be seen that by the end of Day 15, the smart meter had recorded an overall power loss of 1.91%. This was due to the attack on the smart meter. Also, when observing the power consumption for the baseline and the power consumption during the cyber-attack, a trend was noticeable and it showed a decline in the average power consumption recorded by the smart meter and sent to the remote monitoring computer. It is easy to think that the 1.91% loss is negligible however that is not true as it would make a huge difference when it comes to deploying smart meters by a large electric company to large commercial organizations. An example to demonstrate this is shown below:

**Financial loss estimation due to the cyber-attack for a large electric company's deployment under experiment III setup.**

The point of this is to estimate how much a cyber-attack on smart meters affects the revenue of a large electric company if they use the type of smart meter suggested above.

It should be noted that some of the data used were Pacific Gas & Electric data obtained from [53] and the data can be seen below.

- Company Name: Pacific Gas & Electric
- Number of customers (Residential and Commercial): 5,069,189
- Overall monthly power consumption: 6,040,152,083 kWh
- Average price from [53] = 17.41 cents/kWh
- Loss of power due to security attack on Smart Meter = 11,556,622,980 kWh/month (using our 1.91% power loss)
- Overall revenue loss because of cyber-attacks on smart meter = $2,012,008,060 Million/month.

### 3.4.4 Result for Experiment IV

During the first 24 hours of the attack, there was no particularly meaningful impact on the power usage reading but after the first 24 hours, the smart meter showed that power consumption started rapidly declining. The table 3.4 below shows the power consumption data for 30 days (From the 1$^{st}$ day to the 30$^{th}$ day).

**Average power consumption with and without the cyber-attack on the Smart Meter measured for 7 days.**

| No of Days | Baseline Average Power consumption (In Watt-Hour) | Average Power consumption under attack (In Watt-Hour) | Percentage Power loss |
|---|---|---|---|
| 1 | 203.32 | 203.09 | 0.1131 |
| 2 | 203.33 | 203.00 | 0.1623 |
| 3 | 203.23 | 202.70 | 0.2608 |
| 4 | 203.25 | 202.58 | 0.3296 |
| 5 | 203.24 | 202.25 | 0.4871 |
| 6 | 203.28 | 202.04 | 0.6100 |
| 7 | 203.26 | 201.68 | 0.7773 |
| 8 | 203.23 | 201.20 | 0.9989 |
| 9 | 203.16 | 200.75 | 1.1863 |
| 10 | 203.35 | 200.45 | 1.4261 |
| 11 | 203.25 | 200.05 | 1.5744 |
| 12 | 203.26 | 199.80 | 1.7023 |
| 13 | 203.28 | 199.49 | 1.8644 |
| 14 | 203.29 | 199.42 | 1.9037 |
| 15 | 203.31 | 199.42 | 1.9133 |
| 16 | 203.30 | 199.31 | 1.9626 |
| 17 | 203.29 | 199.23 | 1.9971 |

| | | | |
|---|---|---|---|
| 18 | 203.30 | 198.72 | 2.2528 |
| 19 | 203.22 | 198.43 | 2.3571 |
| 20 | 203.30 | 198.41 | 2.4053 |
| 21 | 203.28 | 198.31 | 2.4449 |
| 22 | 203.28 | 198.31 | 2.4449 |
| 23 | 203.25 | 198.22 | 2.4748 |
| 24 | 203.26 | 198.22 | 2.4796 |
| 25 | 203.27 | 198.23 | 2.4795 |
| 26 | 203.16 | 197.90 | 2.5891 |
| 27 | 203.15 | 197.77 | 2.6483 |
| 28 | 203.01 | 197.60 | 2.6649 |
| 29 | 203.00 | 197.51 | 2.7044 |
| 30 | 203.98 | 197.47 | 2.7146 |
| 31 | 203.90 | 200.45 | 1.2075 |

Table 3.4

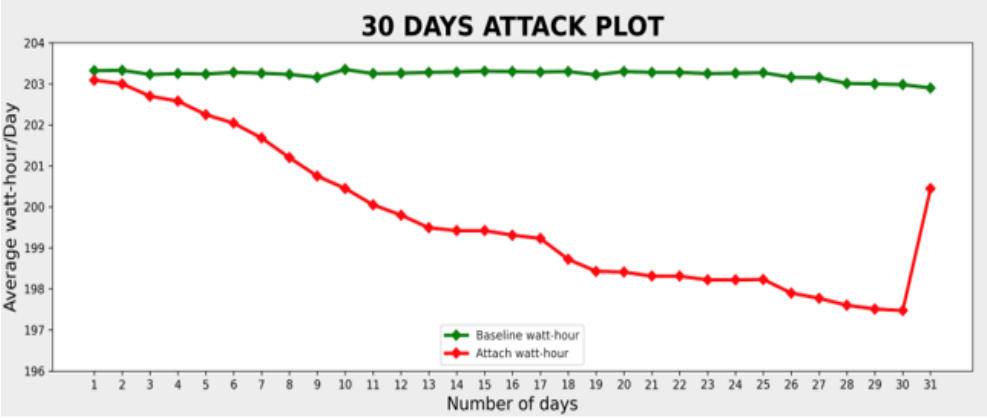


Figure 3.11: 30 Days Attack Plot

The average power consumption measured in Watt-Hours for Experiment IV without any cyber-attack is shown in green and the power consumption with an indirect cyber-attack is measured in red.

**Loss of Power recorded (during the cyber-attack)**

$$\% \text{ Loss of Power after 7 days} = \frac{Power\ consumption\ (Baseline) - Power\ consumption\ (Under\ cyber\ attack)}{Power\ consumption\ (Baseline)}$$

$$= \frac{203.90 - 200.45}{203.90} x\ 100$$

$$= 1.2075\%$$

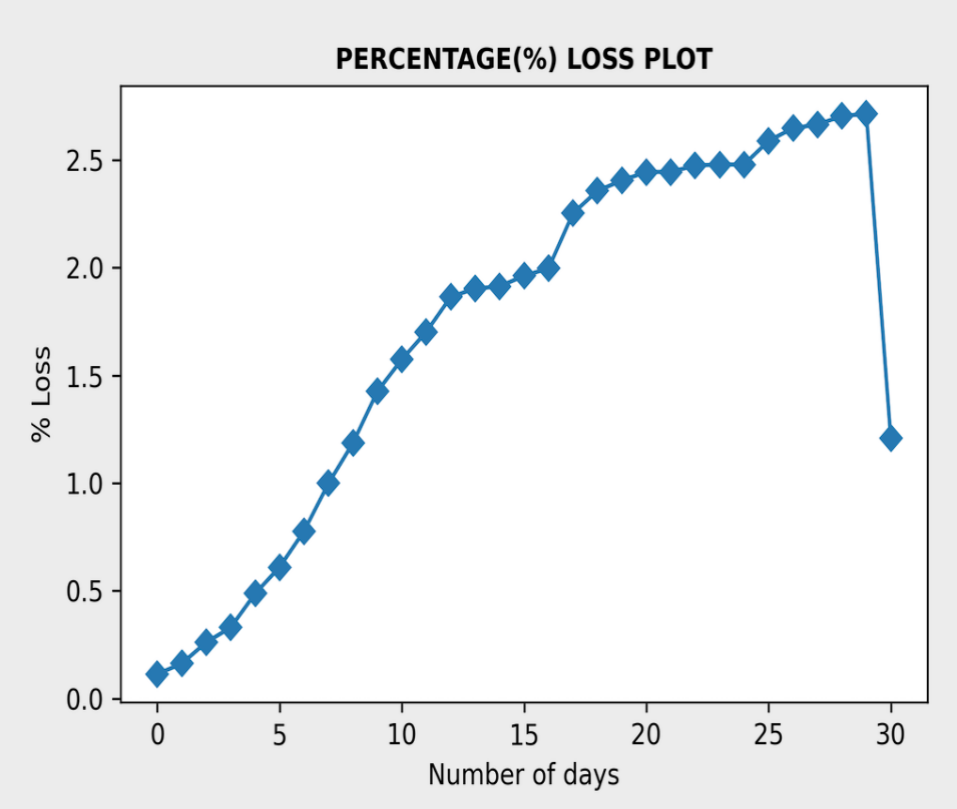


Figure 3.12: Percentage Loss Plot for Experiment IV

In the Percentage loss plot shown above, the power consumption loss increased linearly in the first 24 hours although it was minimal. During the next six days, the power loss increased exponentially from 0.2% to approximately 1.1%. Over the following 8 days, the percentage loss kept increasing till it reached 1.6% before it took another sharp increase over the 14 days to peak at approximately 3.4%. On the last day, this loss dropped sharply after the attack was removed.

In Experiment IV, it could be seen that by the end of Day 31, the smart meter had recorded an overall power loss of 1.2075%. This was due to the attack on the smart meter. Also, when observing the power consumption for the baseline and the power consumption during the cyber-attack, a trend was noticeable and it showed a decline in the average power consumption recorded by the smart meter and sent to the remote monitoring computer. It is easy to think that the 1.2075% loss is negligible however that is not true as it would make a huge difference when it comes to deploying smart meters by a large electric company to large commercial organizations. An example to demonstrate this is shown below:

**Financial loss estimation due to the cyber-attack for a large electric company's deployment under experiment IV setup.**

The point of this is to estimate how much a cyber-attack on smart meters affects the revenue of a large electric company if they use the type of smart meter suggested above.

It should be noted that some of the data used were Pacific Gas & Electric data obtained from [53] and the data can be seen below.

- Company Name: Pacific Gas & Electric
- Number of customers (Residential and Commercial): 5,069,189
- Overall monthly power consumption: 6,040,152,083 kWh

- Average price from [53] = 17.41 cents/kWh
- Loss of power due to security attack on Smart Meter = 7,293,483,640 kWh/month (using our 1.2075% power loss)
- Overall revenue loss because of cyber-attacks on smart meter = $1,269,795,501 Million/month.

What these experiments have demonstrated is that cyber-attacks can have a damaging effect on the operation of smart meters and this can have a ripple effect on the finances of large electric companies as they could suffer heavy losses due to cyber-attacks

## 3.5 Chapter Summary

In this chapter, we performed both direct and indirect cyber-attacks on the EPM 6100 Smart electric meter from General Electric in a bid to understand and evaluate the effects of these attacks on the operation of the smart meter and how data traffic moves between the smart meter and a remote monitoring computer. It is known that smart meters are very useful for customers and especially utilities particularly when we consider how they implement their smart grid infrastructure and provide consistent power assessment and problem troubleshooting.

These experiments shaded light on the effect of these attacks. We found out that even an indirect ping-based attack can have a very large impact on a smart meter operation especially for large electric companies. When we did the indirect cyber-attack 30-Day experiment, we noticed that on the first day, the impact was minimal but at the end of the entire billing cycle, the impact had become significant.

For the direct attacks, we could see an immediate impact as there was a total loss of data communication between the smart meter and the remote monitoring computer. In any of these two cases, whether direct or indirect, the one constant thing is that these attacks can lead to big financial losses in millions of dollars for electric companies, especially the ones that focus on large scale smart grid infrastructure.

# CHAPTER IV

## WIRELESS CONNECTIVITY TEST OF EMP 6100, EPM 7000 AND E650 SMART METERS UNDER DIFFERENT TYPES OF CYBERSECURITY ATTACKS

Ensuring that smart meters are always connected to nodes is a very important process of ensuring reliability in electric utility companies. If a smart meter is to relay consumption related information for billing purposes, network providers need to understand the response of smart meters to unexpected cybersecurity attacks such as a DDOS attack. For energy consumption to be sequence and analyzed, AMI systems need to maintain a bidirectional communication between the devices concerned. Therefore, this chapter evaluates the connectivity of smart electric meters when exposed to malicious cybersecurity attacks.

We performed a series of experiments using a software provided by a utility company to the networking lab of University of Texas Rio Grande Valley (UTRGV). In summary, the aim of this chapter is to analyze the connectivity of a smart meter provided to us by a utility company. We aim to provide a recommendation for the company based of the vulnerability we observed during the experiment.

## 4.1 Experimental Setup

In this experiment, we utilized three different smart meters i.e. EPM6100, EPM7000, and E650 smart meters. We did not used any load because we are not interested in the consumption, instead we are interested in the connectivity of the smart meters. Given that most of the smart meters are designed to be connected using ethernet cable, we used 2 wireless access points to bridge the communication between the attacking computer, remote monitoring computer, and the smart meters. Using that we were able to direct attack traffic from the attack computer to the smart meter. A close observation of the experimental setup as shown in(fig 4.1) shows how the Ethernet cables from the attack computer was connected to the wireless access point. Also, from the second wireless access point, it can be observed how the three smart meters were connected to the wireless access point using three Ethernet cables. Since the remote monitoring computer is WIFI enabled, there was no need to connect it to the wireless access point using an Ethernet cable, instead the WIFI feature of the computer was enabled and configured to communicate with the wireless access point.

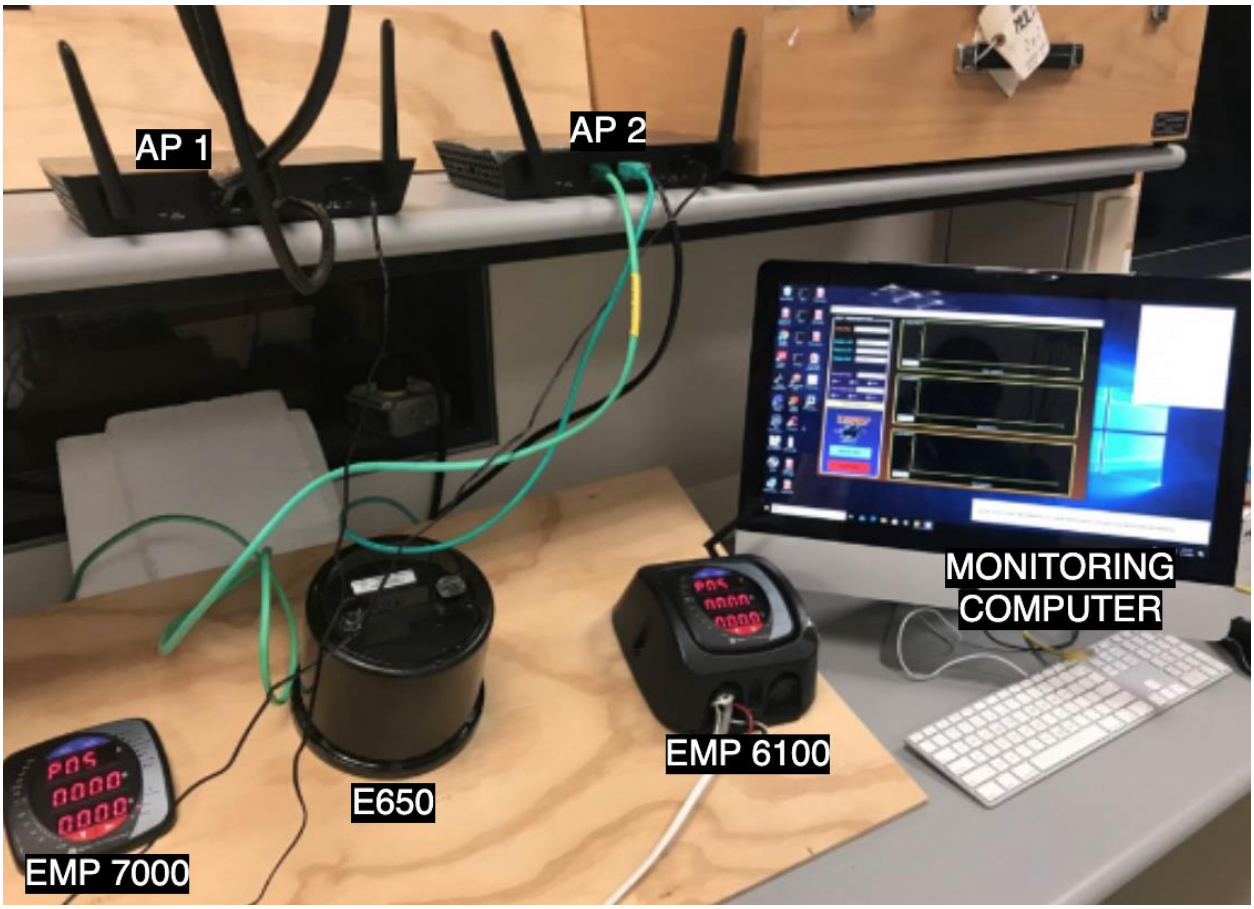


Figure 4.1: Lab experimental setup for evaluating EPM6100, EPM700 and E650 Electric smart meters.

Each and every device connected to the setup shown above was assigned a unique IP address that corresponds to the network it belongs. The wireless access point works by connecting directly to the devices an exchanging protocol information. It then transmits and receives a wireless signal in either the 2.4Ghz or 5Ghz frequency range (WIFI).This in turn allows connection to other wireless devices and other connected wireless devices to a Local Area Network (LAN) or the internet. The wireless access point is used to enable an attack on the communication lines of the smart meter. While there are so many types of attacks that can be used for this, in this experiment, we used the ping, smurf and the TCP/SYN because they are part of the most practical attacks used today by attackers. To create an environment for this, we used

an attacking computer that generates the attack, this acts as the “bad guy” who wants to disconnect the communication links using DDos attacks. Haven established that cyber security attacks has an effect on the communication between the meter and the remote monitoring device, we move further to determine the minimum bandwidth of cyber-attack required to terminate the communication. Also, we observed how long it took the smart meter to reestablish connection when completely disconnected. We also checked for information availability in the recording computer, the aim is to determine if the remote monitoring computers was able to access all the consumption information communicated by the smart meter.

### 4.2 Smart Meter Overseer (SMO)

To accurately determine the connection and disconnection time of the smart meter, a special software know as Smart Meter Overseer was used. The Smart Meter Overseer does not record the watthour consumption of the smart meter, instead it focuses on the connectivity state of all the smart meter connected to it. The Smart Meter Overseer is very efficient because it simultaneously give the connectivity plots of all the smart meters it is connected to. A close observation of the sample output of the smart meter overseer meter show below(fig 5.3) shows how it was able to simultaneously display the connectivity status of the three smart meters connected to it. The science behind this application relies in the phenomena that occurs when a smart meter is under attack. If a smart meter works under normal conditions, the monitoring computer can ensure communication by sending a single ping request. If the smart meter replies with a ping response, then the communication between the monitoring computer and the smart meter is active. If the smart meter does not send the ping response, it means that there is a problem in communication. When meters are under attack, there is no communication, and any

ping request initiated by the monitoring computer results in a timeout, therefore the communication is termed inactive. SM overseer allows the user to make readings in any size of time, and it achieves this by sending ping requests to the smart meter. The readings samples were able to be done from even less than a second, up to any value the user could come up to. SM Overseer could reveal us the communication status of the smart meter with high reliability and precision.

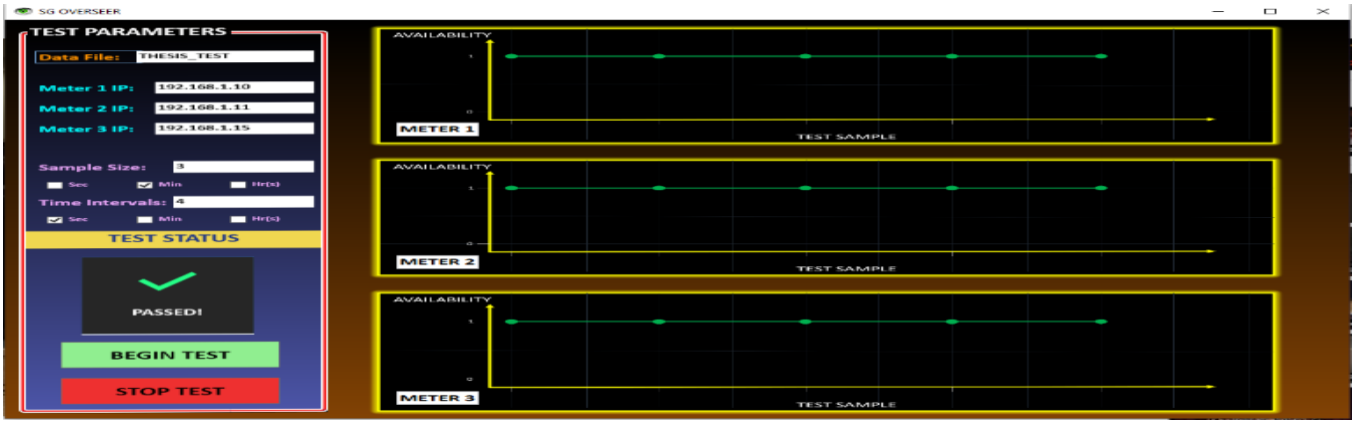


Figure 4.2: SM Overseer Software for checking connectivity status of meters

### 4.3 Experimental Results and Discussion from EPM 6100 Smart Electric Meter

To determine the connectivity of EPM 6100 smart meter, a couple of experiment was conducted. In the past, common DDoS attacks come in the form of sustained, high-volume traffic floods that gradually increases, reach a peak, and then followed by a sudden or a slow descent. Nowadays, a new attack pattern known as bursts attacks or hit-and-run attacks have emerged. This type of attack use repeated short bursts of high intensity attacks at unpredictable intervals. A burst can last for as little as 2 seconds while a more malicious attack can span for hours non-stop, sending hundreds of gigabits per second of packets to a victim. In this experiment, we measured the effect of this two types of attack and noted the different impact it

has on EPM 6100. The maximum  bandwidth capacity of ethernet cable used for this experiment is 100 Mbps which is the standard capacity of a regular CAT 5 cable. The Attacker computer has maximum capacity to send flooding traffic at the rate of 1Gbps . Therefore10% of the total flooding capacity of the attack computer was used for the experiment. Figure(5.3) shows the lab setup diagram for the evaluation of EPM6100.

### 4.3.1 Experimental result of connectivity test of EMP 6100 Power Quality Meter Under Different cyber attacks

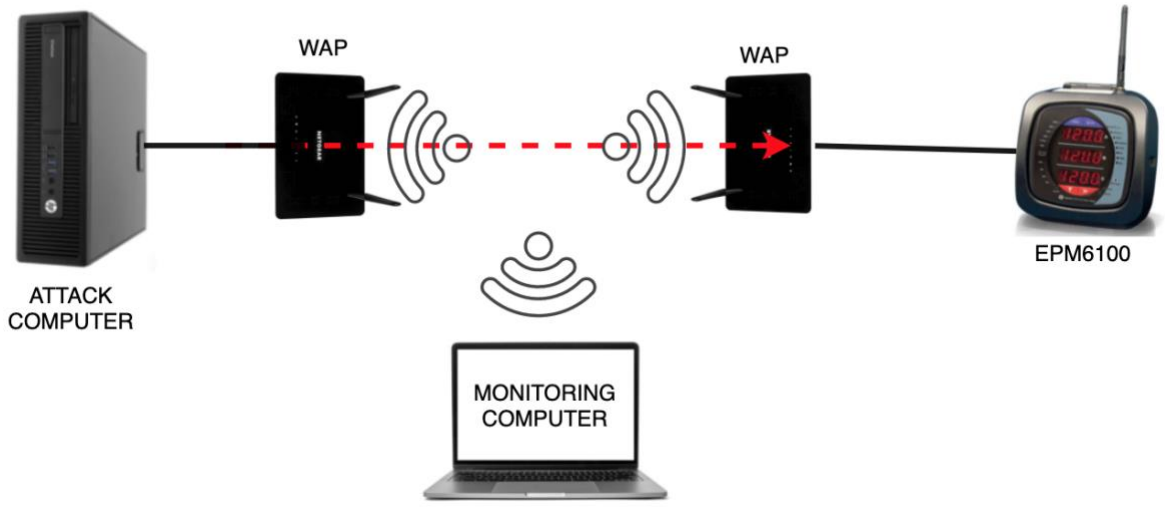


Figure 4.3: Lab experiment setup for evaluating EPM 6100 connectivity.

After the experiment, the connectivity information was summarized in Table 5.1 as shown below. The term minimum effect means the minimum Mbps bandwidth we started noticing a fluctuating in the connectivity while the term disconnection means the Mbps bandwidth at which communication was completely lost.

**Table 4.1: Experiment Result of Performance of smart Metering Data Communication for EPM 6100 Power Quality Smart Quality Smart Electric Meter Under Different Cyber-Attacks.**

| DESCRIPTION. | PING | SMURF | TCP/SYN |
|---|---|---|---|
| Minimum effect burst attack bandwidth (Mbps) | 0.3 | 1.0 | 2 |
| Disconnection burst attack bandwidth (Mbps) | 2.0 | 3.0 | 5.0 |
| Minimum effect continuous attack bandwidth (Mbps) | 0.5 | 1.7 | 4 |
| Disconnection continuous attack bandwidth (Mbps) | 3.0 | 5.0 | 1000 |
| Time to disconnect (seconds) | 1.0 | 1.0 | 1.0 |
| Time to reconnect (seconds) | 2.0 | 2.0 | 2.0 |

### 4.3.2 Experimental Result Under PING.

While evaluating EPM 6100 under a burst and continuous PING attack we observed that for burst attack the minimum effective bandwidth was 0.3Mbps while the disconnection bandwidth was 2.0Mbps as show in fig (5.4). For continuous attack, we observed that the Minimum effective bandwidth was 0.5Mbps while the disconnection bandwidth was 3.0Mbps as shown in fig (5.5). We also recorded that the time taken to disconnect and reconnect were 1 seconds and 2 seconds respectively as shown in fig (5.6).

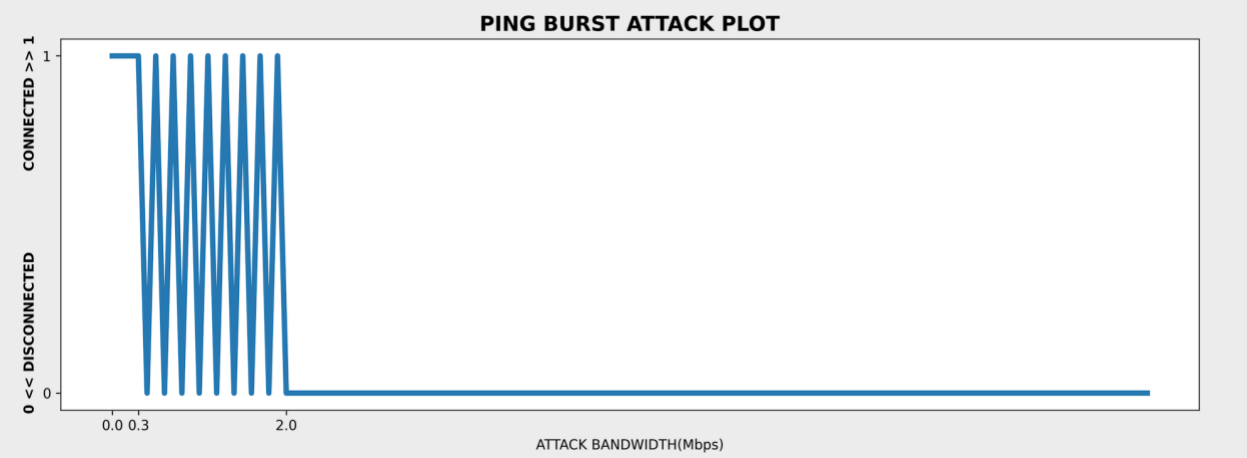


Figure 4.4: Observation of ping burst attack on EPM6100

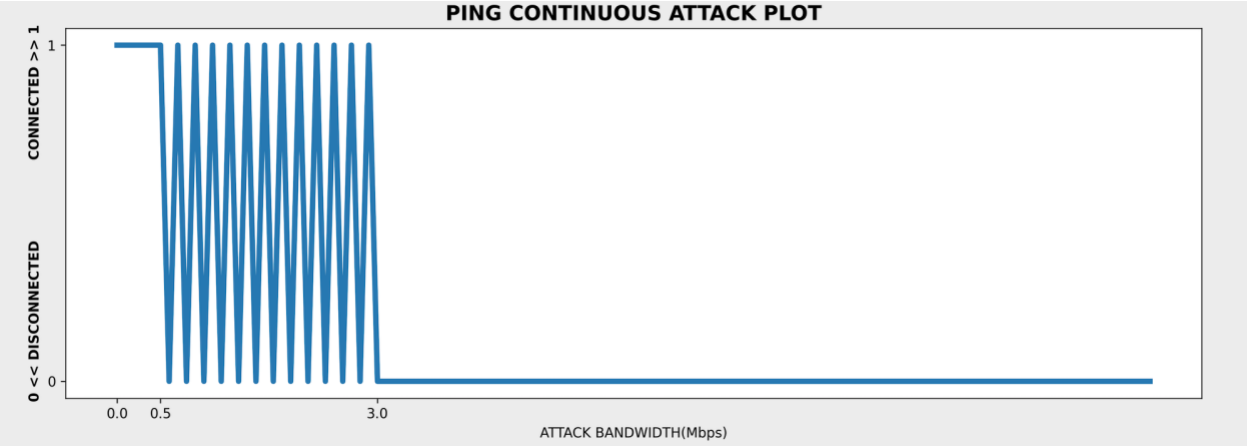


Figure 4.5: Observation of continuous ping attack on EPM6100

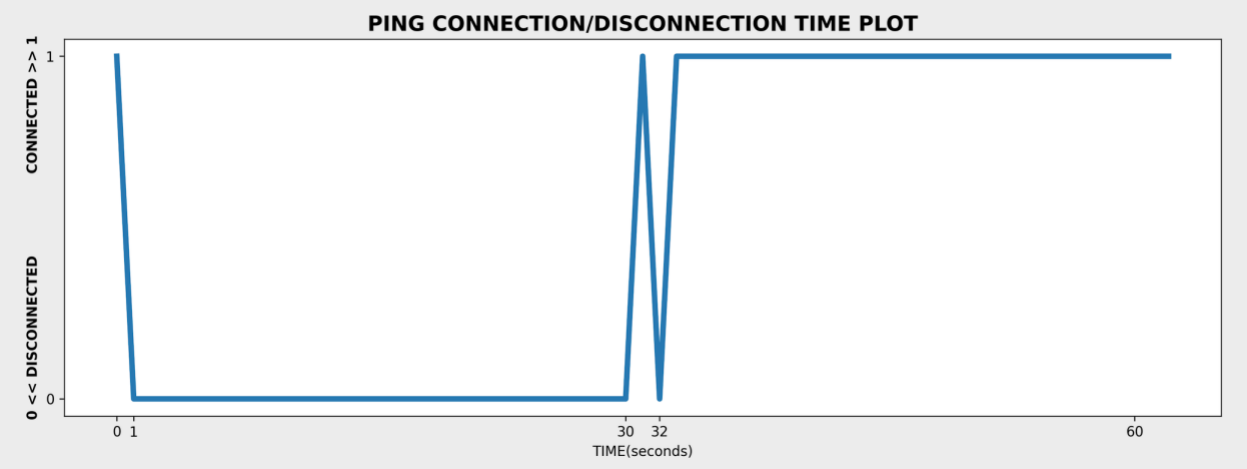


Figure 4.6: Observation of connection/disconnection time on EPM6100

### 4.3.3 Experimental Result Under SMURF

While evaluating EPM 6100 under a burst and continuous SMURF attack we observed that for burst attack the minimum effective bandwidth was 1.0Mbps while the disconnection bandwidth was 3.0Mbps as show in fig (5.7). For continuous attack, we observed that the Minimum effective bandwidth was 1.7Mbps while the disconnection bandwidth was 5.0Mbps as shown in fig (5.8). We also recorded that the time taken to disconnect and reconnect were 1 seconds and 2 seconds respectively as shown in fig (5.9).

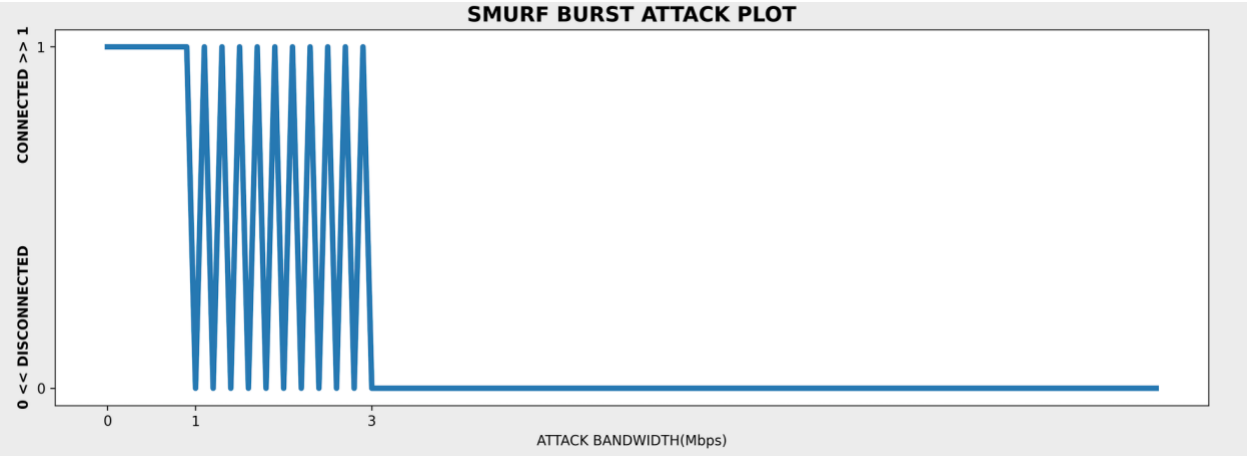


Figure 4.7: Observation of SMURF burst attack on EPM610

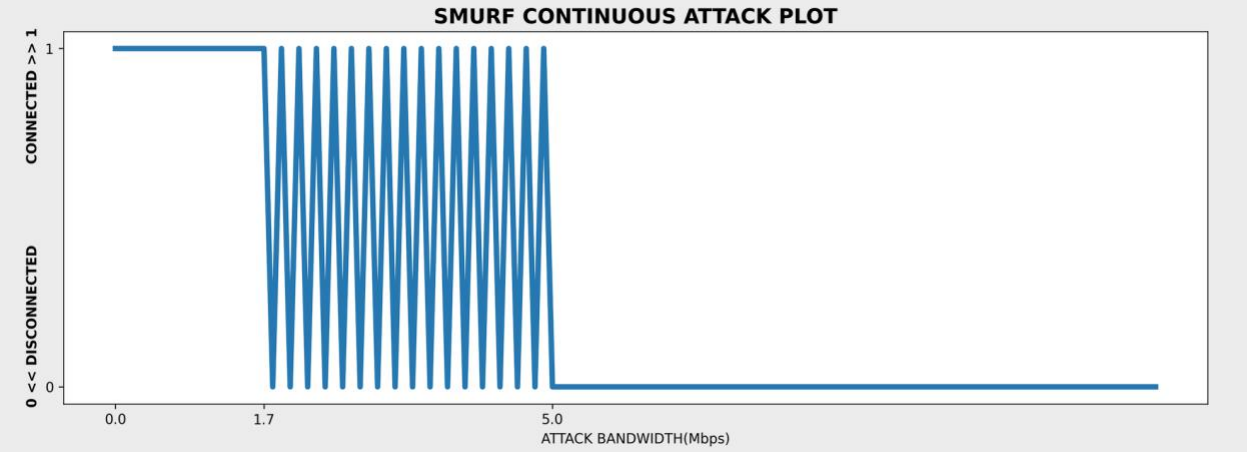


Figure 4.8: Observation of continuous SMURF attack on EPM6100

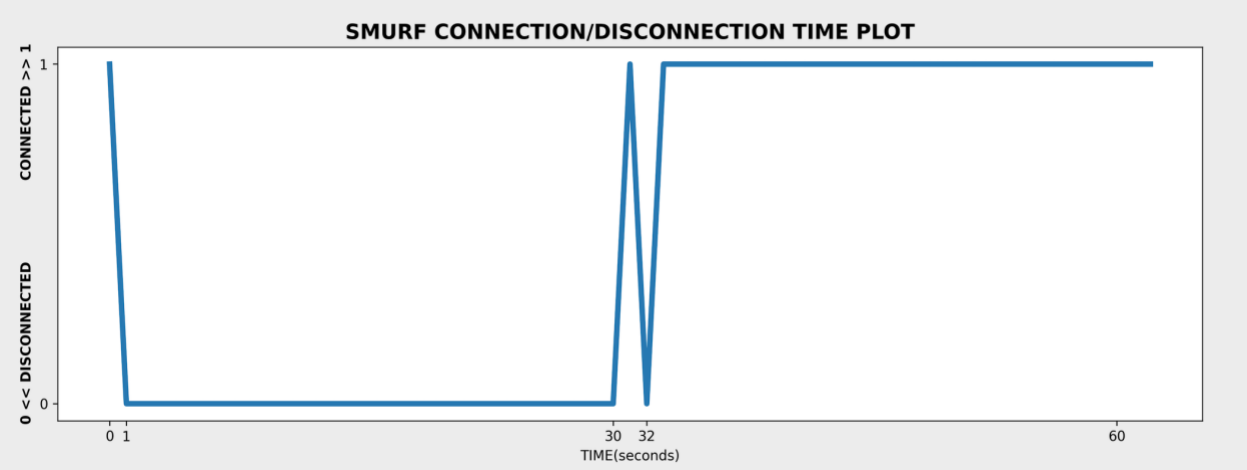


Figure 4.9: Observation of connection/disconnection time on EPM6100

### 4.3.4 Experimental Result Under TCP/SYN

While evaluating EPM 6100 under a burst and continuous TCP/SYN attack we observed that for burst attack the minimum effective bandwidth was 2.0Mbps while the disconnection bandwidth was 5.0Mbps as show in fig (5.10). For continuous attack, we observed that the Minimum effective bandwidth was 4.0Mbps while the meter never total disconnected as shown in fig (5.11). We also recorded that the time taken to disconnect and reconnect were 1 seconds and 2 seconds respectively as shown in fig (5.12).

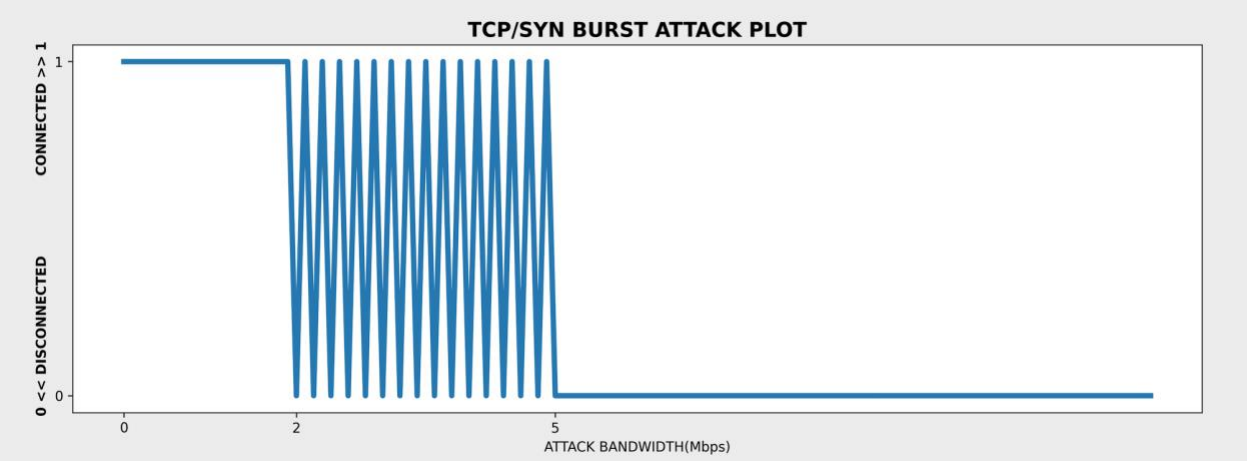


Figure 4.10: Observation of TCP/SYN burst attack on EPM6100

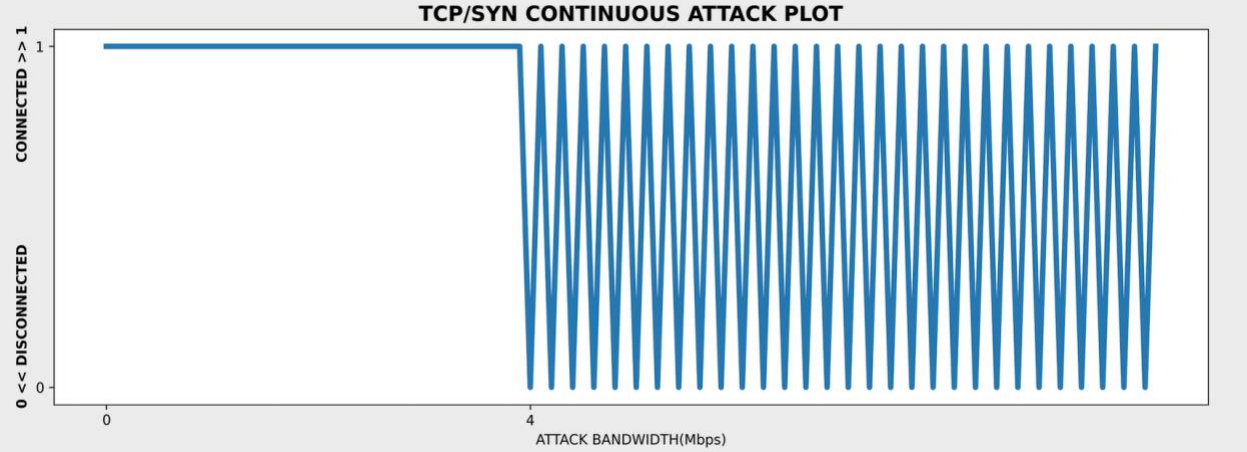


Figure 4.11: Observation of continuous TCP/SYN attack on EPM6100

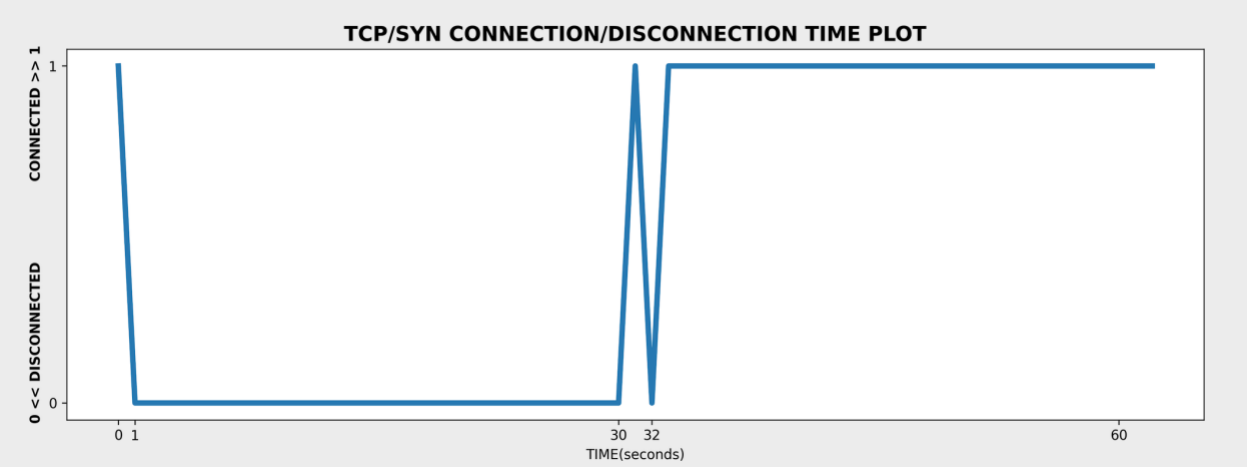


Figure 4.12: Observation of connection/disconnection time on EPM6100

### 4.4 Experimental Results and Discussion from EPM 7000 Smart Electric Meter

To determine the connectivity of EPM 7000 smart meter, a couple of experiment was conducted. In the past, common DDoS attacks come in the form of sustained, high-volume traffic floods that gradually increases, reach a peak, and then followed by a sudden or a slow descent. Nowadays, a new attack pattern known as bursts attacks or hit-and-run attacks have emerged. This type of attack use repeated short bursts of high intensity attacks at unpredictable intervals. A burst can last for as little as 2 seconds while a more malicious attack can span for hours non-stop, sending hundreds of gigabits per second of packets to a victim. In this experiment, we measured the effect of this two types of attack and noted the different impact it has on EPM 7000. The maximum  bandwidth capacity of ethernet cable used for this experiment is 100 Mbps which is the standard capacity of a regular CAT 5 cable. The Attacker computer has maximum capacity to send flooding traffic at the rate of 1Gbps . Therefore10% of the total flooding capacity of the attack computer was used for the experiment. Figure(5.3) shows the lab setup diagram for the evaluation of 7000.

### 4.4.1 Experimental result of connectivity test of EMP 7000 Power Quality Meter Under Different cyber attacks

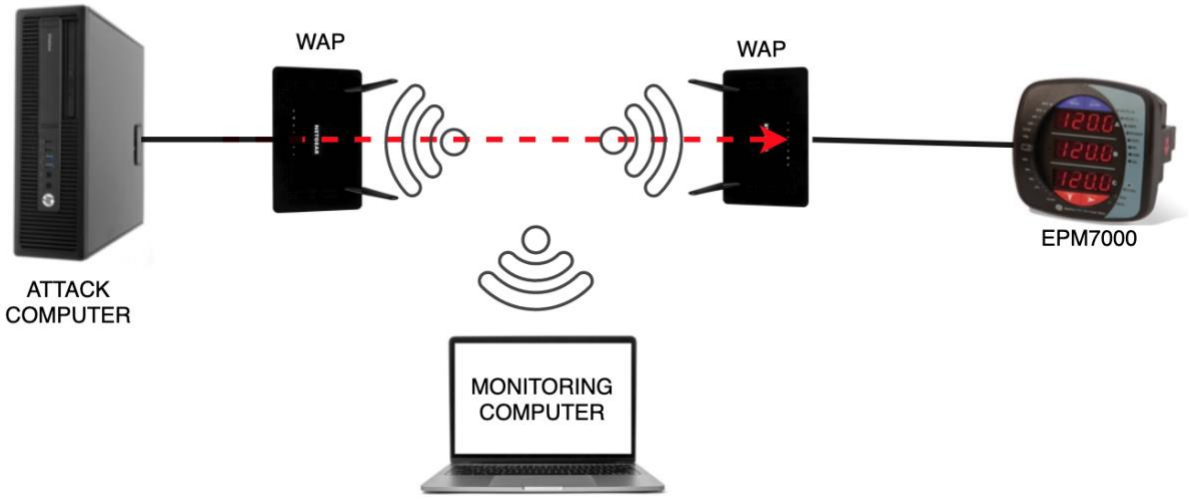


Figure 4.13: Lab experiment setup for evaluating EPM 7000 connectivity.

After the experiment, the connectivity information was summarized in Table 5.2 as shown below. The term minimum effect means the minimum Mbps bandwidth we started noticing a fluctuating in the connectivity while the term disconnection means the Mbps bandwidth at which communication was completely lost.

**Table 4.2: Experiment Result of Performance of smart Metering Data Communication for EPM 7000 Power Quality Smart Quality Smart Electric Meter Under Different Cyber-Attacks.**

| DESCRIPTION | PING | SMURF | TCP/SYN |
|---|---|---|---|
| Minimum effect burst attack bandwidth (Mbps) | 0.5 | 2.0 | 5.0 |
| Disconnection burst attack bandwidth (Mbps) | 3.0 | 5.0 | 11 |
| Minimum effect continuous attack bandwidth (Mbps) | 0.7 | 0.5 | 5.0 |
| Disconnection continuous attack bandwidth (Mbps) | 4.0 | 1000 | 1000 |
| Time to disconnect (seconds) | 1.0 | 1.0 | 1.0 |
| Time to reconnect (seconds) | 1.0 | 1.0 | 1.0 |

### 4.4.2 Experimental Result Under PING.

While evaluating EPM 7000 under a burst and continuous PING attack we observed that for burst attack the minimum effective bandwidth was 0.5Mbps while the disconnection bandwidth was 3.0Mbps as show in fig (5.14). For continuous attack, we observed that the Minimum effective bandwidth was 0.7Mbps while the disconnection bandwidth was 4.0Mbps as shown in fig (5.15). We also recorded that the time taken to disconnect and reconnect were both 1 seconds as shown in fig (5.16).

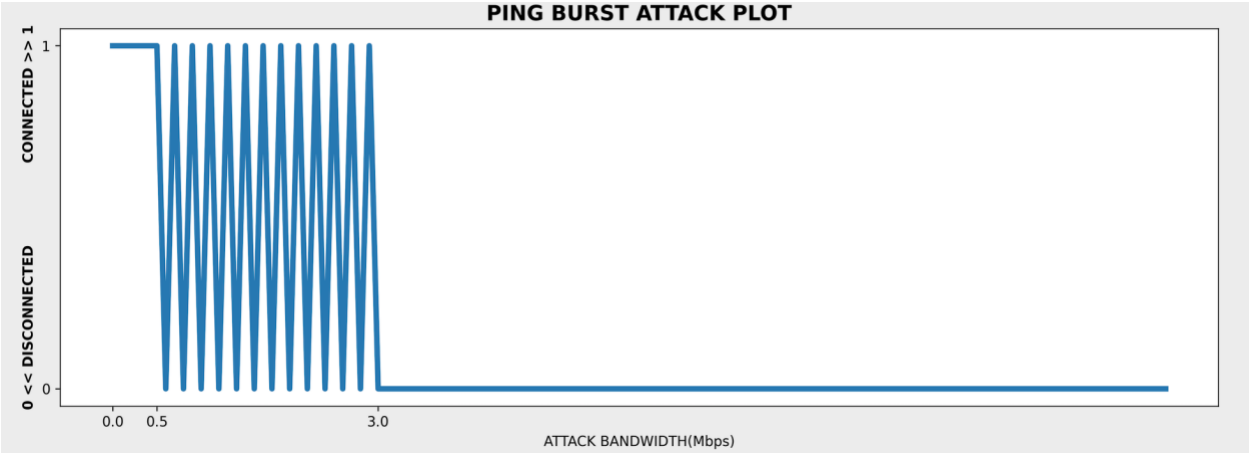


Figure 4.14: Observation of ping burst attack on EPM7000

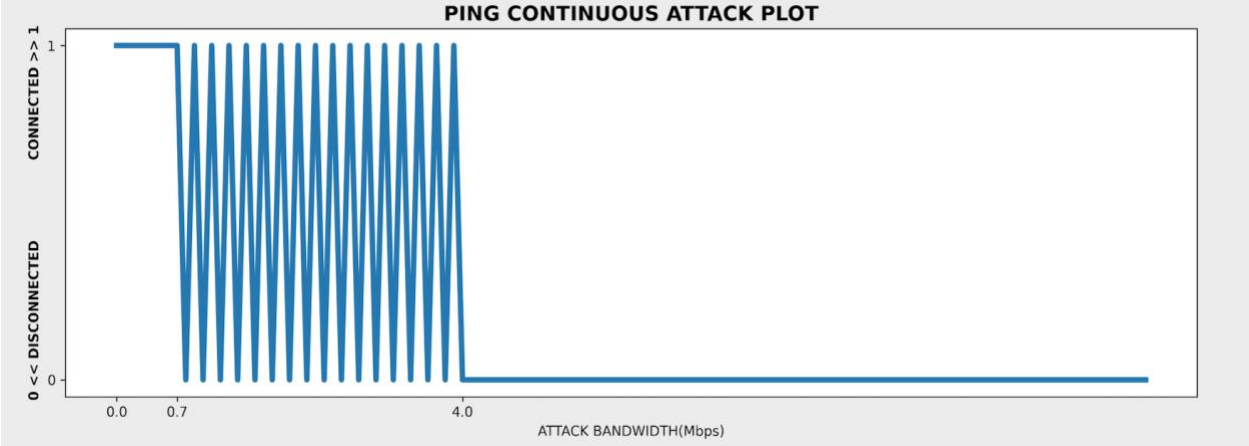


Figure 4.15: Observation of continuous ping attack on EPM7000

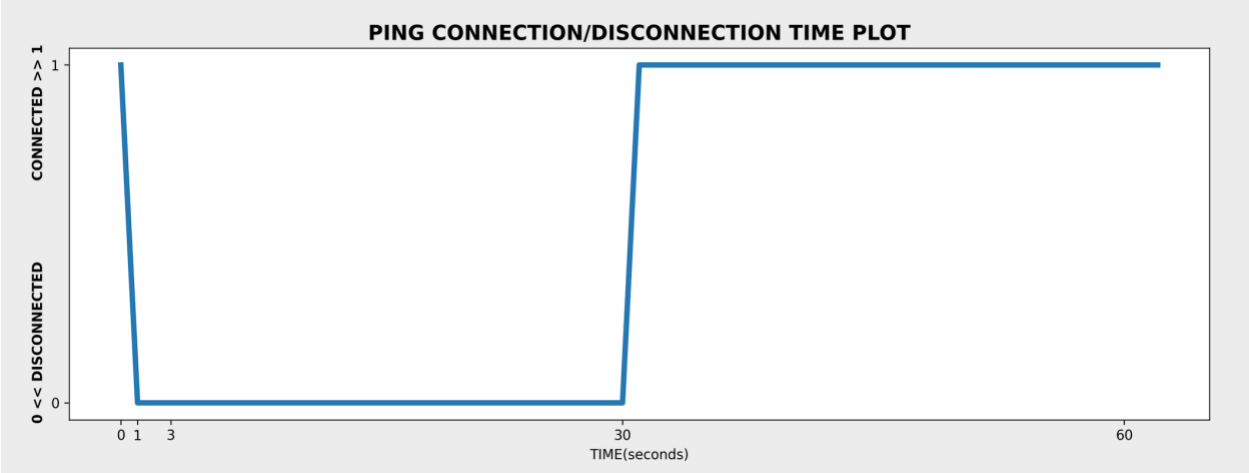


Figure 4.16: Observation of connection/disconnection time on EPM7000

### 4.4.3 Experimental Result Under SMURF.

While evaluating EPM 7000 under a burst and continuous SMURF attack we observed that for burst attack the minimum effective bandwidth was 2.0Mbps while the disconnection bandwidth was 5.0Mbps as show in fig (5.17). For continuous attack, we observed that the Minimum effective bandwidth was 3.0Mbps while the disconnection bandwidth was 7.0Mbps as shown in fig (5.18). We also recorded that the time taken to disconnect and reconnect were both 1 seconds as shown in fig (5.19).

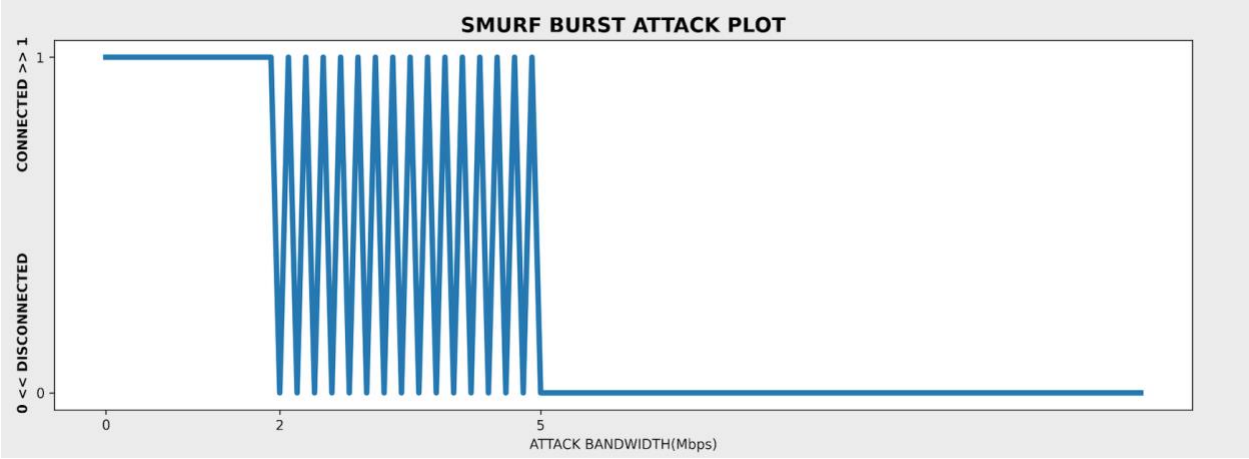


Figure 4.17: Observation of SMURF burst attack on EPM7000

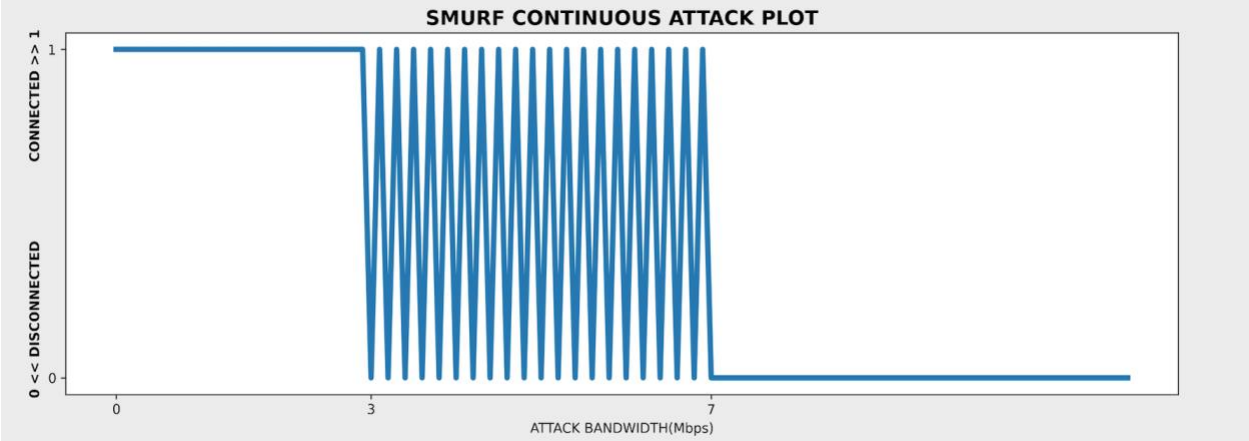


Figure 4.18: Observation of continuous SMURF attack on EPM7000

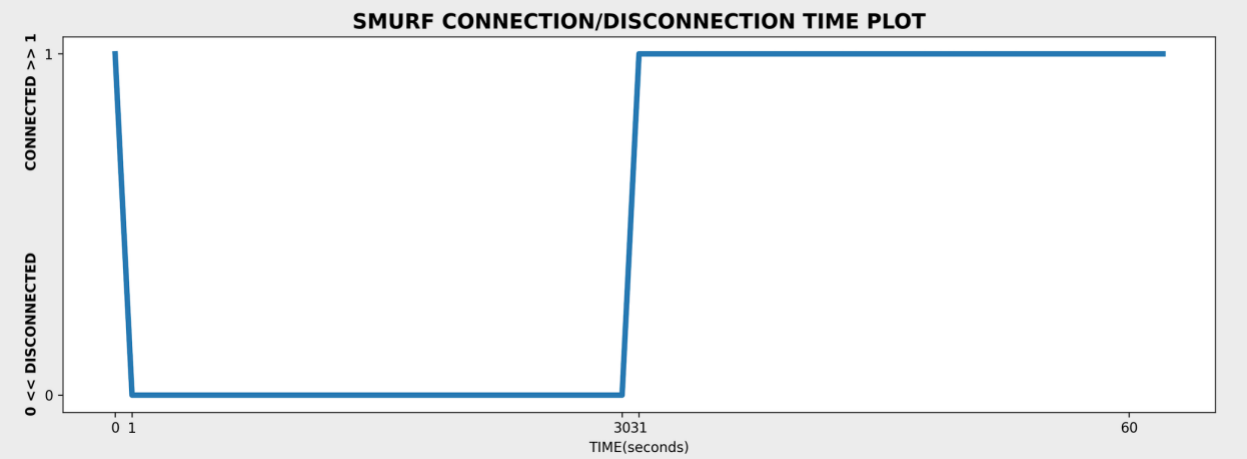


Figure 4.19: Observation of connection/disconnection time on EPM7000

### 4.4.4 Experimental Result Under TCP/SYN.

While evaluating EPM 7000 under a burst and continuous TCP/SYN attack we observed that for burst attack the minimum effective bandwidth was 5.0Mbps while the disconnection bandwidth wa11.0Mbps as show in fig (5.20). For continuous attack, we observed that the Minimum effective bandwidth was 5.0Mbps while the meter never disconnected as shown in fig (5.21). We also recorded that the time taken to disconnect and reconnect were both1 seconds as shown in fig (5.22).

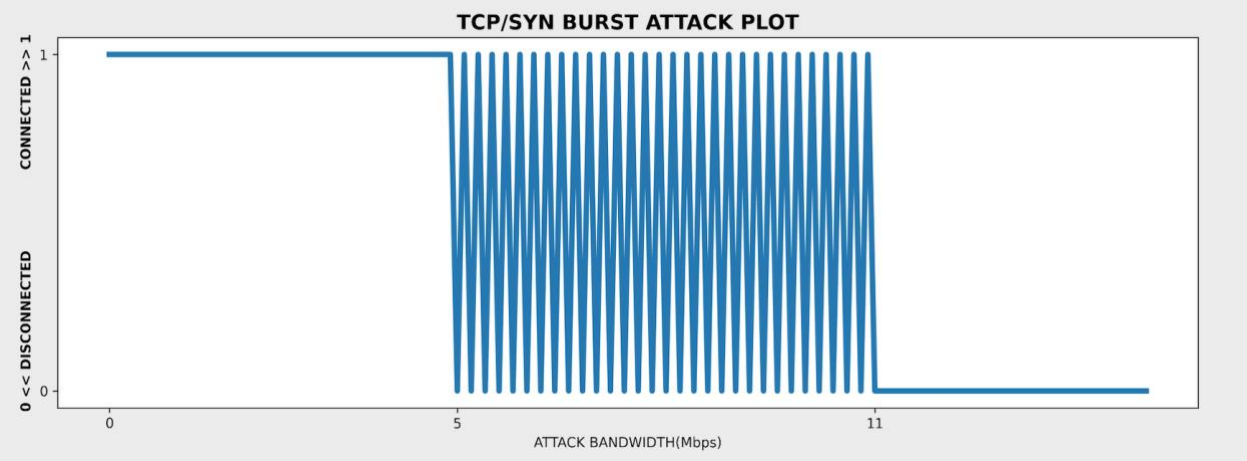


Figure 4.20: Observation of TCP/SYN burst attack on EPM7000

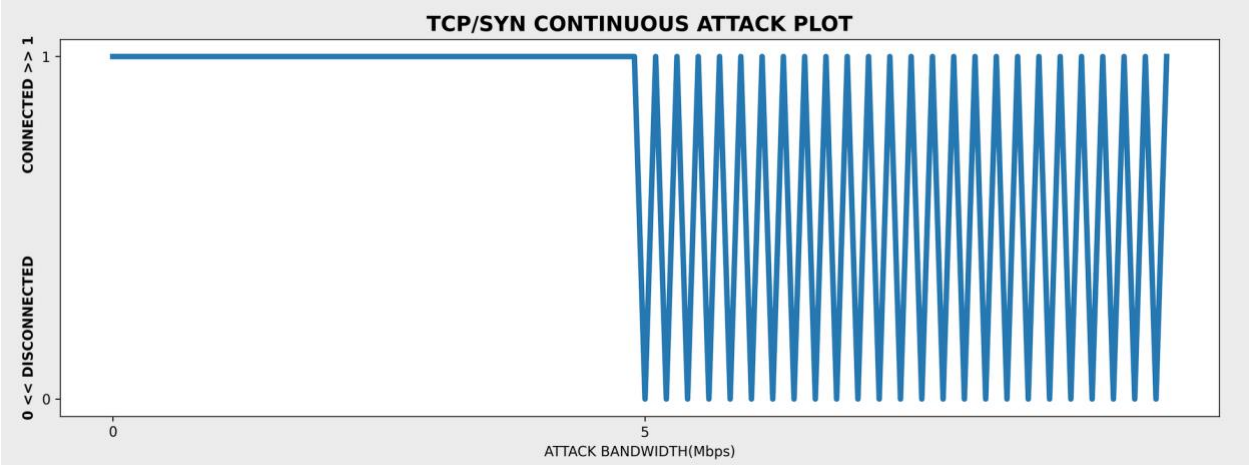


Figure 4.21: Observation of continuous TCP/SYN attack on EPM7000

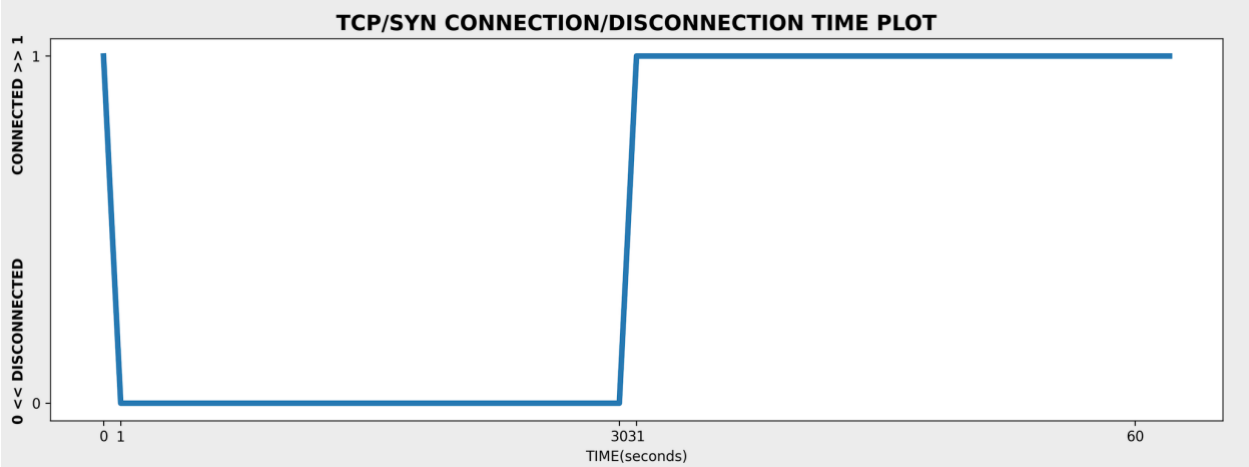


Figure 4.22: Observation of connection/disconnection time on EPM7000

### 4.5 Experimental Results and Discussion from E650 Smart Electric Meter

To determine the connectivity of E650 smart meter, a couple of experiment was conducted. In the past, common DDoS attacks come in the form of sustained, high-volume traffic floods that gradually increases, reach a peak, and then followed by a sudden or a slow descent. Nowadays, a new attack pattern known as bursts attacks or hit-and-run attacks have emerged. This type of attack use repeated short bursts of high intensity attacks at unpredictable intervals. A burst can last for as little as 2 seconds while a more malicious attack can span for hours non-stop, sending hundreds of gigabits per second of packets to a victim. In this experiment, we measured the effect of this two types of attack and noted the different impact it has on E650. The maximum bandwidth capacity of ethernet cable used for this experiment is 100 Mbps which is the standard capacity of a regular CAT 5 cable. The Attacker computer has maximum capacity to send flooding traffic at the rate of 1Gbps . Therefore10% of the total flooding capacity of the attack computer was used for the experiment. Figure(5.3) shows the lab setup diagram for the evaluation of E650.

### 4.5.1 Experimental result of connectivity test of Ladis Power Quality Meter Under Different cyber attacks

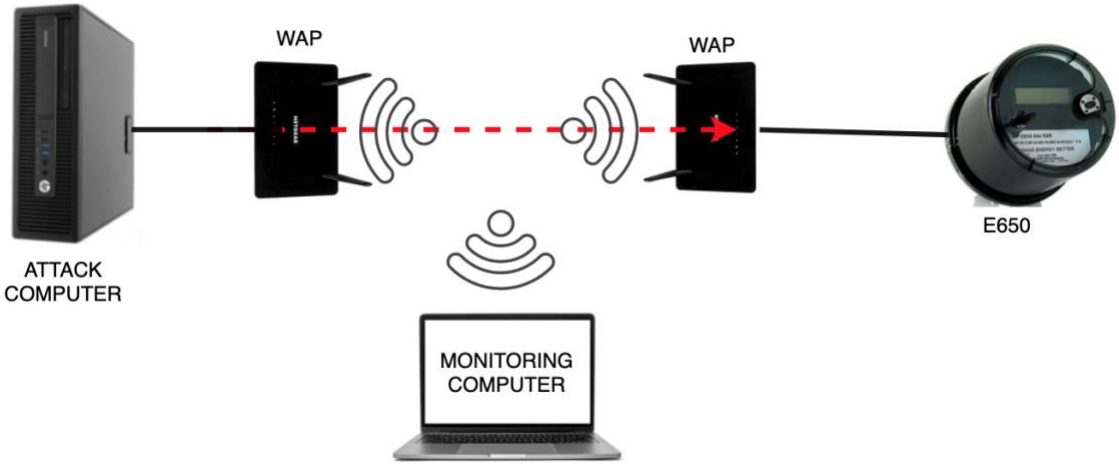


Figure 4.23: Lab experiment setup for evaluating E650 connectivity.

After the experiment, the connectivity information was summarized in Table 5.1 as shown below. The term minimum effect means the minimum Mbps bandwidth we started noticing a fluctuating in the connectivity while the term disconnection means the Mbps bandwidth at which communication was completely lost.

**Table 4.3: Experiment Result of Performance of smart Metering Data Communication for E650 Power Quality Smart Quality Smart Electric Meter Under Different Cyber-Attacks.**

| DESCRIPTION | PING | SMURF | TCP/SYN |
|---|---|---|---|
| Minimum effect burst attack bandwidth (Mbps) | 0.5 | 1.5 | 3.5 |
| Disconnection burst attack bandwidth (Mbps) | 3.0 | 5.0 | 7.0 |
| Minimum effect continuous attack bandwidth (Mbps) | 1.0 | 2.0 | 5.0 |
| Disconnection continuous attack bandwidth (Mbps) | 6.0 | 6.0 | 1000.0 |
| Time to disconnect (seconds) | 2.0 | 2.0 | 2.0 |
| Time to reconnect (seconds) | 15.0 | 15.0 | 15.0 |

### 4.5.2 Experimental Result Under PING

While evaluating E650 under a burst and continuous PING attack we observed that for burst attack the minimum effective bandwidth was 0.5Mbps while the disconnection bandwidth was 3.0Mbps as show in fig (5.24). For continuous attack, we observed that the Minimum effective bandwidth was 1.0Mbps while the disconnection bandwidth was 6.0Mbps as shown in fig (5.25). We also recorded that the time taken to disconnect and reconnect were 1 seconds and 15 seconds respectively as shown in fig (5.26).

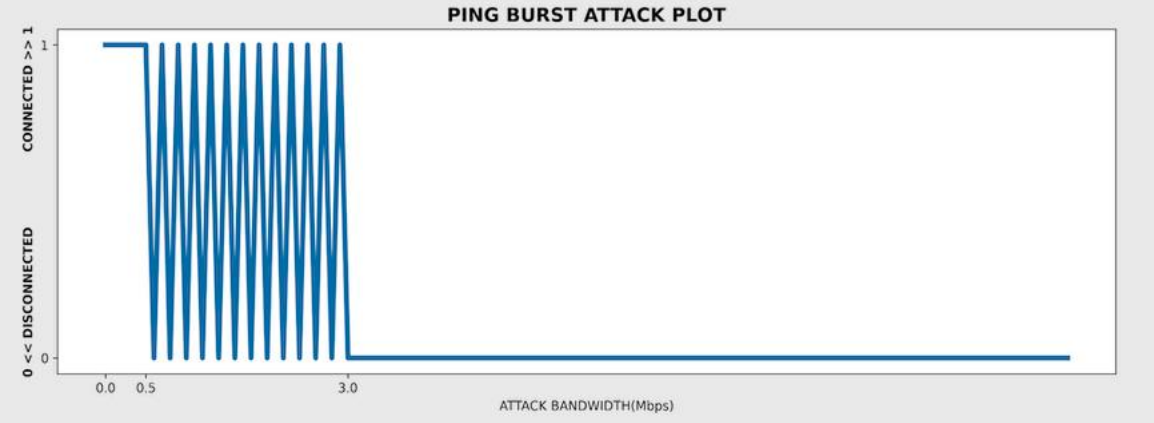


Figure 4.24: Observation of ping burst attack on E650

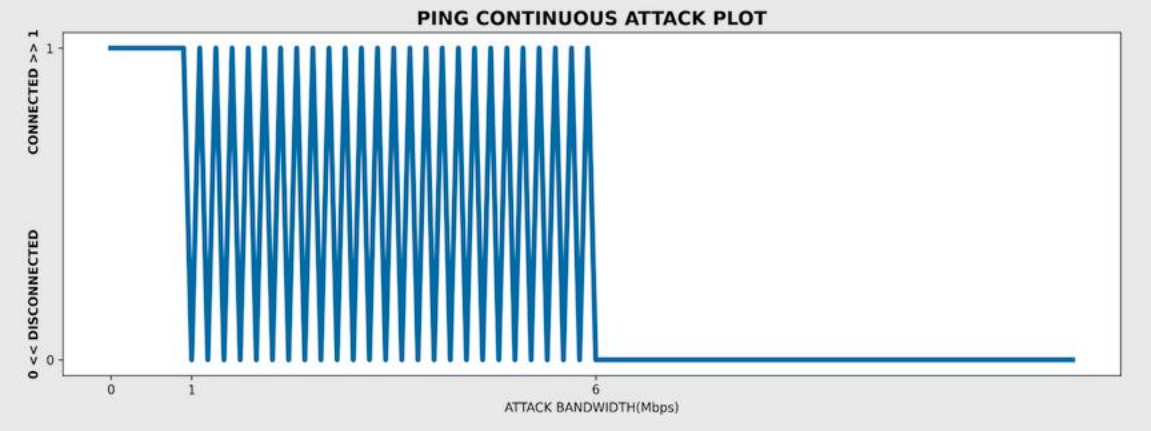


Figure 4.25: Observation of continuous ping attack on E650

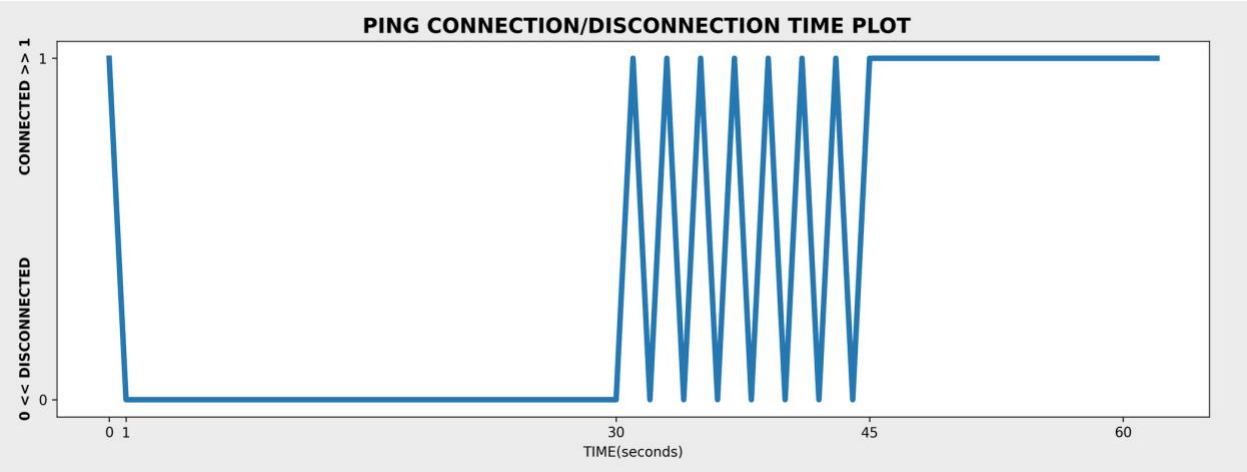


Figure 4.26: Observation of connection/disconnection time on E650

### 4.5.3 Experimental Result Under SMURF

While evaluating E650 under a burst and continuous SMURF attack we observed that for burst attack the minimum effective bandwidth was 1.5Mbps while the disconnection bandwidth was 5.0Mbps as show in fig (5.27). For continuous attack, we observed that the Minimum effective bandwidth was 2.0Mbps while the disconnection bandwidth was 6.0Mbps as shown in fig (5.28). We also recorded that the time taken to disconnect and reconnect were 1 seconds and 15 seconds respectively as shown in fig (5.29).

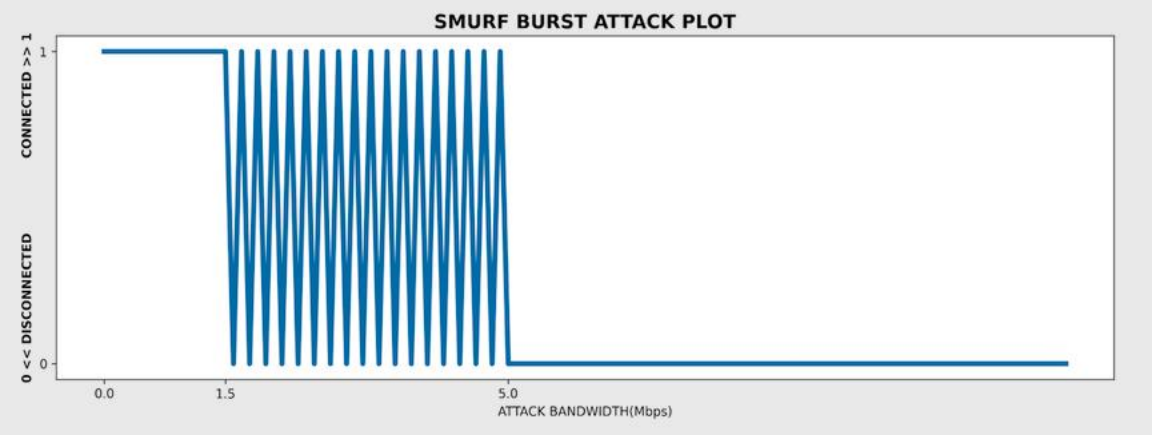


Figure 4.27: Observation of SMURF burst attack on E650

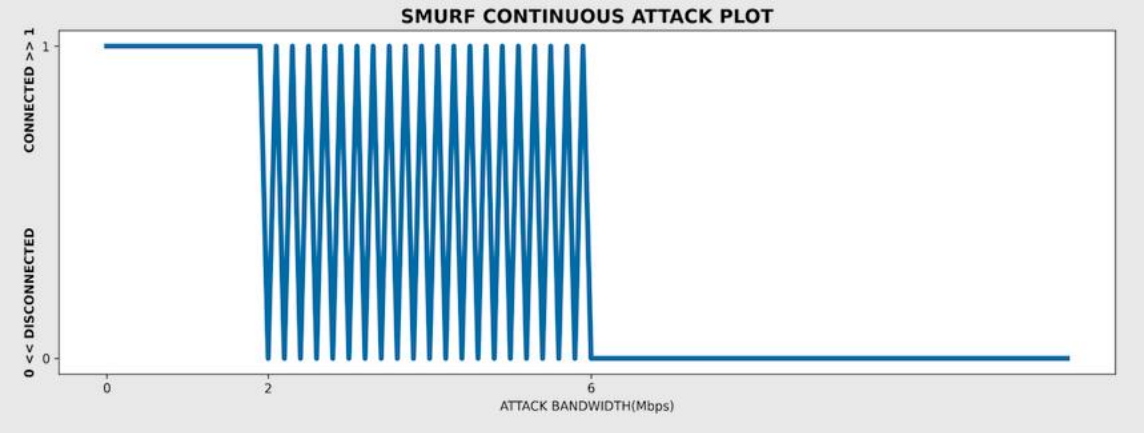


Figure 4.28: Observation of continuous SMURF attack on E650

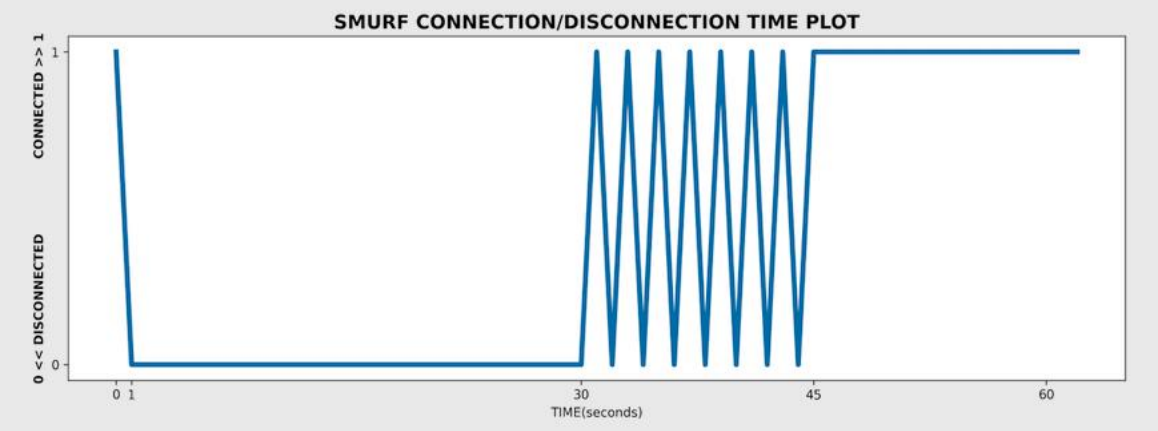


Figure 4.29: Observation connection/disconnection time on E650

### 4.5.4 Experimental Result Under TCP/SYN

While evaluating E650 under a burst and continuous TCP/SYN attack we observed that for burst attack the minimum effective bandwidth was 3.5Mbps while the disconnection bandwidth was 7.0Mbps as show in fig (5.30). For continuous attack, we observed that the Minimum effective bandwidth was 5.0Mbps while the meter never totally disconnected as shown in fig (5.31). We also recorded that the time taken to disconnect and reconnect were 1 seconds and 15 seconds respectively as shown in fig (5.32).

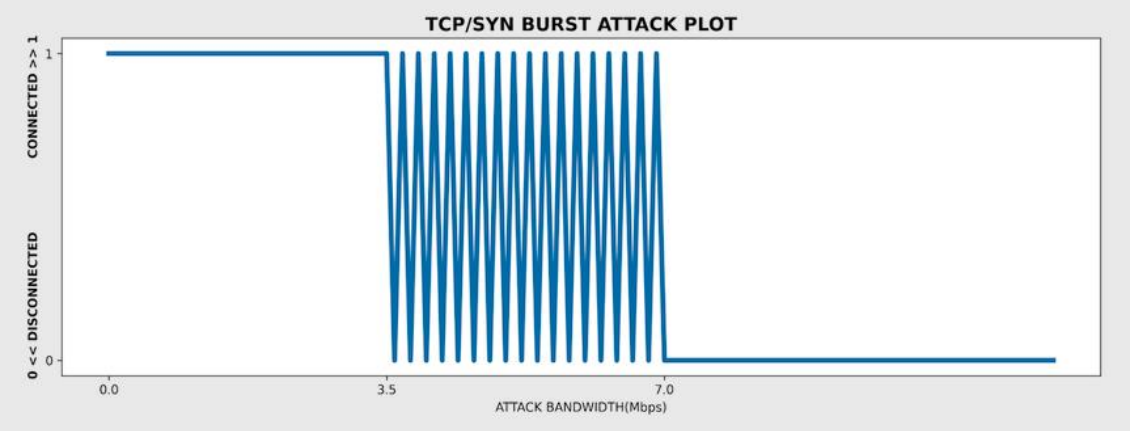


Figure 4.30: Observation of TCP/SYN burst attack on E650

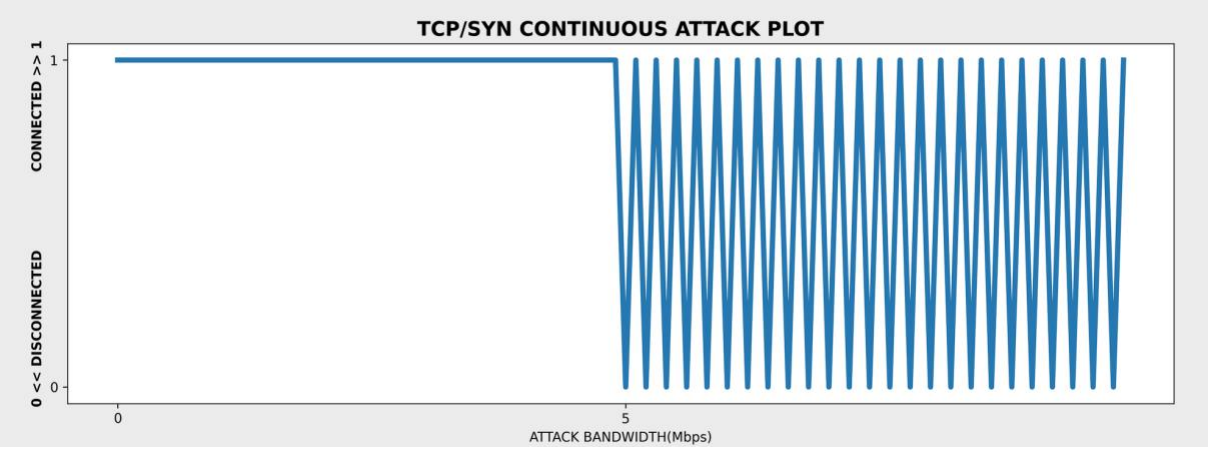


Figure 4.31: Observation of continuous TCP/SYN attack on E650

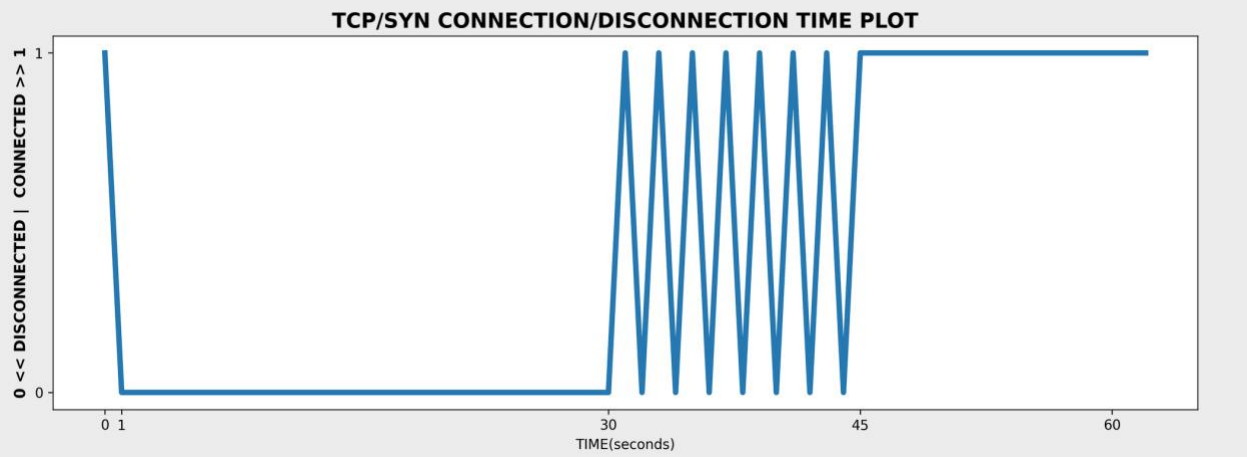


Figure 4.32: Observation of connection/disconnection time on E650

## 4.6 Chapter Summary

In the past, common DDoS attacks come in the form of sustained, high-volume traffic floods that gradually increases, reach a peak, and then followed by a sudden or a slow descent. Nowadays, a new attack pattern known as bursts attacks or hit-and-run attacks have emerged. This type of attack use repeated short bursts of high intensity attacks at unpredictable intervals. In this chapter, we measured the effect of this two types of attack and noted the different impact it has on EPM6100, EPM7000 and E650 smart meters. Contrary to the previous experiments, This chapter centers on the connectivity the different smart electric meters. It can be deduced from the experiments that the PING attack has the highest effect followed by the SMURF attack and then the TCP/SYN attack. The TCP/SYN plot shows the major difference between the effect of continuous and burst attack. For continuous TCP/SYN attacks, the smart meter never disconnected even when the attack was increased to a significant limit. This was not the case with the burst attack, none of the smart meters was able to communicate when the burst attack reached the disconnection bandwidth.

# CHAPTER V

# COMPARISON OF DIFFERENT RESULTS AND ATTACKS

## 5.1 Comparison of the effects of Cyber-Security Attacks on Different Communication Methods

From the series of experiment conducted so far, it is completely obvious that for EPM 6100, the consumption reporting can be altered when the smart meter is subjected to cybersecurity attacks. This have been verified to hold for wired, wireless, and a hybrid of both. In this chapter, we compared the effect of this attacks on consumption reading relative to the method of communication i.e. Wired, wireless, or hybrid of both. For the three experiments, the baseline consumption values were first observed and recoded. The baseline consumption values are calculated when the electric smart meter is operating on a zero treat or no cybersecurity attack. After the baseline recording, the EPM 6100 smart meter was first evaluated for its security integrity of its data collection under a cyber-attack starting with evaluating it for 4 days followed by 7 days and 15 days extending up to 30 days which corresponds to a conventional customer billing cycle. The same procedure was used for all the experimental set ups shown in the Figures (6.1 – 6.3) for wired, a hybrid of wired and wireless, and wireless respectively.

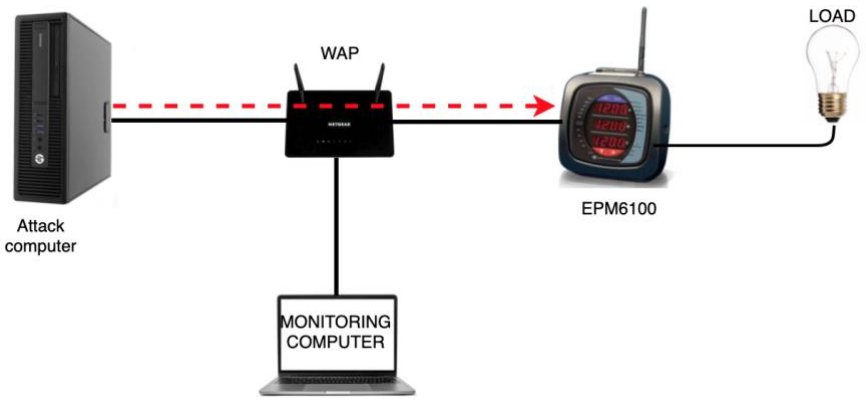


Figure 5.1 Experimental Setup for evaluating the effect of wired(Ethernet based) cybersecurity attack on wired smart meter.

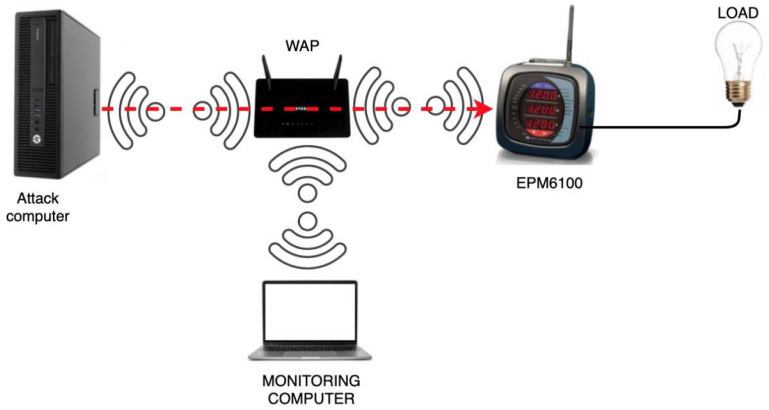


Figure 5.2 Experimental Setup for evaluating the effect of wireless(WiFi based) cybersecurity attack on wireless smart meter.

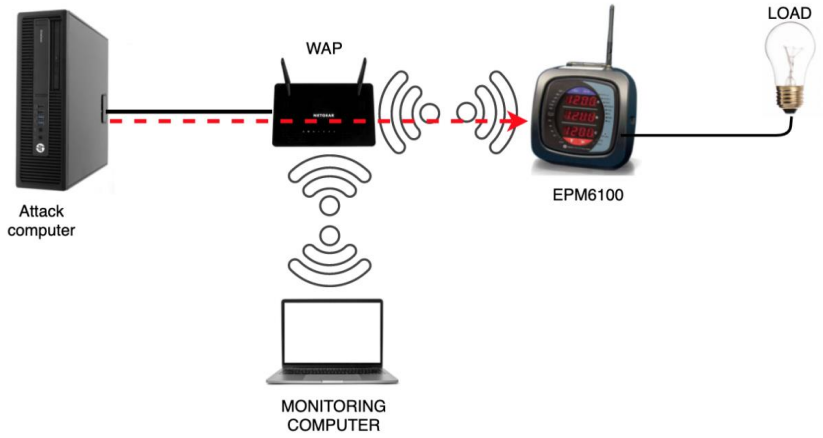


Figure 5.3 Experimental Setup for evaluating the effect of a hybrid( Ethernet and WiFi) of wired and wireless cybersecurity attack on wireless smart meter.

From the plot shown below in (Figure 5.4). The green plot represents Wireless smart meter communication utilizing Ethernet cables only.The blue plot represents a Hybrid connection of Wifi and Ethernet for smart meter communication and then the red plot represents smart meter wired connection using Ethernet cable only. It can be observed from the graph that for the first two to three days, there was a little bit of fluctuation in the power consumption plot of Wireless and Hybrid plots. After the third day, the consumption plot for wireless connecting was substantial, steeping further below the consumption in hybrid mode. For four days attack both hybrid and wireless attack where at logahead with each othere, however the wired or Ethernet based consumption decreased substancially.

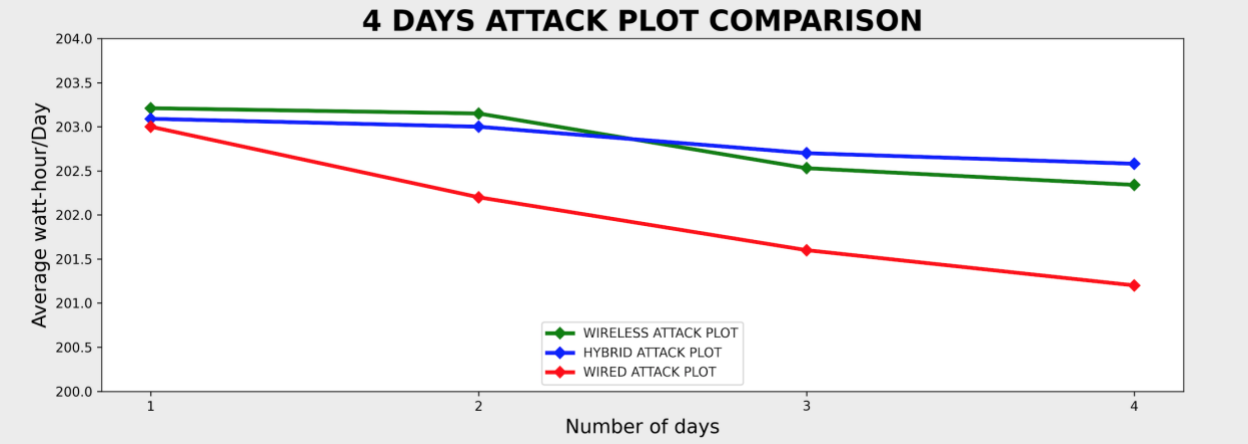


Figure 5.4: Average Power Consumption measured in Average Watt hour for Wireless, Hybrid and Wired smart meter connection for 4 days.

From the plot show in (Figure 6.5). The green plot represents Wireless smart meter communication utilizing Ethernet cables only. The blue plot represents a Hybrid connection of WIFI and Ethernet for smart meter communication and then the red plot represents smart meter wired connection using Ethernet cable only. It can be observed from the graph that for the first 5 days, the wireless and hybrid smart meter connection plot was crossing each other without a clear definition of trend. However, after the seventh day the hybrid meter connection proved to me more effective in consumption. The wired smart meter connection proved to me more effective in altering the consumption values of the smart meter .

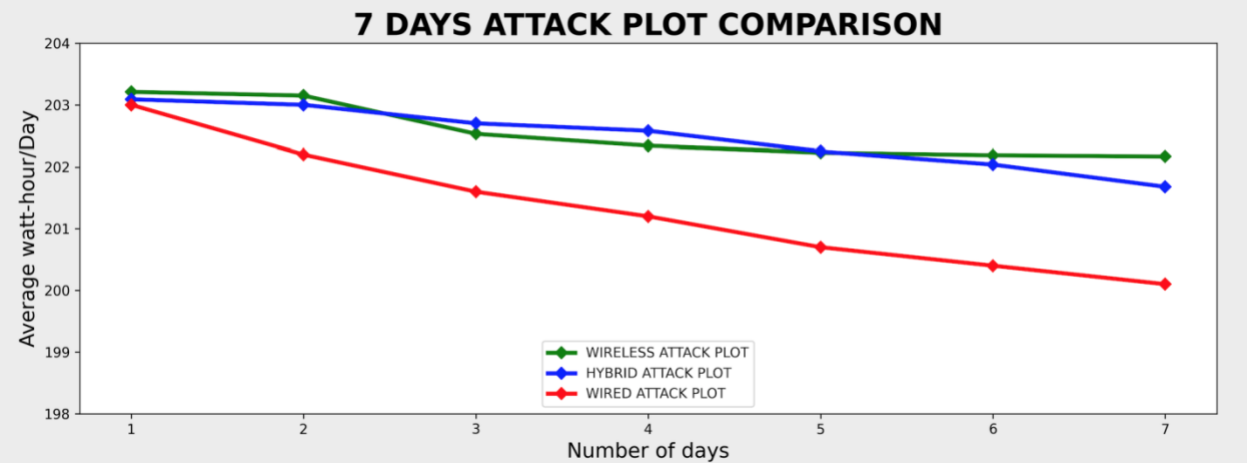


Figure 5.5: Average Power Consumption measured in Average Watt hour for Wireless, Hybrid and Wired smart meter connection for 7 days.

From the plot shown below in (Figure 6.6). The green plot represents Wireless smart meter communication utilizing Ethernet cables only. The blue plot represents a Hybrid connection of WIFI and Ethernet for smart meter communication and then the red plot represents smart meter wired connection using Ethernet cable only. It can be observed from the graph that for the first two to three days, there was a little bit of fluctuation in the power consumption plot of Wireless and Hybrid plots. After the third day, the consumption plot for wireless connecting was substantial, steeping further below the consumption in hybrid mode. After the attack for the fourth day, both hybrid and wireless attack where at log ahead with each other, however the wired or Ethernet based consumption decreased substantially. Also, it can be observed from the graph that for the first 5 days, the wireless and hybrid smart meter connection plot was crossing each other without a clear definition of trend. However, after the seventh day the hybrid meter

connection proved to me more effective in consumption. From the seventh day to the fifteenth day, it became clear that hybrid connection attack had more effect on the meter compared to the wireless connection. The completely wired connection still proved dominant and more effective in altering the consumption recording of the wireless smart meter.

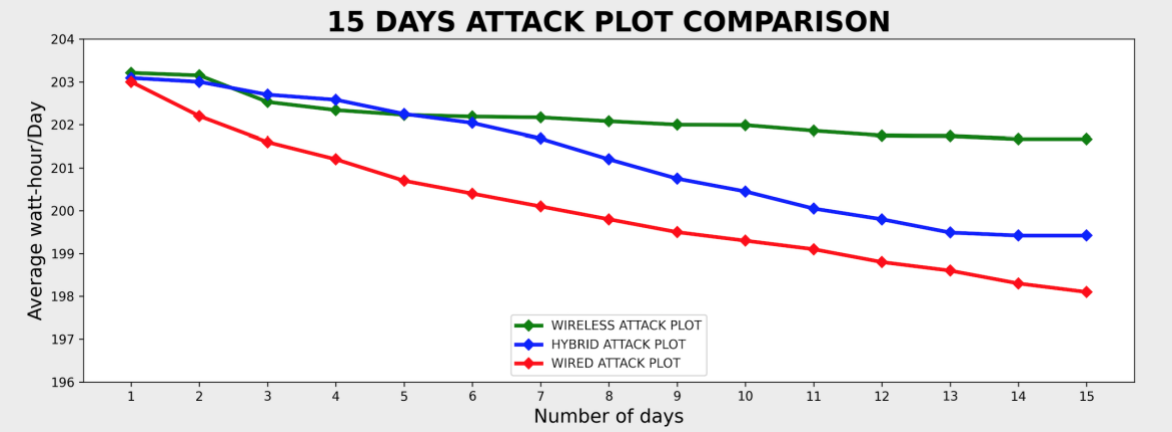


Figure 5.6: Average Power Consumption measured in Average Watt hour for Wireless, Hybrid and Wired smart meter connection for 15 days

From the plot shown below in (Figure 6.7). The green plot represents Wireless smart meter communication utilizing Ethernet cables only. The blue plot represents a Hybrid connection of WIFI and Ethernet for smart meter communication and then the red plot represents smart meter wired connection using Ethernet cable only. It can be observed from the graph that for the first two to three days, there was a little bit of fluctuation in the power consumption plot of Wireless and Hybrid plots. After the third day, the consumption plot for wireless connecting was substantial, steeping further below the consumption in hybrid mode. After the attack for the fourth day, both hybrid and wireless attack where at log ahead with each other, however the wired or Ethernet based consumption decreased substantially. Also, it can be observed from the graph that for the first 5 days, the wireless and hybrid smart meter connection plot was crossing

each other without a clear definition of trend. However, after the seventh day the hybrid meter connection proved to me more effective in consumption. From the seventh day to the thirtieth day, it became clear that hybrid connection attack had more effect on the meter compared to the wireless connection.  It is now clear, after attacking the meter for 30 days using the three different types of connection, that wired, or Ethernet based attack is most effective in effecting the consumption reading of EPM 6100 followed by the hybrid connection and then the wireless connection.

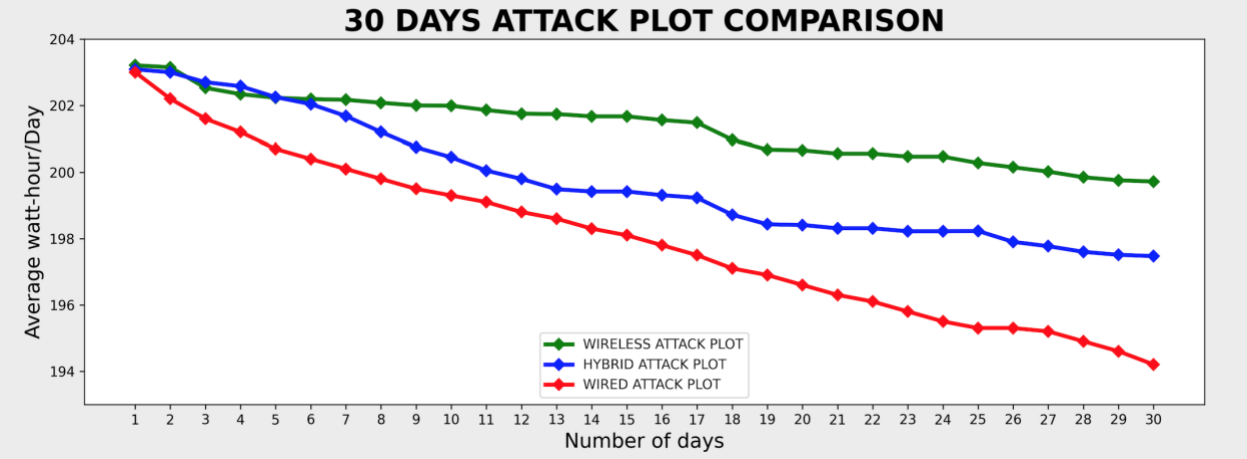


Figure 5.7: Average Power Consumption measured in Average Watt hour for Wireless, Hybrid and Wired smart meter connection for 7 days

## 5.2 Comparison of the connectivity strength of EMP 6100, EPM 7000 and E650 under different types of cybersecurity attacks.

In this experiment, we utilized three different smart meters i.e. EPM6100, EPM7000, and E650 smart meters. We did not used any load because we are not interested in the consumption, instead we are interested in the connectivity of the smart meters. Given that most of the smart meters are designed to be connected using ethernet cable, we used 2 wireless access points to bridge the communication between the attacking computer, remote monitoring computer, and the smart meters. Using that we were able to direct attack traffic from the attack computer to the smart meter. A close observation of the experimental setup as shown in(fig 5.1) shows how the Ethernet cables from the attack computer was connected to the wireless access point. Also, from the second wireless access point, it can be observed how the three smart meters were connected to the wireless access point using three Ethernet cables. Since the remote monitoring computer is WIFI enabled, there was no need to connect it to the wireless access point using an Ethernet cable, instead the WIFI feature of the computer was enabled and configured to communicate with the wireless access point.

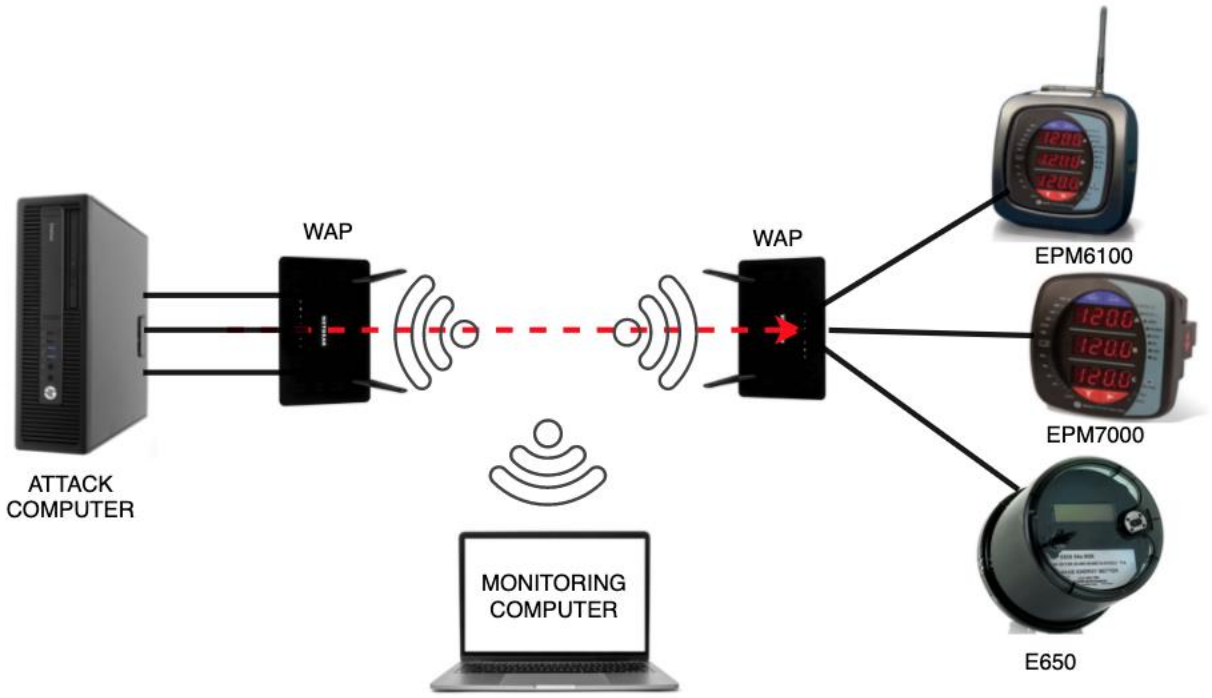


Figure 5.8: Lab Experimental setup for checking the connectivity strength EPM6100, EPM7000 and E650.

### 5.2.1 Ping burst attack plot comparison for epm6100, EPM7000 and E650 smart meters.

Comparing the three smart meters we can see the various effects of a burst ping attack on the three meters as show in Fig (5.9) below. The plot shows that for EPM 6100 under a ping burst attack the minimum effective bandwidth was 0.3Mbps while the disconnection bandwidth was 2.0Mbps. For EPM 7000, the plot shows that under a ping burst attack, the minimum effective bandwidth was 0.5Mbps while the disconnection bandwidth was 3.0Mbps. For E650, the plot shows that under a ping burst attack, the minimum effective bandwidth was 0.5Mbps while the disconnection bandwidth was 3.0Mbps. Deducing from the plot and readings from the three different meters, we can conclude that the EPM 6100 smart meter is more susceptible to the effects of ping burst cybersecurity attack while the E650 has a more resistant NIC.

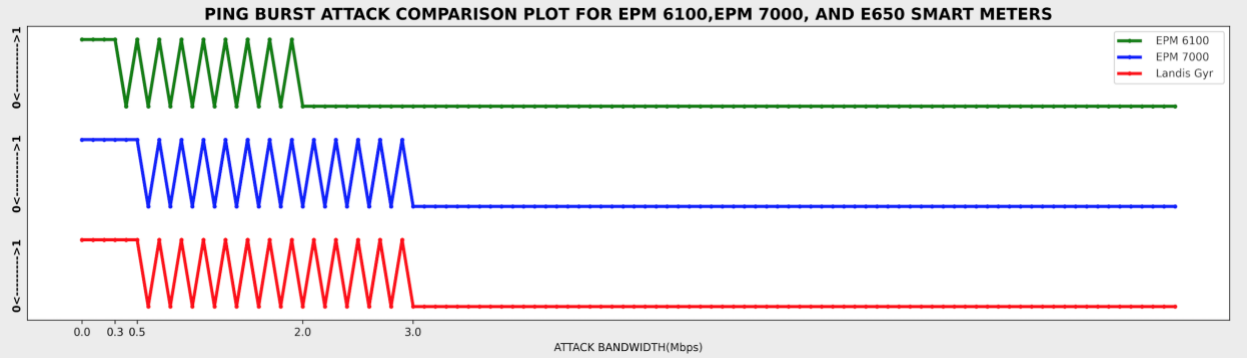


Figure 5.9: Observation of the effect of ping burst attack on the connectivity strength EPM6100, EPM7000 and E650.

### 5.2.2 Continuous ping attack plot comparison for EPM6100, EPM7000 and E650 Smart Meters.

Comparing the three smart meters we can see the various effects of a continuous ping attack on the three meters as show in Fig (5.10) below. The plot shows that for EPM 6100 under a continuous ping attack the minimum effective bandwidth was 0.5Mbps while the disconnection bandwidth was 2.0Mbps. For EPM 7000, the plot shows that under a ping burst attack, the minimum effective bandwidth was 0.7Mbps while the disconnection bandwidth was 4.0Mbps. For E650, the plot shows that under a ping burst attack, the minimum effective bandwidth was 1.0Mbps while the disconnection bandwidth was 6.0Mbps. Deducing from the plot and readings from the three different meters, we can conclude that the EPM 6100 smart meter is more susceptible to the effects of continuous ping cybersecurity attack while the E650 has a more resistant NIC.

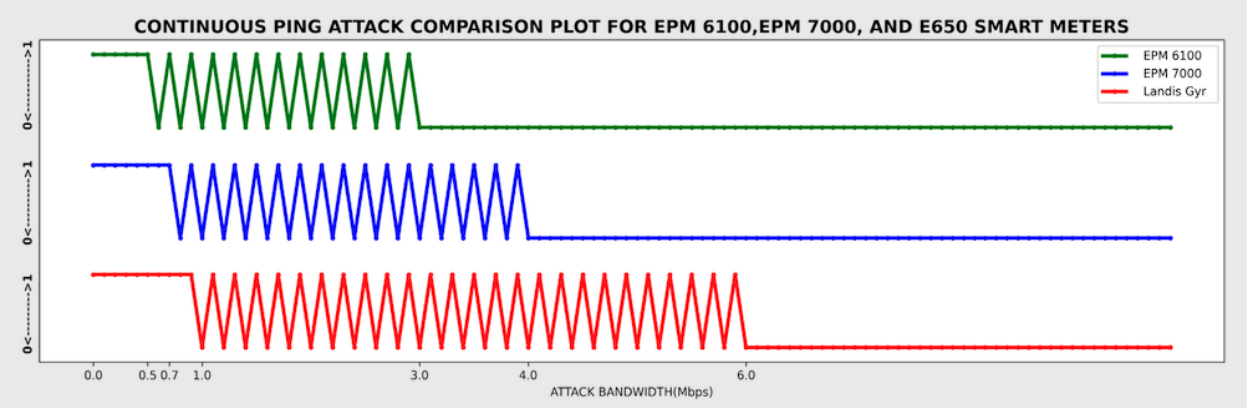


Figure 5.10: Observation of the effect of continuous ping attack on the connectivity strength EPM6100, EPM7000 and E650.

### 5.2.3 Smurf burst attack plot comparison for epm6100, EPM7000 and E650 smart meters.

Comparing the three smart meters we can see the various effects of a SMURF burst attack on the three meters as show in Fig (5.11) below. The plot shows that for EPM 6100 under a SMURF burst attack the minimum effective bandwidth was 1.0Mbps while the disconnection bandwidth was 3.0Mbps. For EPM 7000, the plot shows that under a ping burst attack, the minimum effective bandwidth was 2.0 Mbps while the disconnection bandwidth was 5.0 Mbps. For E650, the plot shows that under a ping burst attack, the minimum effective bandwidth was 1.5Mbps while the disconnection bandwidth was 5.0Mbps. Deducing from the plot and readings from the three different meters, we can conclude that the EPM 6100 smart meter is more susceptible to the effects of SMURF burst cybersecurity attack while the EPM7000 has a more resistant NIC.

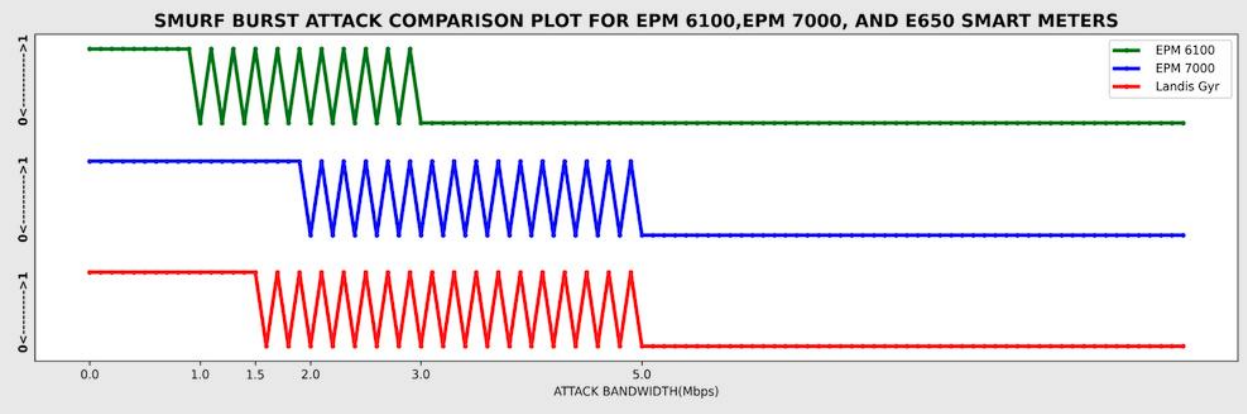


Figure 5.11: Observation of the effect of SMURF burst attack on the connectivity strength EPM6100, EPM7000 and E650.

### 5.2.4 Continuous Smurf attack plot comparison for epm6100, EPM7000 and E650 smart meters.

Comparing the three smart meters we can see the various effects of a continuous SMURF attack on the three meters as show in Fig (5.12) below. The plot shows that for EPM 6100 under a continuous SMURF attack the minimum effective bandwidth was 1.7Mbps while the disconnection bandwidth was 5.0Mbps. For EPM 7000, the plot shows that under a ping burst attack, the minimum effective bandwidth was 3.0Mbps while the disconnection bandwidth was 7.0Mbps. For E650, the plot shows that under a ping burst attack, the minimum effective bandwidth was 2.0Mbps while the disconnection bandwidth was 6.0Mbps. Deducing from the plot and readings from the three different meters, we can conclude that the EPM 6100 smart meter is more susceptible to the effects of SMURF burst cybersecurity attack while the EPM7000 has a more resistant NIC.

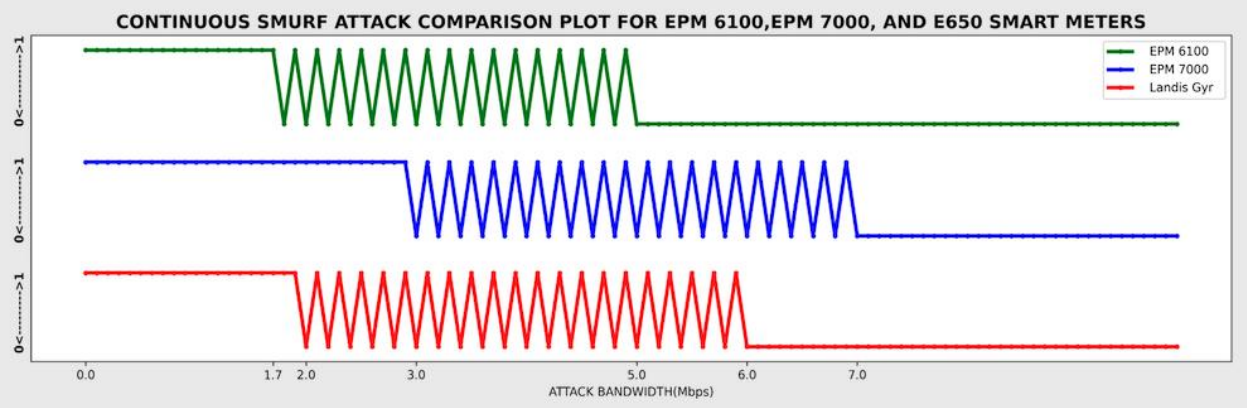


Figure 5.12: Observation of the effect of continuous SMURF attack on the connectivity strength of EPM6100, EPM7000 and E650.

### 5.2.5 TCP/SYN burst attack plot comparison for EPM6100, EPM7000 and E650 smart meters.

Comparing the three smart meters we can see the various effects of a burst TCP/SYN attack on the three meters as show in Fig (5.13) below. The plot shows that for EPM 6100 under a TCP/SYN burst attack the minimum effective bandwidth was 2.0 Mbps while the disconnection bandwidth was 5.0Mbps. For EPM 7000, the plot shows that under a ping burst attack, the minimum effective bandwidth was 5 Mbps while the disconnection bandwidth was 11 Mbps. For E650, the plot shows that under a ping burst attack, the minimum effective bandwidth was 3.5Mbps while the disconnection bandwidth was 7.0Mbps. Deducing from the plot and readings from the three different meters, we can conclude that the EPM 6100 smart meter is more susceptible to the effects of TCP/SYN burst cybersecurity attack while the EPM7000 has a more resistant NIC.

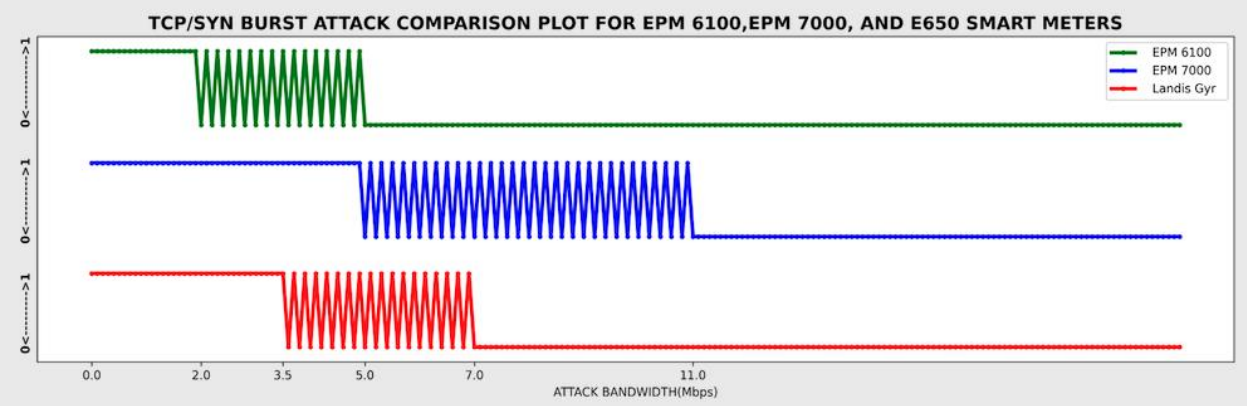


Figure 5.13: Observation of the effect of TCP/SYN burst attack on the connectivity strength of EPM6100, EPM7000 and E650.

### 5.2.6 Continuous TCP/SYN attack plot comparison for EPM6100, EPM7000 and E650 smart meters.

Comparing the three smart meters we can see the various effects of a continuous TCP/SYN attack on the three meters as show in Fig(5.14) below. The plot shows that for EPM 6100 under a continuous TCP/SYN attack the minimum effective bandwidth was 4.0 Mbps and the smart meter never completely disconnected. For EPM 7000, the plot shows that under a ping burst attack, the minimum effective bandwidth was 5.0 Mbps and the smart meter never completely disconnected. For E650, the plot shows that under a ping burst attack, the minimum effective bandwidth was 0.5Mbps and the smart meter never completely disconnected. Deducing from the plot and readings from the three different meters, we can conclude that the EPM 6100 smart meter is more susceptible to the effects of continuous TCP/SYN cybersecurity attack while the EPM7000 has a more resistant NIC.

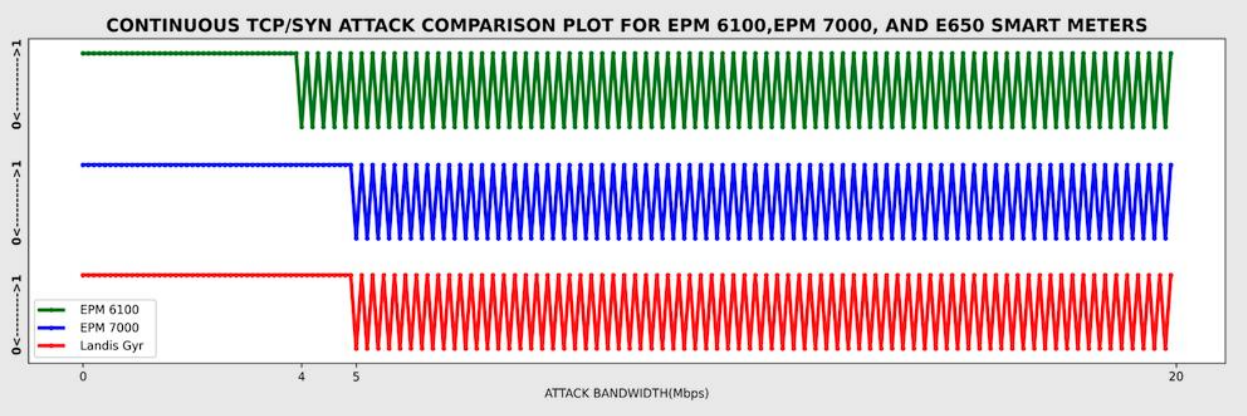


Figure 5.14: Observation of the effect of continuous TCP/SYN attack on the connectivity strength EPM6100, EPM7000 and E650.

### 5.2.7 Effect of different types of cybersecurity attacks on EPM 6100

In this comparison plot, we compared the effect of popular cybersecurity attacks on the connectivity of EPM 6100 power quality meter, we used the PING, SMURF and TCP/SYN cybersecurity attacks, all are configured to come in burst. Comparing the three types of attack we can see its various effects on an EPM 6100 smart meter as shown in Fig (5.15) below. The plot shows that for EPM 6100 under a PING attack the minimum effective bandwidth was 0.3 Mbps while the disconnection bandwidth was 2.0Mbps. Under SMURF attack, the plot shows that the minimum effective bandwidth was 1.0 Mbps while the disconnection bandwidth was 3 Mbps. Under TCP/SYN attack, the plot shows that the minimum effective bandwidth was 2.0 Mbps while the disconnection bandwidth was 5.0 Mbps. Deducing from the plot and readings from the three different attacks, we can conclude that PING attacks have the most effect on the connectivity of EPM 6100 smart meter while the TCP/SYN attacks has the list effect.

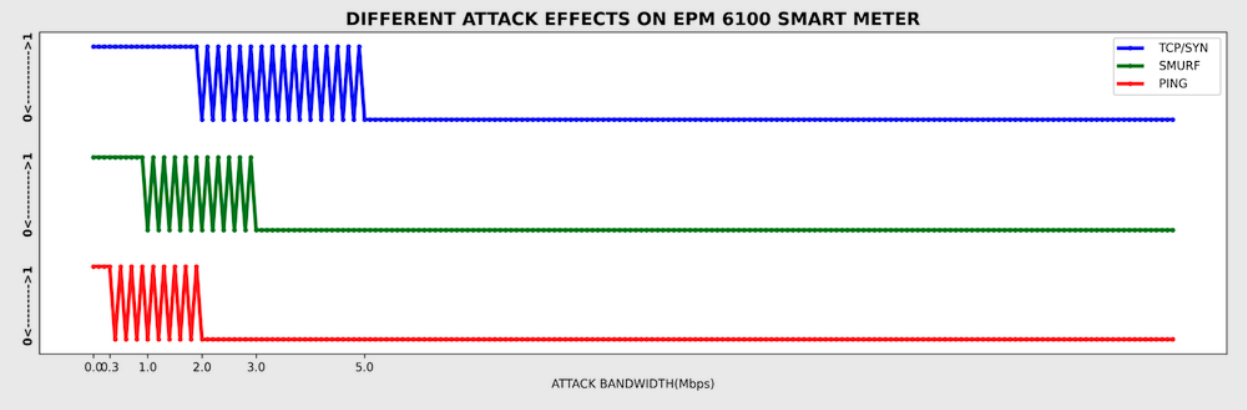


Figure 5.15: Effects of PING, SMURF and TCP/SYN attacks on the connectivity of EPM 6100

### 5.2.8 Effect of different types of cybersecurity attacks on EPM 7000

In this comparison plot, we compared the effect of popular cybersecurity attacks on the connectivity of EPM7000 power quality meter, we used the PING, SMURF and TCP/SYN cybersecurity attacks, all are configured to come in burst. Comparing the three types of attack we can see its various effects on an EPM 6100 smart meter as shown in Fig (5.15) below. The plot shows that for EPM7000 under a PING attack the minimum effective bandwidth was 0.5 Mbps while the disconnection bandwidth was 3.0Mbps. Under SMURF attack, the plot shows that the minimum effective bandwidth was 2.0 Mbps while the disconnection bandwidth was 5.0 Mbps. Under TCP/SYN attack, the plot shows that the minimum effective bandwidth was 5.0 Mbps while the disconnection bandwidth was 11.0 Mbps. Deducing from the plot and readings from the three different attacks, we can conclude that PING attacks have the most effect on the connectivity of EPM 7000 smart meter while the TCP/SYN attacks has the list effect.

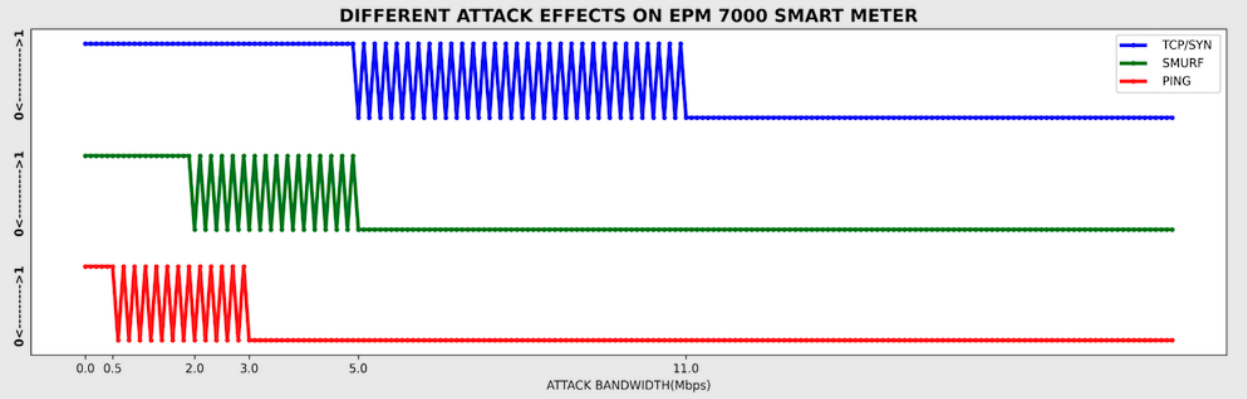


Figure 5.16: Effects of PING, SMURF and TCP/SYN attacks on the connectivity of EPM 7000

### 5.2.9 Effect of different types of cybersecurity attacks on E650

In this comparison plot, we compared the effect of popular cybersecurity attacks on the connectivity of E650 power quality meter, we used the PING, SMURF and TCP/SYN cybersecurity attacks, all are configured to come in burst. Comparing the three types of attack we can see its various effects on an E650 smart meter as shown in Fig (5.15) below. The plot shows that for E650 under a PING attack the minimum effective bandwidth was 0.5 Mbps while the disconnection bandwidth was 3.0Mbps. Under SMURF attack, the plot shows that the minimum effective bandwidth was 1.5 Mbps while the disconnection bandwidth was 5 Mbps. Under TCP/SYN attack, the plot shows that the minimum effective bandwidth was 3.5 Mbps while the disconnection bandwidth was 7.0 Mbps. Deducing from the plot and readings from the three different attacks, we can conclude that PING attacks have the most effect on the connectivity of E650 smart meter while the TCP/SYN attacks has the list effect on connectivity.

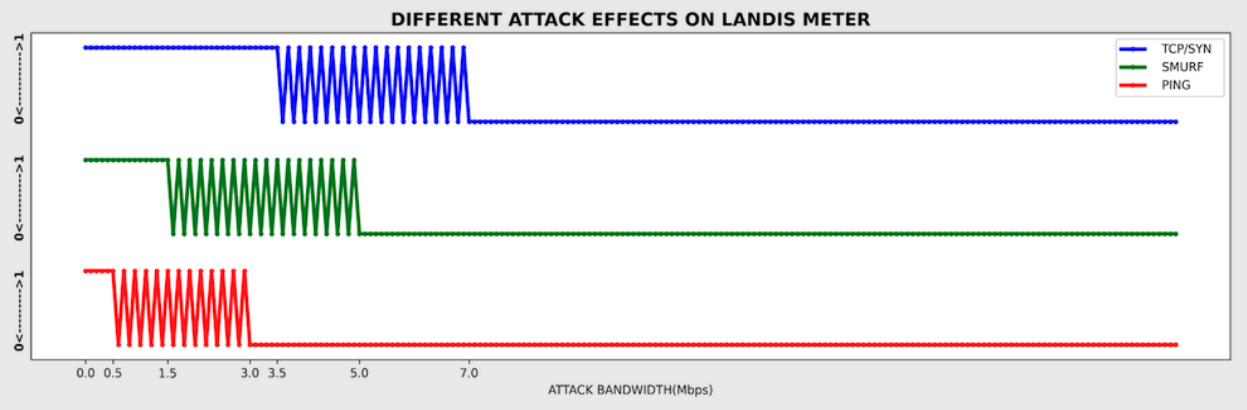


Figure 5.17: Effects of PING, SMURF and TCP/SYN attacks on the connectivity of E650

## 5.3 Chapter Summary

The aim of this chapter is to give a clear comparison of the different types of attack, devices and attacks that are most practical in smart meter industries today. The chapter starts by comparing the effect of cyber security attacks on the different types of smart meter connections. It compares the results obtained for wired connection (Ethernet based), wireless connection (WIFI based), and a hybrid of wired and wireless. The results shows that the more wired a smart meter connection is, the higher the intensity of the attack an vice versa. The second section compares the different types of attacks and its effect on different types of smart meters, the plots will serve as a guide for a company that wishes to decide on the time of smart meter to be used in industries in other to minimize the effects of cyber-attacks. The last section compares the types of attack on a particular smart meter and gives a clear picture of how it is affected by cybersecurity attacks such as PING, SMURF and TCP/SYN. The plots can serve as a guide for a company that wishes to decide on the type of smart meter to be used in other to minimize the effects of cyber security attacks.

# CHAPTER VI

# CONCLUSION

This research is the first time a wireless (WIFI based) smart electric meter has been tested and evaluated both in connectivity and consumption. The major aim of the experiment is to understand the effect of different cyber security attacks on smart meters. Smart meters are indispensable to customers as well as utility companies. Using the results in this research, customers can make a better choice on the type of Smart electric meter they need to acquire. Also, utility companies can use the results from this paper to further improve the resistance of their products to cybersecurity attacks. While it is true that utility companies already have security measures in place to prevent the types of attacks presented in this Thesis, those solutions are not inherent to the meters. There have been cases where such security measures have been compromised, leaving the smart meters without any defense mechanism. Therefore, this research shows the effect of cybersecurity attacks when smart meters are exposed to intentional attacks. The results show that if smart meters are not designed to inherently detect and prevent cybersecurity attacks, a huge number of expenditures can be incurred to ameliorate the effect of this attacks. A section of the research shows how utility monitoring systems may be completely disconnected from remote smart meters under cyber-attacks. When such attacks take place, attackers can leverage hacking software's to re-establish a connection to the smart meter and take control of it.

Disclaimer: It is important to note that the experiments in this Thesis does not try to promote or favor a particular smart meter over another. Rather, the work presented here provides limited evaluations to get insight of the working of selected electric smart meters when subjected to limited cyber security attacks available in our lab.

# REFERENCES


[1] S. McLaughlin, D. Podkuiko, and P. McDaniel, “Energy Theft in the Advanced Metering Infrastructure,” CRITIS'09 Proceedings of the 4th international conference on information infrastructures security, pp.176-187, 2009.

[2] Ponemon Institute, “Critical Infrastructure: Security Preparedness and Maturity,” July 2014, online:http://www.hunton.com/files/upload/Unisys_Report_Critical_Infrastructure_Cybersecurity.pdf, retrieved Oct 2014.

[3] R. Anderson and S. Fuloria, “Who controls the off switch?” 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, USA, Oct 2010.

[4] E. Naone, “Hacking the Smart Grid,” MIT Technology Review 2010. Online: http://www.technologyreview.com/news/420061/hacking-the-smart-grid/, retrieved Sep 2014.

[5] Ping Yi; Ting Zhu; Qingquan Zhang; Yue Wu; Jianhua Li, “A denial of service attack in advanced metering infrastructure network,” Communications (ICC), 2014 IEEE International Conference on, vol., no., pp. 1029-1034, 10-14 June 2014. DOI: 10.1109/ICC.2014.6883456.

[6] P. McDaniel and S. McLaughlin, “Security and privacy challenges in the smart grid,” IEEE Security Privacy, vol. 7, no. 3, pp. 75–77, May 2009.

[7] F. M. Cleveland, “Cyber security issues for advanced metering infrastructure (AMI),” in 2008 IEEE Power and Energy Society General Meeting -Conversion and Delivery of Electrical Energy in the 21st Century, July 2008, pp. 1–5.

[8] Energy Information Administration, Frequently Asked Questions, online: http://www.eia.gov/tools/faqs/faq.cfm?id=108&t=3, retrieved Oct 2014.

[9] The Edison Foundation, “Utility-Scale Smart Meter Deployments, Plans, and Proposals,” 2012. Online:http://www.edisonfoundation.net/iee/documents/iee_smartmeterrollouts_0512.pdf, retrieved Oct 2014.

[10] SmartGrid.gov “What is the Smart Grid”. https://www.smartgrid.gov/the_smart_grid/smart_grid.html

[11]Sanjeev Kumar, Harsh Kumar and Ganesh Reddy Gunnam “Security integrity of data collection from smart electric meter under a cyber-attack” 2nd international conference on data intelligence and security page 5-9

[12Wi-Fi. Online: https://en.wikipedia.org/wiki/Wi-Fi, retrieved January 2021

[13]Wireless Networking(Wi-Fi)- Advantages and Disadvantages to Wireless networking, Online: https://ipoint-tech.com/wireless-networking-wi-fi-advantages-and-disadvantages-to-wireless-networking/, retrieved January 2021.

[14] Ethernet. Online: https://en.wikipedia.org/wiki/Ethernet, retrieved January 2021

[15] Limitations and Benefits of Wired Networks. Online: https://www.hitechwhizz.com/2020/03/4-advantages-and-disadvantages-drawbacks-benefits-of-ethernet.html, retrieved January 2021

[16] Tiago D. P. Mendez, Radu Godina, Eduardo M. G. Rodriques, Joao C. O. Matias and Joao P. S. Catalao “Smart Home Communicatin Techologies and Applications: Wireless Protocol Assessment for Home Area Network Resources.

[17] Wireless Networking-Advantages and Disadvantages to wireless networking. Available: https://ipoint-tech.com/wireless-networking-wi-fi-advantages-and-disadvantages-to-wireless-networking/

[18] Communication technologies in smart metering. Available: https://m2mserver.com/en/communications-technologies-in-smart-metering/

[19] Communication Technologies and Networks for Smart Grid and Smart Metering. Available:http://450alliance.org/wp-content/uploads/2014/05/WhitePaper_Comm_Tech_Networks_for_SmartGrid_SmartMetering.pdf

[20] Tutorial on ZigBee protocol basics. Available: https://www.rfwireless-world.com/Tutorials/Zigbee_tutorial.html

[21] Sadiq Ahmed, Taimoor Muzaffar Gondal, Muhammad Adil, Sabeeh Ahmad Malik and Rizwan Qureshi. A Survey on Communication Technologies in Smart Grid. Proceedings of the 2019 IEEE PES GTD Asia.

[22] Vehbi C. Güngö, Dilan Sahin, Taskin Kocak, Salih Ergüt, Concettina Buccella, Senior Member, Carlo Cecati, and Gerhard P. Hancke. 'Smart Grid Technologies: Communication Technologies and Standards". IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 7, NO. 4, NOVEMBER 2011.

[23] E.D. Knapp and R. Samani, Applied Cyber Security and the Smart Grid. Elsevier, pp. 147-159, 2013.

[24] E. Luiijf, "Understanding Cyber Threats and Vulnerabilities," J. Lopez et al. (Eds.): Critical Information Infrastructure Protection, LNCS 7130, Springer-Verlag Berlin Heidelberg, pp.52-67, 2012.

[25] F. G. Marmol, C. Sorge, O. Ugus, G. M. Perez, "Do not snoop my habits: preserving privacy in the smart grid," IEEE Communication Magazine, vol. 50, no. 5, pp. 166-172, May 2012.

[26] DDoS Attacks, Available online at https://burmabit.wordpress.com/2014/04/22/dos-attack/

[27] S. Kumar, "Impact of Distributed Denial of Service (DDoS) attack due to ARP-storm," published in The Lecture Notes in Computer Science -Book Series- LNCS-3421 – Networking-ICN 2005, part-II, vol. 3421, pp. 997-1002, April 2005, Publisher – Springer-Verlag

[28] Kumar, S. (2006) PING Attack—How Bad Is It. Computers & Security, 25, 332-337.

[29] Smurf Attack. http://en.wikipedia.org/wiki/Smurf_attack

[30] Ferguson, P. and Senie, D. (2000) Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing. RFC 2827, BCP 38.

[31] Vellalacheruvu, H.K. and Kumar, S. (2011) Effectiveness of Built-In Security Protection Microsoft's Windows Server 2003 against TCP SYN Based DDoS Attacks. Journal of Information Security, 2, 131-138. https://doi.org/10.4236/jis.2011.23013

[32] S. Kumar and E. Petana, "TCP protocol attacks on Microsoft's Windows XP-based Computers," International Conference on Networking, pp. 238-242, April 2008. Available from IEEE online library Xplore

[33]Gunnam, G.R. and Kumar, S. (2017) Do ICMP Security Attacks Have Same Impact on Servers? Journal of Information Security, 8, 274-283. https://doi.org/10.4236/jis.2017.83018

[34] S. Kumar, R. Valdez, O. Gomez, S. Bose, “Survivability Evaluation of a Wireless Sensor Network” – International Conference on Networking (ICN’06), April 2006;

[35]Praveen Vadda Sreerama Murthy Seelam, “Smart Metering for Smart Electricity Consumption” Schools Of Computing, Blekinge Institute Of Technology 37179 Karlskrona, Sweden. Master’s Thesis Electrical Engineering, May 2013.

[36]G. Dudek, A. Gawlak, M. Kornatka and J. Szkutnik, "Analysis of Smart Meter Data for Electricity Consumers," 2018 15th International Conference on the European Energy Market (EEM), 2018, pp. 1-5, diol: 10.1109/EEM.2018.8469896.

[37]Tellbach, Denise, and Yan-Fu Li. 2018. "Cyber-Attacks on Smart Meters in Household Nanogrid: Modeling, Simulation and Analysis" Energies 11, no. 2: 316. https://doi.org/10.3390/en11020316

[38] S. Kumar, H. Kumar, and G. R. Gunnam, "Security Integrity of Data Collection from Smart Electric Meter under a Cyber Attack," *2019 2nd International Conference on Data Intelligence and Security (ICDIS)*, 2019, pp. 9-13, diol: 10.1109/ICDIS.2019.00009.

[39] EPM 6100 Power Quality Meter Energy and Demand Submeter with Wi-Fi, Instruction Manual, GE Grid Solutions, Available online http://www.gegridsolutions.com/app/ViewFiles.aspx?prod=epm6100 &type=3

[40] Independent Statistics & Analysis, U.S. Energy Information Administrationhttps://www.eia.gov/energyexplained/index.cfm?page=electricity_home#tab2

[41] Harsh Kumar, “The Cybersecurity Evaluation of a Smart Electric Meter” Submitted to the Graduate College of The University of Texas Rio Grand Valley. May 2020.

[42] Sirisha Surisetty and Sanjeev Kumar, “Microsoft’s Windows7 Vs. Apple’s Snow Leopard: An Experimental Evaluation of Resilience against Distributed Denial of Service (DDoS) Attacks,” *IEEE Security and Privacy*, Vol.10, Issue 2, pp. 60-64, April 2012.

[43] Rodolfo Baez Jr., Sanjeev Kumar, “Apple’s Lion Vs. Microsoft’s Windows 7: Comparing Built-In Protection against ICMP Flood Attacks,” *Journal of Information Security*, vol. 5, no.3, pp. 123-135, July 2014.

[44] Surisetty, S, Dr. S. Kumar, “Is Apple's iMac Leopard Operating System Secure under ARP-Based Flooding Attacks?” Second International Conference on Internet Monitoring and Protection (ICIMP 2010).

[45] Sanjeev Kumar, Sirisha Surishetty, Apple's Leopard Versus Microsoft's Windows XP: Experimental Evaluation of Apple's Leopard Operating System with Windows XP-

SP2under Distributed Denial of Service Security Attacks, Information Security Journal: A Global Perspective, Vol.20 No.3, Page(s):163-172, 2011.

[46] S. Surisetty and S. Kumar, “Apple’s Leopard Versus Microsoft’s Windows XP: Experimental Evaluation of Apple’s Leopard Operating System with Windows XP-SP2 under Distributed Denial of Service Security Attacks,” Information Security Journal, 20:163–172, May 2011

[47] S. Surisetty and S. Kumar, “Evaluation of a Security Vulnerability in Apple’s Leopard Operating System,” International Conference on Internet Monitoring and Protection, May 2010. Available from IEEE online library Xplore

[48] S. Surisetty and S. Kumar, “Is McAfee SecurityCenter/Firewall Software Providing Complete Security for your Computer?” International Conference on Digital Society (ICDS’10), Feb. 2010. Available from IEEE online library Xplore

[49] S. Kumar, R. Valdez, O. Gomez, S. Bose, “Survivability Evaluation of a Wireless Sensor Network” – International Conference on Networking (ICN’06), April 2006; Available from IEEE online library Xplore

[50] S. Kumar, M. Azad, O. Gomez, and R. Valdez, “Can Microsoft’s Service Pack 2 (SP2) Security Software Prevent Smurf Attacks?” Proceedings of the Advanced International Conference on Telecommunications (AICT’06), Feb 2006.

[51] S. Kumar and T. Doganer, “Effect of Scan-Planes on the Memory Bandwidth of Sliding Window Switch Architecture,” - Proceedings of the IEEE Workshop on High Performance Switching and Routing (HPSR05), May 2005.

[52] S. Kumar "On Impact of Distributed Denial of Service (DDoS) attack due to ARP storm, Lecture Notes in Computer Science – Book Series, LNCS-3421, Networking - ICN 2005, Part-II, Publisher: Springer-Verlag, April 2005.

[53] S. Kumar and T. Doganer, “Memory-Bandwidth Performance of the Sliding-Window based Internet Routers/Switches,” Proceedings of the IEEE Workshop on Local and Metropolitan Area Networks, San Francisco, CA, April 2004.

[54] S. Kumar, T. Doganer, A. Munoz, “Effect of Traffic Burstiness on Memory-Bandwidth of the Sliding-Window Switch Architecture,” Proceedings of the International Conference on Networking, March 2004.

[55] S. Kumar, A. Munoz, T. Doganer, “Performance Comparison of Memory-Sharing Schemes for Internet Switching Architecture,” Proceedings of the International Conference on Networking, March 2004.

# BIOGRAPHICAL SKETCH

Patrick Nnaji was born on June 3rd, 1992. He has completed his Diploma in Electronic Engineering from The University of Nigeria Nsukka, Nigeria in July 2015. He has completed his Master of Science in Electrical Engineering from University of Texas Rio Grande Valley, Texas, USA in August 2021. He also worked as a Research Assistant in in Network Research Lab at UTRGV from September 2019 to August 2021. He also worked as a Teaching Assistant Computer Engineering department at UTRGV from August 2019 to August 2021.

Address:

5275 Town and Country BLVD.

Frisco, Texas, USA, 75034.