5-2020

Cyber Security Evaluation of Smart Electric Meters

Harsh Kumar
The University of Texas Rio Grande Valley

CYBER SECURITY EVALUATION OF SMART ELECTRIC METERS

A Thesis

by

HARSH KUMAR

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

May 2020

Major Subject: ELECTRICAL ENGINEERING

CYBER SECURITY EVALUATION OF SMART ELECTRIC METERS

A Thesis
by
HARSH KUMAR

COMMITTEE MEMBERS

Dr. Sanjeev Kumar
Chair of Committee

Dr. Jun Peng
Committee Member

Dr. Weidong Kuang
Committee Member

May 2020

ABSTRACT

Harsh Kumar, Cyber Security Evaluation of Smart Electric Meters. Master of Science in Engineering (MSE); May 2020, 131 pp., 17 table, 108 figures, 74 references.

In this thesis, effect of intermediate network systems on power usage data collection from Smart Electric Meter in Smart Grid was evaluated. Security integrity of remote data collection from GE's Power Quality Smart Electric Meter EPM 6100 and EPM 7000 under cyber-attacks were evaluated. Experimental security evaluations of Smart Electric Meters were conducted to understand their operation under cyber-attacks. Integrity of data communication between the GE's smart meters and remote monitoring computer was evaluated under different types of cyber security attacks. Performance comparison was done for security integrity of EPM 6100 and EPM 7000 power quality meter under various cyber-attacks.

DEDICATION

The completion of my master's studies would not have been possible without the love and support of my family. I would like to dedicate my thesis to my parents, Sheela Devi, Uma Shankar Tiwari, my sister, Sonal, my uncle Upendra Kumar Tiwari and my brother Shashi Shekhar Dubey, they wholeheartedly inspired, motivated and supported to accomplish this degree. I would like to thank my friend Chu Wen Cheng, Oscar A Alvarez, Elizabeth Cantu Deyarmin, Chintan Patel Sir, Sudeshna Ghosh Madam, for your support and believe. Thank you for your love and patience.

ACKNOWLEDGEMENTS

I will always be grateful to Dr. Sanjeev Kumar, chair of my thesis 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 thesis committee members: Dr. Wiedong Kuang, and Dr. Jun Peng. Their advice, input, and comments on my dissertation helped to ensure the quality of my intellectual work.

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 and colleagues at Dr Kumar’s Network Research Laboratory in ECE Department at UTRGV. Also, I would like to acknowledge the many volunteers who participated in the focus group research.

Work in this thesis is based upon the grant awarded to Dr. Sanjeev kumar the US National Science Foundation under Grant No. 0421585, Houston Endowment Chair in Science, Math and Technology Fellowship, Lloyd M. Bentsen, Jr. Endowed Chair in Engineering fellowship, and UTRGV Presidential Graduate Research Assistant (PGRA) scholarship funding.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

Motivation has been important factor in order to understand and respond to cyber-attacks. Cyber-attacks targeted towards Advanced Metering Infrastructure (AMI) disrupt a nation's critical infrastructure. Even casual crackers/ hackers seeking to test their skills are attracted to such a prominent target. Industrial espionage and other business disruptions, whether politically motivated or not, are another key motivation. Additionally, some attacks may seek to utilize Smart Grid as a launching point for other Internet attacks by virtue of the vast number of devices, their ability to initiate many-pronged attacks, and even their ability to hide malicious data through dispersion among many nodes [1].

According to research by Ponemon [2], the organizations managing the U.S. critical infrastructure facilities are not well prepared for the attacks, if it takes place [2]. All nations are vulnerable without making the smart meters resilient. Smart meters have been game changers for cyber attackers, affording them a rich new resource for widespread disruption [3]. Beyond the Denial of Service, Theft of Power, and Disruption of Grid attacks on the power grid symptoms of AMI network attacks include unauthorized web pages posted on Internet-connected web servers collecting data, outbound data transmissions using unknown protocols and ports, huge compressed file transmissions over AMI networks, unusual data load between data collectors and the smart meters, and unusual log entries. According to the 2014 McAfee report [4], 80% of the surveyed electric utilities have faced at least one large-scale Denial of Service (DoS) attack to their communication networks, and 80% of the utilities have suffered network infiltrations.

It indicates in one years' time that one in four have been the victims of cyber extortion or threatened cyber extortion; denial of service attacks had increased from 50% to 80% of respondents; and approximately two-thirds have found malware designed to sabotage their systems. Potential cyber security threats and vulnerabilities existing in the AMI are analyzed in [4]. For a specific DoS attack targeted at the AMI communication network, the attack model and its physical impact are proposed in [5], where an attacker may compromise the AMI devices and disrupt data traffic on the network. A malicious attack targeting smart meters is introduced in [6], where an attacker can alter the meter measurement data. A cyber-attack scenario of an attacker hacking the AMI communication network and performing DoS attacks are simulated in [7].

Cyber security of AMI was recently a topic of major interest at a Black Hat conference where some vulnerabilities and simulated attacks were demonstrated [4]. Yi et al [5] demonstrated a specific denial of service attack where an attacker may select any node and disrupt traffic on the AMI network. Attackers may also compromise a smart meter to change energy usage data or fabricate other meter data [6]. Cleveland [7] discussed an example of a possible scenario of a smart hacker cracking AMI security and sending 5 million remote disconnect commands. As of 2012, over 43 million smart meters have been installed in the U.S., 89% of which are residential with the remainder to commercial and industrial consumers [8].

According to the Institute for Electric Efficiency smart meter deployment projections, approximately 65 million smart meters will be deployed in the U.S. by 2015 [9]. The cost of AMI is huge given this scale, and frequent replacement with more secure units is extremely cost prohibitive. This research adds value in a concurrent way by aiding understanding of AMI cyber security exposure, which enables utilities to be more informed regarding the security posture of AMI.

1.1 Smart Grid

Term “grid” here refers to the electrical grid, a network consisting of transmission lines, substations, transformers, and power generators which deliver electricity from electric power plant to houses and industrial or business premises. “Smart” denotes digital and internet-based technology that helps set up two-way communication between a utility and its customers. It has ability to sense the transmission lines parameters.

These grids have been a new concept with multiple benefits to both customers and utilities. The main idea behind using this technology is that this offers internet-based communication. Having the knowledge of the energy a user consumes make him/her aware of energy waste created. Energy waste reduction is also an energy cost reduction. Some Key benefits of smart grid are more efficient electricity transmission, quick electricity restoration after power disturbances, less operations and management costs for utility company, and hence lower power costs for consumers, reduced peak demand, which helps lower down electricity rates, increased integration of large-scale renewable energy systems, better integration of customer-owner power generation systems, including renewable energy systems and improved security [10-17].

The smart grid is modernization of the existing electrical manual reading system, which gives an option to remotely monitor, control and usage prediction for customers and utilities. Smart grid enables application of digital technology, internet-based communication with electric power network. Smart grid makes the performance of the electric network more reliable, controllable, and more cost effective.

The smart grid is a complex cyber-physical system (CPS) incorporating various spatially distributed subsystems including sensors, actuators, and controllers, which is expected to be a critical technological infrastructure for our nation [18].

1.2 Advanced Metering Infrastructure

To realize the Smart Grid, Advanced Metering Infrastructure (AMI) is an important key based on smart meters. Advanced Metering Infrastructure (AMI) refers to the full continuous measurement and data collection system used by meter manufacturers and utility companies. AMI additionally refers to the communication networks between the client and a service supplier, and data reception and management systems that make the information available to the service provider. AMI replaced AMR (Automatic Meter Reading) whose purpose was the reading of data from the meter. The main difference between AMI and AMR is the two-way communication that AMI offers is shown in (Figure 1.1) [15,19].

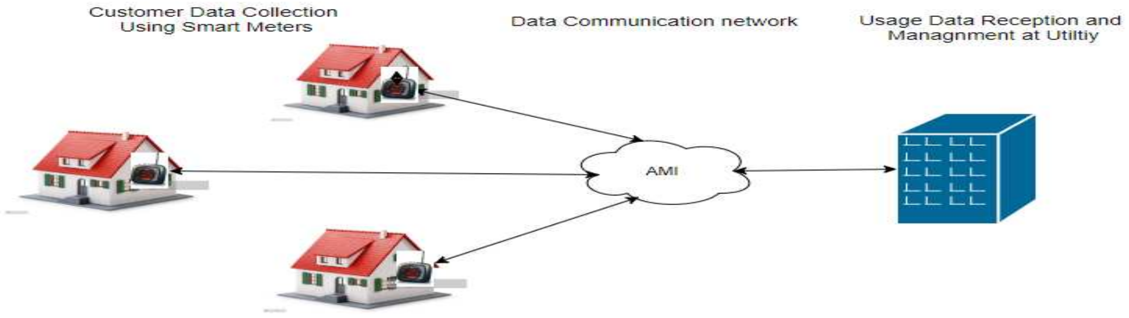


Figure 1.1: Advanced Metering Infrastructure.

AMI is rapidly being deployed due to its ability to provide remote meter reading and control. The implementation of AMI is widely seen as the first step in the digitalization of the electric grid control systems. The AMI is the architecture for automated two□way communications between smart meters and utility companies.

The AMI includes smart meters at customer premises, access points, communication backbone network either wired or wireless between customer and service providers, and data management systems to measure, collect, manage, and analyze the data for further processing. The smart meter periodically sends the collected information back to the utility company for load monitoring and billing purposes. Besides remote collection of automated data from smart meter readings are also critical for the control center to implement Demand/Response mechanism. By using smart meters, customers can control their power consumption and manage how much power they are using, particularly managing the peak load. In particular, the AMI network can include thousands of smart meters, multiple access points, wired communication network using switches, routers or modems using Ethernet, optical cable, power line communication and wireless communication networks using WI-FI, Wireless Local Area Network (WLANs), Radio frequency (RF), which is created for data routing purposes from customer to the utility [10-19].

There are two classes of AMIs used today – wireline based AMIs and wireless based AMIs. Different AMIs are suitable for deployment in different types of environment. Wireless interference can corrupt power uses data as a result in many environments wireline AMIs are more suited for deployment especially in new built dense areas. Many dense areas may consider deploying Ethernet based AMIs for ease of access and accuracy of remote data collections. Ethernet based AMIs deploy switches and routers for data communication from smart meter at consumer premise to the utility company for billing and control purposes. The AMI is one important element of the smart grid being implemented allowing for bi-directional communication between electric utility companies and customers [20-22]. The AMI mainly integrates the information/communication network, smart meters, and meter data management system (MDMS).

The communication network of the AMI is primarily comprised of three important areas including Home Area Network (HAN), Wide Area Network (WAN), and the utility system. Smart meters are the main customer-side installed electronic devices in the AMI, which forward the customers' electricity consumption information to the electric utility. The utility then integrates this information to generate electricity bills, enable demand response, predict user electricity consumption patterns, and update pricing in real time.

1.3 Smart Electric Meter

Smart electric meter is an important component of the smart grid technology which is commercially being deployed very rapidly. More than half of the US population is now using smart meters [41] which is almost 65 million smart meters, a milestone that would not have been met until 2019 based on pre-ARRA utility plans and proposals [9].

Smart electric meters are connected over wireline or wireless network, helps in remote monitoring and data collection such as power consumption at a customer premise by the service provider. The smart meters at customer premise can also be used to remotely control smart appliances such as smart air conditioning, smart refrigerator, smart lights, smart locks, smart cameras, smart smoke detectors etc. by interfacing these appliances to the smart meters. In electric power system smart electric meters uses internet of things (IoT) for automatic meter reading locally as well as to remote data collection. It led to the modernization of old manual data reading system and hence called automatic metering infrastructure. Automatic metering infrastructure helps set up 2-way communication between meter and the utility companies.

Smart meters allow usage of digital system, Internet of things (IoT), Internet based communication within electric power system or network which makes the performance of the electric power system more reliable, controllable, and even cost effective.

Smart meters are valuable part of the electric power network which is being deployed rapidly both residentially and commercially. Smart meters are IoT-ready devices which will have access to rich, real-time data which helps utility to provide better service alongside reducing costs and boosting profit.

It also helps in effectively manage electric loads, reduce power outages and streamline energy distribution through more accurate forecasting. While smart electric meters provide convenience of remote monitoring and data collection for power usage information via various network protocols, they also can become vulnerable to Cyber-attacks which in turn can hamper the integrity of power usage data collection and reporting.

1.4 Statement of Purpose

The security of Advanced Metering Infrastructure (AMI) has recently become an area of interest as its deployment has grown. The affinity towards AMI by utility companies, energy markets, and regulators is primarily to facilitate near real-time collection of power flow and usage data. This will allow utilities to provide dynamic pricing services, demand response, and perform better management of the power grid, although these new abilities increase the chances of cyber-attack [23-24]. Smart meters are installed at homes, buildings, and other facilities of the power consumer and thus, the vast number in deployment will be in the many of millions [6-7].Like any nascent system, AMI have yet to establish security measures to handle cyber-attacks beyond rudimentary measures commonly employed in general, e.g., network encryption. A cyber-attack is an attempt by hackers to damage or destroy a computer network or system.

Attacks can vary in complexity, magnitude, and impact. A cyber-attack on AMI may involve intelligence gathering, infecting the target AMI systems, AMI exploitation, exfiltration of data from various attack points of AMI, and maintaining control [25-26].

The cyber-attack surface can be defined by the methods an environment or a system can be attacked by an adversary to introduce or retrieve data from that environment or system. A targeted attack on AMI could potentially result in shutdown of the power grid, disabling energy delivery systems [27]. This could have devastating effects on government, trade, commerce, banking, transportation and other important aspects, which rely on energy to operate [24]. A compromise of AMI may also result in an invasion of privacy [28] and provide a platform from which to extract information from users such as Internet activity, financial, or health records. As a critical point between electric utilities and customers, the security of AMI is an important area for the smart grid monitoring and operation and the customers' privacy. For example, a malicious attacker can manually compromise smart meters and change the meter measurements, affecting the integrity of reported data. Moreover, the information and communication technologies (ICTs) integrated with the AMI opens window for potential hackers, where cyber-attacks can compromise electronic devices, and insert bad data into the communication network. Owing to the expansive deployment of the AMI devices, these cyber-physical attacks can have the potential to disconnect electricity from end consumers, even leading the cascading failures in smart grid and other connected critical infrastructures such as transportation and telecommunications. There are two main attack platform in the AMI including the smart meter and the communication network. Smart Meters are electronic devices which records consumption and then reports this information back to the utility, often in assigned intervals. Smart meter facilitates the dash boarding of smart grid system monitoring, automated operation, system recovery, dynamic electricity pricing, and more consumption-based customer services. Traditional meters were already susceptible to physical attacks due to their importance, but smart meters open another window that cyber attackers can get access to.

In design, smart meters are purchased in bulk (by the millions) and thus driven by low cost. As a result, internal hardware and firmware may limited. In the sense of capabilities, it means that security often takes a backseat when design must meet both the cost and requirements. Coupled with the vast number in deployment and limited defense resource, a series of the theoretical and demonstrated attacks aimed at compromising smart meters [33-40], [55-73] such as Denial of Service (DoS) Attacks compromise smart meters by overwhelming a network or tampering with the routing. This attack can render a meter incapable of responding to any request from electric utilities or consumers.

False Data Injection Attacks (FDIAs) insert random and/or deliberate errors within normal smart meter traffic activity to cause corrupted measurements to deliberately cause issues in the smart grid network. De-pseudonymization Attacks compromise identity and privacy of smart meter data. Man-in-the-Middle Attacks where attackers can place themselves between electric utilities and customers. Meter Spoofing and Energy Fraud Attacks can get the ID number of smart meters through physical access. Authentication Attacks can authenticate hackers as a valid customer via methods such as stealing a session or acquiring the authentication from memory. Disaggregation Attacks attempt to profile customer energy consumption behavior. The communication network is a key component of the AMI that links the devices using a wireless or wired network. The AMI communication network usually accomplishes 2-way communication between the user and the utility.

The communication network of AMI and the potential cyber-physical attacks targeted at the network. the link to the local HAN on the consumers’ side through WIFI, Zigbee or Z-wave protocols. The communication network then connects to the utility’s WAN, which is usually an Ethernet infrastructure.

Moreover, the communications network is distributed through an urban sector in company with the smart grid. The scale of this network can vary from a couple of hundreds to thousands of smart meter data collector devices. Each collector is capable of serving thousands of smart meters, raising the number of devices to multiple thousands or millions in total. Therefore, the vulnerabilities of the AMI communication network can be exploited or disabled by attacks on the underlying communication infrastructure, insertion of false user requests, unauthorized alteration of demand side schedules and illegal market manipulation; all of which can impact system operations and result in both power shortage, loss of trust and negative economic impacts. The potential and demonstrated attacks aimed at the communication network [4-7],[11],[29], [30-32] such as Distributed Denial of Service (DDoS) Attacks which target AMI communication networks' data collector, preventing the normal communication between Wide Area Network (WAN) and Neighborhood Area Network (NAN). False Data Injection Attacks (FDIAs) introduce random and corrupted data within standard traffic activity in order to cause invalid measurements with the goal of disrupting the AMI network. Physical Attacks that compromise the smart meter data collectors and disrupt the communication between the electric utility and the end customer of power. DDoS Attacks in the AMI communication networks that attack the WIFI/ZigBee networks in Home Area Network (HAN). Internet Attacks that compromise the software and systems in electric utilities. Data Confidentiality Attack attempts to compromise the information between electric utilities and end customers by targeting the hardware within the AMI communication network.

It is important to understand the impact of cyber security attack on smart electric meter. Cyber security has been a top concern for electric power companies deploying smart meters and smart grid technology. Despite the well-known advantages of smart grid technology and the smart meters, it is not yet very clear how and to what extent, the Cyber-attacks can hamper the operation of the smart meters, and remote data collections regarding the power usage from the customer sites. Given that the possibility of compromising the information transmitted is real, efforts to ensure the security must be done. Cyber security in smart grid and smart meter is the field of research that must secure the information from all the aspects of the security triad (confidentiality, integrity, and availability). As such, using a small-scale simulation of the process done by one of the utility companies, our research showcases a series of experiments performed on smart meters with ethernet-based communication to evaluate the smart grid when subjected under cyber-attacks. To understand these questions, experiments were conducted in a controlled lab environment of Network Research Lab at UTRGV to test commercial grade smart meters i.e. EPM 6100 and EPM 7100 from General Electric. In this thesis different results from investigation done on commercial grade smart meters from GE under different cyber-attack conditions were going to be presented. In this thesis, the impact on customers' power consumption due to Ethernet based AMIs while delivering data from the customer premise to the utility companies in a Smart Grid infrastructure was also evaluated.

1.5 Distributed Denial of Service Attacks

Distributed Denial of Service attack is different from Denial of service attack. In Distributed Denial of Service attack several attacker's attacks one target device server. First attacker develops the zombie or Daemon or Agent. It is a malicious software's which are instructed to attack the target at specific time.

And then attacker tries to multiply the numbers of attackers by installing virtually the zombie at the internet user PCs which may be located at another external network to attack the target [42]. By doing this, the attacker network become giant. We call it “Botnet”. And finally, Victim devices servers are waiting for the command which would be sent by the attacker via the zombie to attack the Target. In DDoS attack, the target can be affected directly or indirectly. In indirect attack, Attacker can multiply the number of zombies to attack the single target [42].

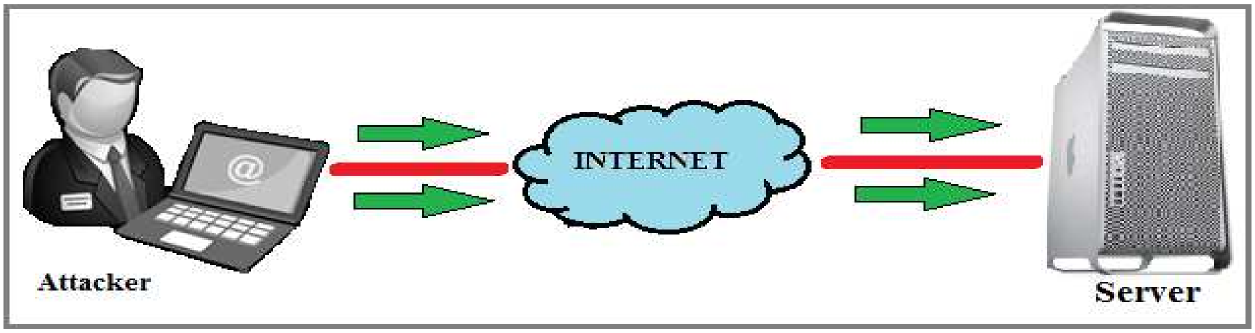


Figure 1.2: Denial of Service Attack [42]

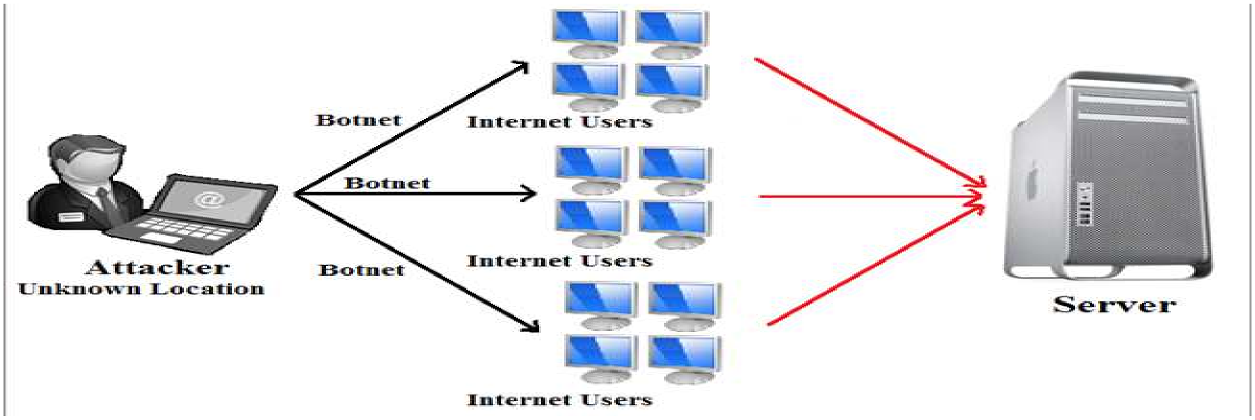


Figure 1.3: Distributed Denial of Service Attack [42]

1.5.1. ARP Flood Attack

The ARP protocol was designed for translation of addresses between the second and third layers of the OSI model. The Data link layer uses MAC addresses to communicate between different hardware devices directly on a small scale.

The Network layer uses IP addresses to create large scalable networks that can communicate across the globe. ARP cache poisoning is one of the oldest forms of modern MITM (Man in the middle) attack. It allows an attacker on the same subnet as its victims to eavesdrop on all network traffic between the victims.

The devices which were using ARP protocol will accept updates at any time whereas the devices with DNS protocol will accept only secure dynamic updates. This means that any device can send an ARP reply packet to another host and force that host to update its ARP cache with the new value. Sending an ARP reply when no request has been generated is called sending a gratuitous ARP. When malicious intent is present the result of a few well-placed gratuitous ARP packets used in this manner can result in hosts who think they are communicating with one host, but, communicating with a listening attacker.

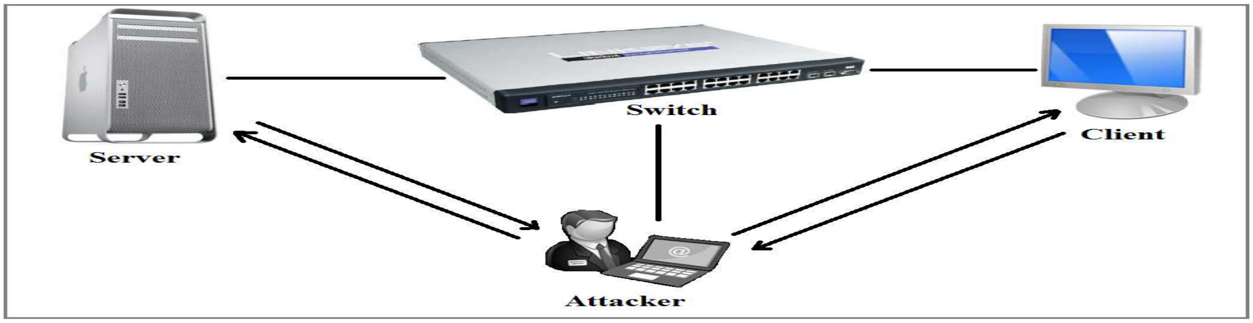


Figure 1.4: ARP Flood Attack [70]

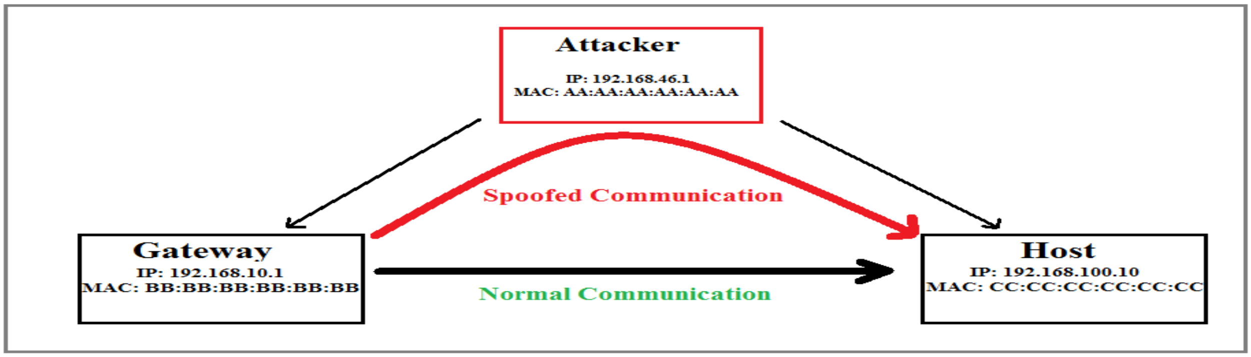


Figure 1.5: ARP Flood Attack Operation [70]

The direct communication from Gateway to Host is the original standard traffic. The spoofing of the ARP Replies (the Gratuitous ARP Replies) convincing both sides they should send the data to the attacker. In a spoofed communication path, attacker listening in the middle of Gateway and Host.

1.5.2. Ping Flood based DDoS Attack

Ping Flood Attack is one of the oldest known network attacks, and its aim is to saturate the network with ICMP (Internet Control Message Protocol) traffic.

ICMP Ping is used to verify the end-to-end internet path operation, where ICMP Echo request packet is sent to the target machine and an ICMP Echo Reply packet is expected to confirm communication between sender and receiver [43].

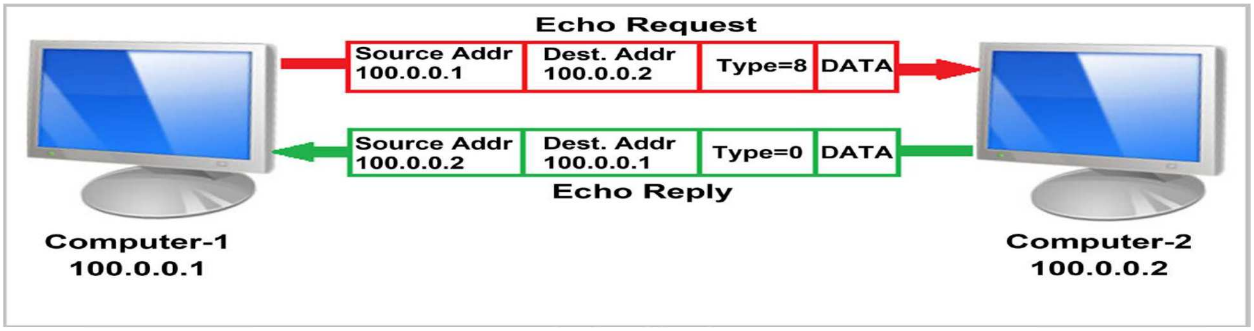


Figure 1.6: Ping Utility [45]

A router, or a host, uses an ICMP echo request (ping) message to test a destination’s reachability. A computer system that receives an ICMP echo request message will respond to it by sending an ICMP echo reply message back to the sender (Figure 1.6). Using this, an ICMP echo request and reply messages together can test the reachability of a computer on a network [44]. The ICMP echo request and reply messages are identified by the value of the type field in the ICMP message format [46]. If the value of type field is equal to 8, it becomes echo request, if the value of type field is equal to 0, it becomes an echo reply [44].

These Ping based DDoS attacks are flood of a large number of ping messages sent to target are known to be quite damaging to the availability of the web-based services.

The Ping attack can exhaust the target server's bandwidth and computing resources [45]. The victim computer continues receiving a Ping message that generates an ICMP echo reply message sent to the source address of the Echo Request.

1.5.3. Smurf Attack

A more sophisticated version of a DDoS attack is commonly known as a SMURF attack. A SMURF attack utilizes massive number of ICMP packets of spoofed source Internet Protocol (IP) addresses targeting the (Figure 1.7). This is achieved by altering the Echo Request sent to the botnet using an IP broadcast address [44] [46]. The larger the Botnet is the faster and the bigger is the flood of Echo reply messages [47]. The increase of traffic reduces the target server's ability to respond and can quickly cause a complete denial of service [48] [49].

In this attack both the ICMP echo request and ICMP echo reply messages are used. While the perpetrator sends ICMP echo request messages to an unprotected broadcast domain for amplifying the attack, the victim computer actually receives amplified attack traffic that comprises mainly of ICMP echo reply messages. If the broadcast domain has N number of computers, then for each ICMP echo request broadcasted in such a domain will generate N number of ICMP echo reply messages that are sent to the victim's server, due to the spoofed source address in the ICMP echo request messages [43].

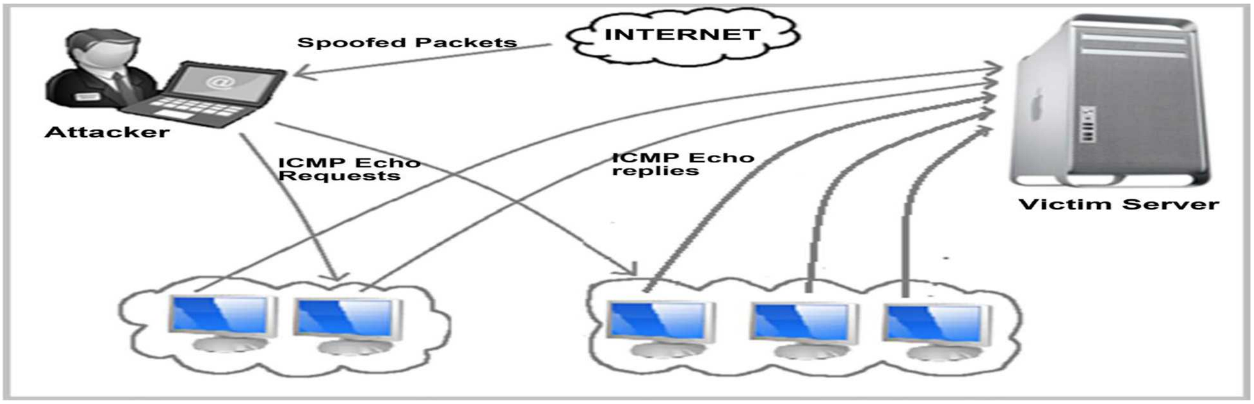


Figure 1.7: SMURF Attack [50]

1.5.4. TCP-SYN Flood Attack

The Transmission Control Protocol (TCP) connection-oriented transport-layer protocol that provides reliable byte-stream delivery between two hosts on a network [51]. TCP uses a three-way handshake to establish a network connection. Before a client attempts to connect with a server, the server must first bind to and listen at a port to open it up for connections: this is called a passive open. Once the passive open is established, a client may initiate an active open. In this three-way handshake method first step is the active open is performed by the client sending a SYN to the server. The client sets the segment's sequence number to a random value A. The server sends back SYN-ACK (Synchronize-Acknowledgement) to the client [52]. The acknowledgment number is set to one more than the received sequence number i.e. A+1, and the sequence number that the server chooses for the packet is another random number, B. And finally, client sends an ACK back to server. The sequence number is set to the received acknowledgement value i.e. A+1, and the acknowledgement number is set to one more than the received sequence number i.e. B+1

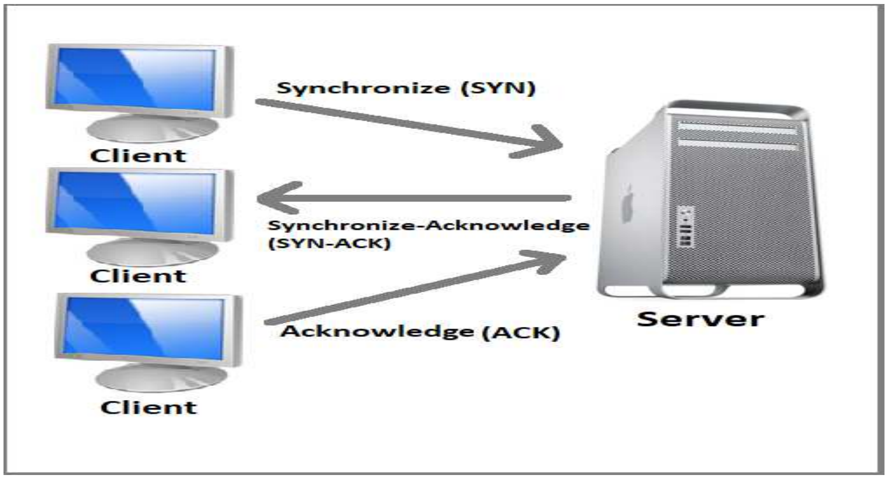


Figure 1.8: Normal 3-way handshake [48]

In this TCP-SYN Attack, the attackers send SYN to server and then server sends SYN-ACK back to attacker, but the attacker won't send Acknowledge (ACK) back to server. Because of this the server is still waiting to get ACK to establish a connection. If the attacker keeps on doing this process the server is going to crash and it's not responds to legitimate users also.

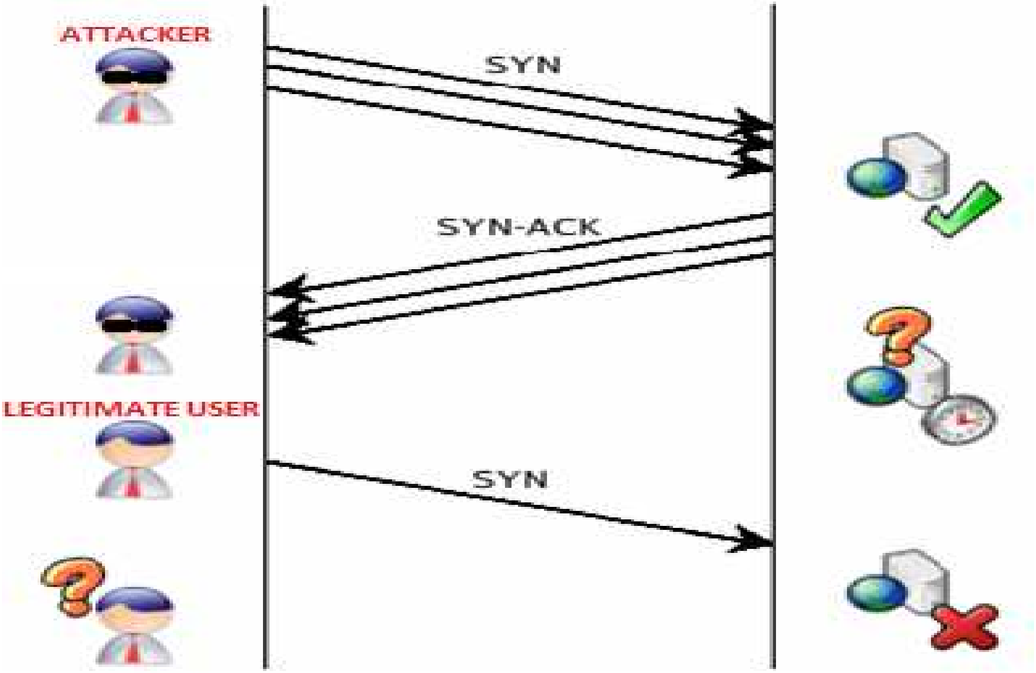


Figure 1.9: TCP/SYN Flood Attack [48]

1.6 Thesis Outline

In this thesis, performance of Smart Metering Communication against different Distributed Denial of Service (DDoS) attacks was investigated and cyber security of Smart Electric Meter against DDoS attacks was evaluated. In Chapter I, introduction of Smart Grid, Smart Electric Meter, Advanced Metering Infrastructure, Distributed Denial of Service attacks and I also mentioned different types of security challenges in Advanced Metering Infrastructure was discussed. In Chapter II, Effect of intermediate network systems on remote power usage data collection in Smart Grid was measured. In Chapter III, security integrity of data collection from EPM 6100 Power Quality Smart Electric Meter under a cyber attack was evaluated. In Chapter IV, I security integrity of data collection from EPM 7000 Power Quality Smart Electric Meter under a cyber-attack was evaluated. In Chapter V, performance of Smart Metering communication of EPM 6100 and EPM 7000 Smart Power Quality Meter under different cyber-attacks was evaluated. In Chapter VI, I security integrity of data collection and performance of Smart Metering communication of EPM 6100 and EPM 7000 Power Quality Smart Electric Meter under different cyber-attacks was compared.

CHAPTER II

EFFECT OF INTERMEDIATE NETWORK SYSTEMS ON REMOTE POWER USAGE DATA COLLECTION IN SMART GRID

This chapter investigates impact of intermediate switches on remote collection of power consumption data in Smart Grid. Advance metering infrastructure (AMI) is one of the important components in the overall architecture of the Smart Grid. Implementation of AMI was a topic of research lately as there are many different implementations being used in today's Smart Grid. One of the AMI network is Ethernet based infrastructure for the access of remote power consumption from the customer premises. In this chapter, we are investigating impact of Ethernet switches on the power consumption data reported to the utility companies. This chapter investigates the impact on the customer power consumption by utilizing commonly used Ethernet switches from different companies. Power consumption data in the presence of Ethernet switch is compared with the baseline Power consumption data when no switches were used. Experimental work as discussed in this chapter shows a clear impact on customer power consumption due to the Ethernet based Advanced Metering Infrastructure. With all the added advantages of AMI based smart meter communication in smart grid there is not enough research published which investigated reliability and integrity of data (collected from smart meters) being communicated to utility over AMI based networks in the Smart Grids. Furthermore, there is not enough work done to show the effect of Ethernet based AMI on overall power consumption.

There are two classes of AMIs used today – wireline based AMIs and wireless based AMIs. Different AMIs are suitable for deployment in different types of environment. Wired interference can corrupt power uses data as a result in many environments wireline AMIs are more suited for deployment especially in new built dense areas. Many dense areas may consider deploying Ethernet based AMIs for ease of access and accuracy of remote data collections. Ethernet based AMIs deploy switches and routers for data communication from smart meter at consumer premise to the utility company for billing and control purposes. In this chapter, we evaluate the impact on customers' power consumption when Ethernet based AMIs are used to deliver data from the customer premise to the utility companies in a Smart Grid infrastructure.

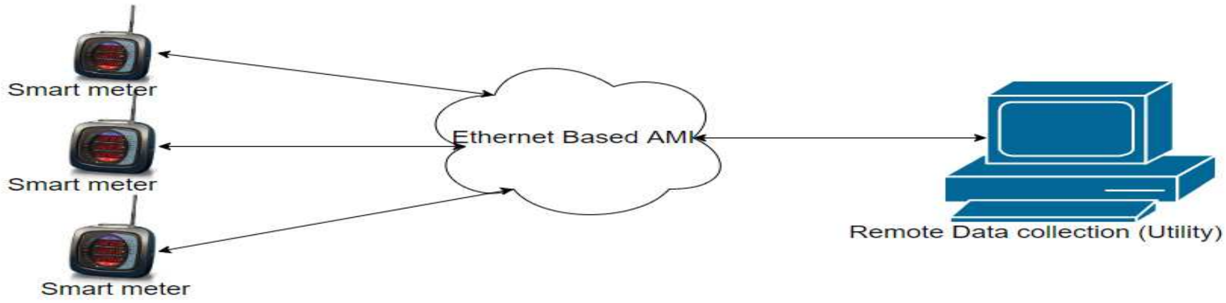


Figure 2.1: Ethernet based Advanced Metering Infrastructure (AMI) of Smart Grid

2.1 Experimental Set Up

For intermediate network system in AMI configuration, different switches were used, namely the NETGEAR switch, a POE switch and a CISCO switch. Experiment consisted of two bulbs of 100 Watts each and two electric fans of 35 Watts each acting as load. A total load of 270 watts was used for the baseline set up. For smart meter, EPM 6100 power quality smart meter from GE was used which was energized from building power. The remote monitoring computer installed Ener Vista data communicator software from GE.

The setup can be observed in (Figure 2.2) Customers can read the usage data and set electrical parameters from front panel of the meter. Smart meters can be configured manually as well as remotely by software through which recording of the usage data can be achieved.

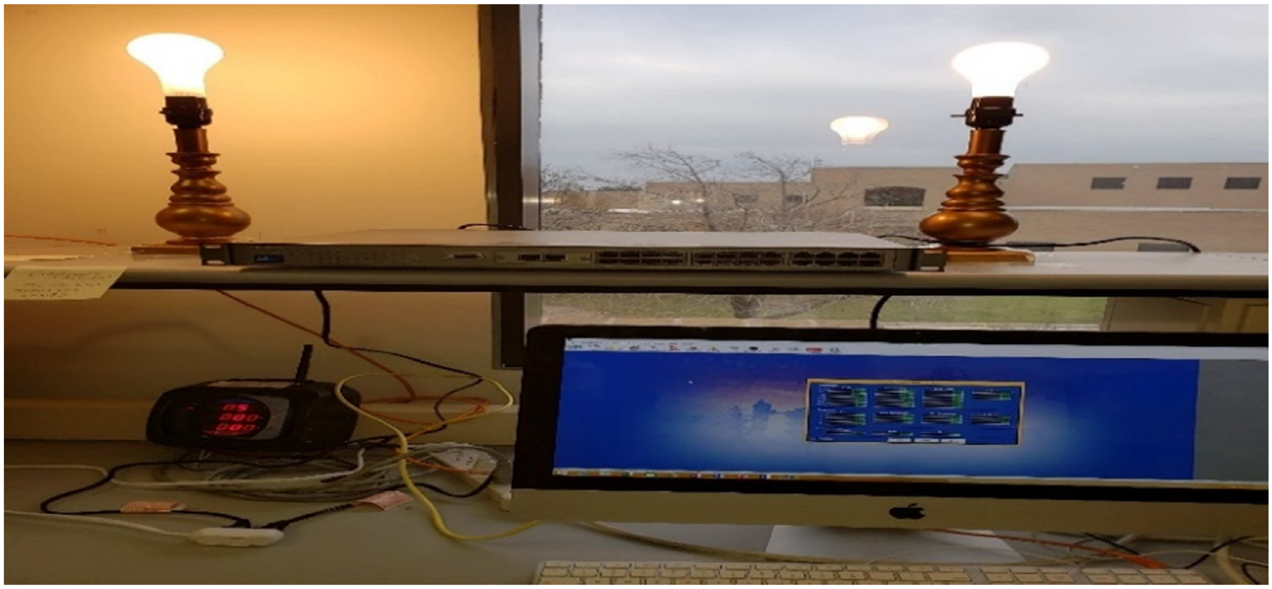


Figure 2.2: An Experimental Set up

The data communicator software supports several features to record various electrical parameters like the voltage, current Watt hours and phase angle between each of the phases. When the meter is being subjected under different loads, meter settings and electrical connections are to be changed. For each data communication session, electrical parameter value along with the consumed watt hours data are stored for billing purposes. The smart meter in this experiment provides automatic meter operations, automatic logs recording, automatic monitoring of parameters remotely and automatic usage data collection and recording.

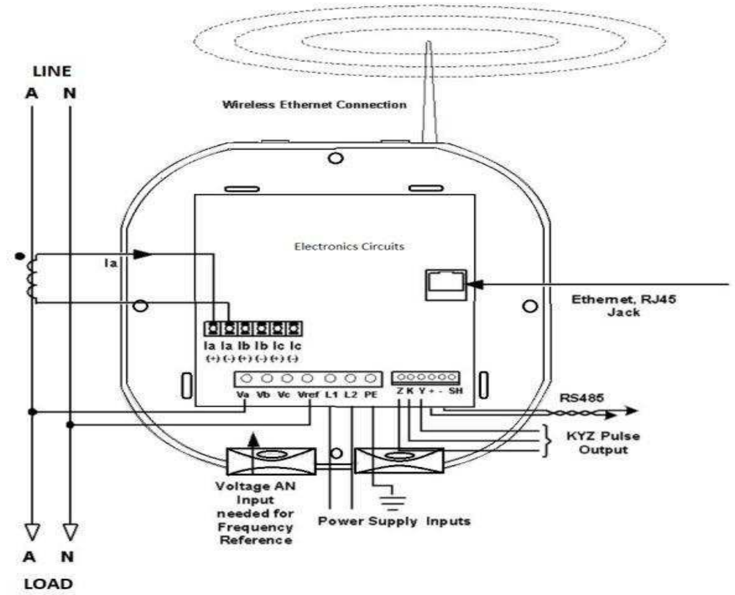


Figure 2.3: Smart Meter Programming Set up [54]

(Figure 2.3) shows the programming set up of the smart meter. It also depicts the internal electrical connection of a smart meter where the meter is connected to the load, intermediate network systems for the usage data communication and data collection. With the help of the figure we can also calibrate the meter by giving test pulses to check its operation and accuracy of the smart meter.

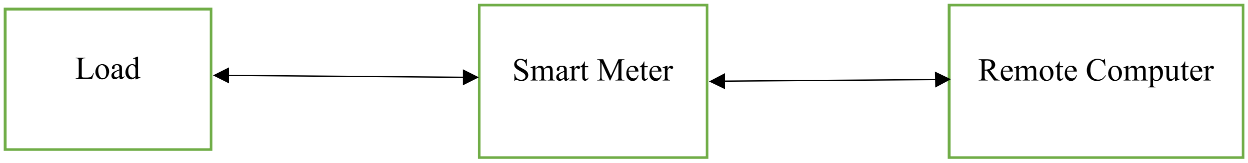


Figure 2.4: Baseline setup (without any Ethernet switch)

The experiment started with evaluating smart meter data collection through data communicator software and recording log file in remote computer. First goal of the experiment was to record the log file for baseline watt hours consumption data directly to the remote computer through set up displayed in (Figure 2.4).

Then started experimenting and recording log file for usage data at remote computer from smart meter communicating through different Ethernet switches acting as the intermediate network system device with set up displayed in (Figure 2.6). Going through different switches will give idea about percentage deviation in watt hours recorded with and without intermediate network system devices stored in remote computer. Instant change in parameters like % Total harmonic distortion (THD), Power factor (PF) with different load, real power, active power and reactive power etc. can also be observed with the help of software installed in remote computer. Several different Ethernet switches were used to understand the impact of these switches on the power consumption data of customers. A typical setup is shown in (Figure 2.5).

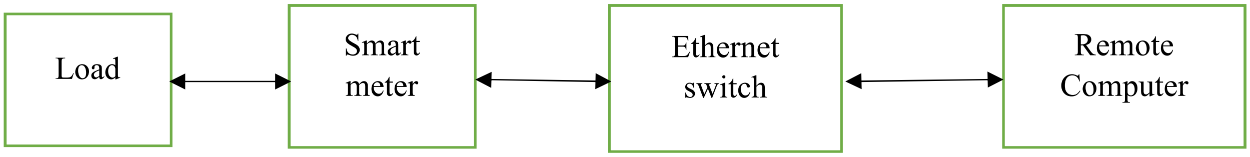


Figure 2.5: Advanced Metering Infrastructure (AMI) configuration with switch

2.2 Experimental Results and Discussions

2.2.1 Experiment with NETGEAR switch

In this experimental setup, we used NETGEAR switch FS608 8-port Fast Ethernet NETGEAR switch and each port supports a bandwidth up to 100 Mbps. For the experiment, the baseline was recorded directly to the computer through Ethernet cable from smart meter (without any switch). Once the baseline was recorded, the experiment continued for same duration of time having NETGEAR switch in the network. Watt hours consumption data were remotely recorded per day basis on the monitoring computer. Watt hour increments compared to baseline were observed (Table 2.1).

(Figure 2.6) shows the cumulative % deviation of watt hour consumption from the baseline while communicating data through an intermediate FS608 8-port Fast Ethernet NETGEAR switch to the remote monitoring computer.

Table 2.1: Reading with and without NETGEAR switch for 270-watt load

Days	Watt hours without NETGEAR switch (Baseline)	Watt hours with NETGEAR switch	Cumulative % Increase compared to Baseline
1	6431	6538	1.67
2	12857	13112	1.98
3	19205	19556	1.83
4	25643	26233	2.03
5	32120	32189	2.16
6	38411	39218	2.10
7	44812	45768	2.13

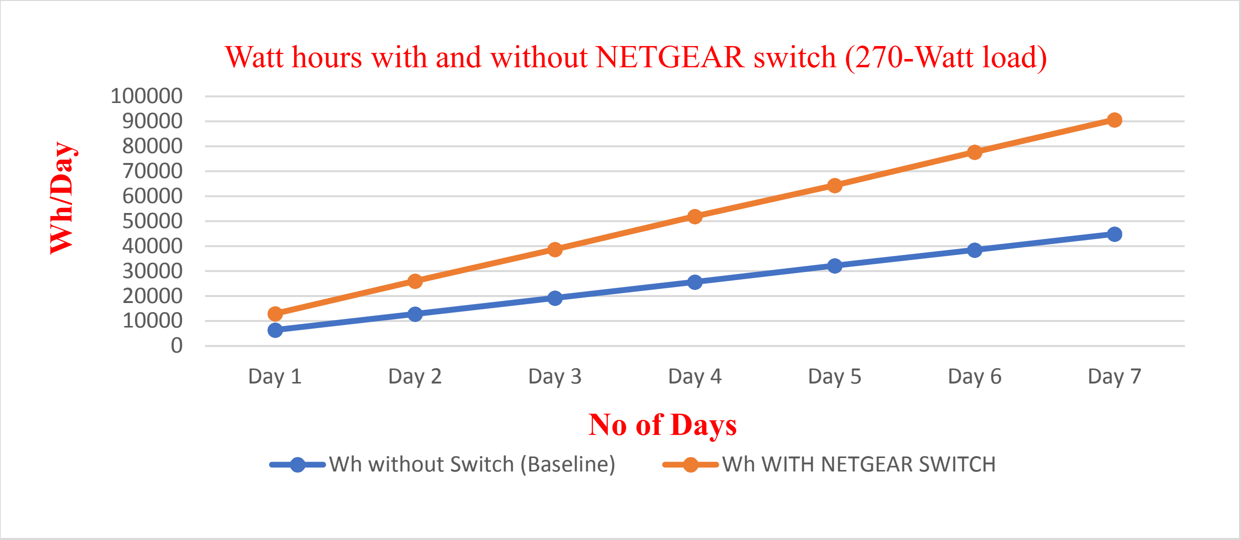


Figure 2.6: Watt hour consumption with and without NETGEAR switch for 270-watt load

2.2.2 Experiment with POE Switch

To further investigate, we used a different Ethernet switch, Cisco Catalyst 3750 48-port POE Ethernet switch. With the stacking feature in this we can create one logical switch with one virtual IP, so we can plug servers (for example) into multiple switches and do channeling for redundancy. Also, when a change to the stack was made, it was applied to every switch.

For this experiment also the baseline was recorded directly to the computer through Ethernet cable from smart meter. Once the baseline was recorded the experiment continued for same duration of time with POE switch was used in AMI configuration. Watt hour increments were observed also while using this POE switch (Table 2.2) but increments were a bit smaller compared to other switches. (Figure 2.7) shows the cumulative % deviation in watt hours consumption from the baseline while communicating data through an intermediate POE switch.

Table 2.2: **Reading with and without POE switch for 270-watt load**

Days	Watt hours without POE switch (Baseline)	Watt hours with POE switch	Cumulative % Increase compared to Baseline
1	6431	6517	1.34
2	12857	12997	1.09
3	19205	19451	1.28
4	25643	26071	1.67
5	32120	32168	1.55
6	38411	38868	1.19
7	44812	45592	1.74

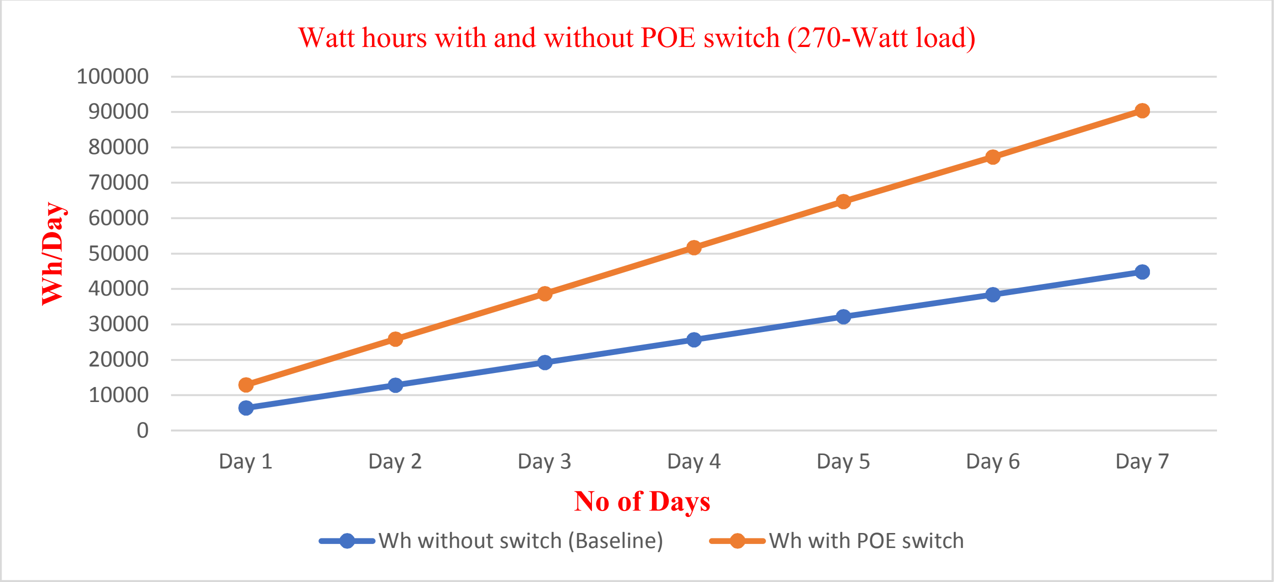


Figure 2.7: Watt Hour Consumption with and without POE switch for 270-watt load

2.2.3 Experiment with a CISCO Switch

To continue with our investigation on the impact of Ethernet based AMI, in this case, we used another switch as the intermediate system in an AMI configuration. It was a 24-port CISCO Ethernet switch SRW2024 v1.2. The Switch was equipped with 24 autosensing, Ethernet ports supporting port speeds of 10 Mbps, 100 Mbps, or 1000 Mbps. It didn't support POE protocol. For this experiment also the baseline was measured for power consumption without the presence of the switch i.e. directly from the Smart meter to the remote monitoring computer over Ethernet. Once the baseline was recorded the experiment continued for the same duration of time having the CISCO switch in the AMI configuration. Like previous switches, this switch is also showing increase in the Watt hour consumption compared to the baseline (Figure 2.8). Cumulative % increment in the watt hours consumption from the base line can be seen in (Table 2.3). In case of this switch, increment was higher than other switches.

Table 2.3: Reading with and without CISCO switch for 270-Watt load

Days	Watt hours without CISCO switch (Baseline)	Watt hours with CISCO switch	Cumulative % Increase compared to Baseline
1	6431	6545	1.77
2	12857	13904	1.84
3	19205	19511	1.59
4	25643	26105	1.80
5	32120	32758	1.98
6	38411	39232	2.14
7	44812	45878	2.38
8	51276	52455	2.29
9	57699	59239	2.67
10	64146	65948	2.81
11	70581	72536	2.77
12	77027	79461	3.16
13	83455	86033	3.09
14	89914	92910	3.33

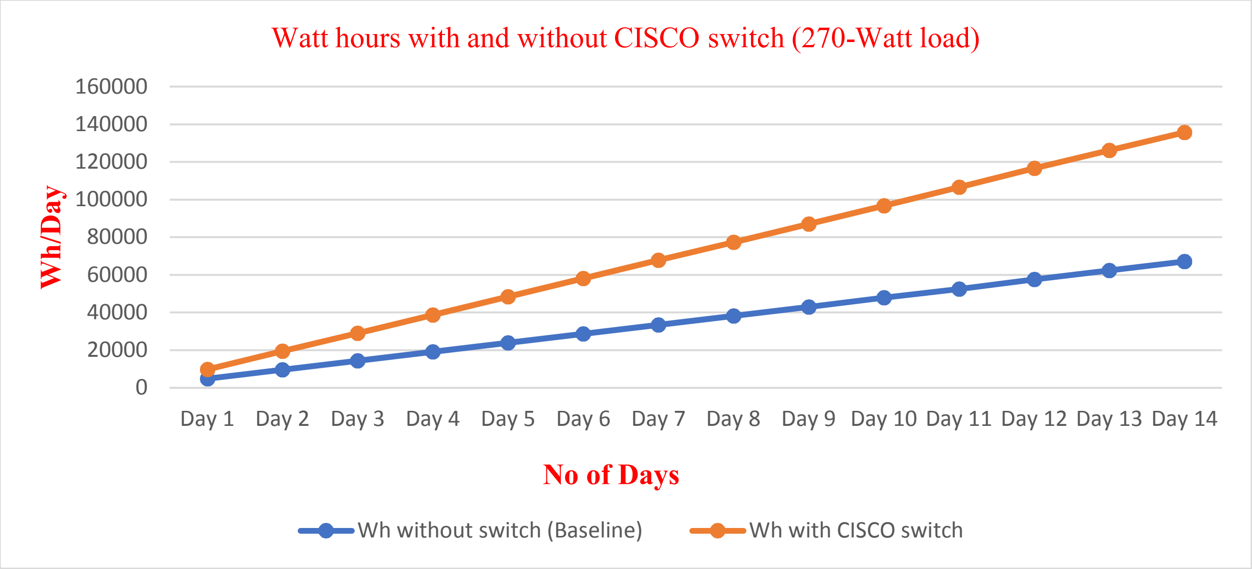


Figure 2.8: Line Graph representation of reading with and without CISCO switch for 270-watt load

2.2.4 Experiment with Tandem Configuration of NETGEAR, POE and CISCO Switch

A typical AMI deployment will include many switches to carry the power consumption data from the customer premise to remote monitoring computer of the utility companies. In this configuration, we used the above three switches connected in tandem to carry the power consumption data in AMI configuration. In this case also the increment in power consumption was recorded and compared to the baseline watt hours (Figure 2.9). For most days, the increment in power consumption was slightly higher than the increments watt hour recorded for individual switches. Furthermore, the increment in tandem configuration was not additive of increments of individual switch increments (Table 2.4). It can be deducted that use of many switches in a large AMI may not linearly increase the watt hour usage for the customer base being served in the area.

Table 2.4: Reading with NETGEAR, POE & CISCO switch in tandem for 270-watt load

Days	Watt hours without CISCO, POE & NETGEAR switch (Baseline)	Watt hours with CISCO, POE & NETGEAR switch	Cumulative % Increase compared to Baseline
1	6431	6863	2.51
2	12857	13181	2.52
3	19205	19657	2.35
4	25643	26274	2.46
5	32120	32993	2.71
6	38411	39371	2.50
7	44812	45842	2.29

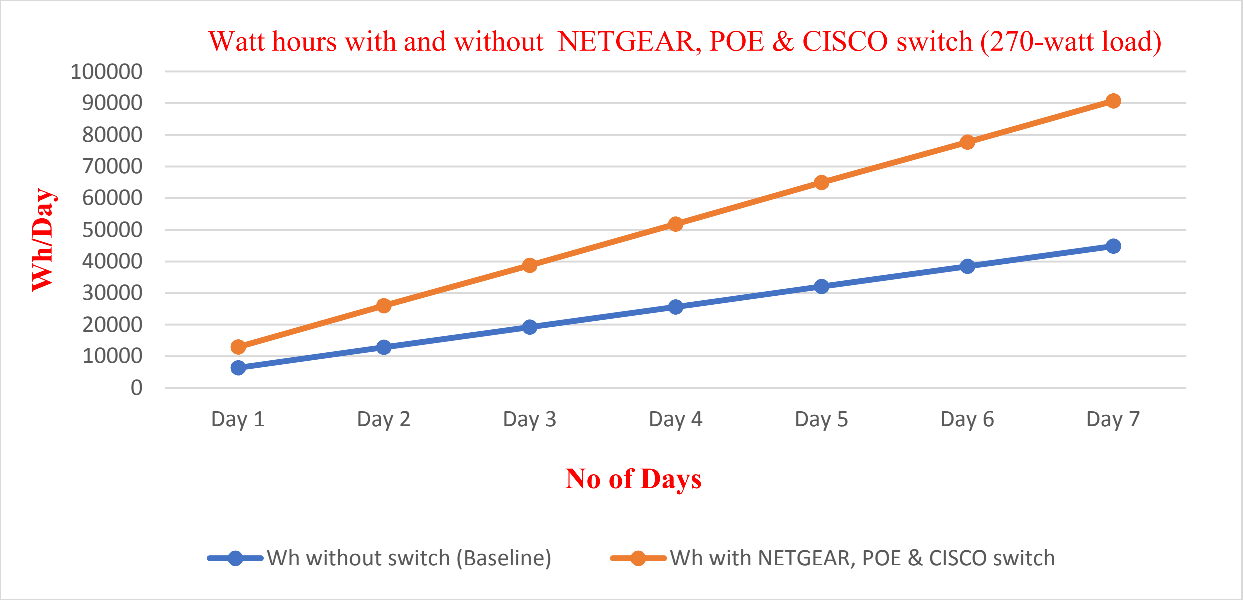


Figure 2.9: Watt hour consumption with and without NETGEAR, POE & CISCO switch in tandem for 270-watt load

2.3.5 Experiment with Ethernet Switch as Load

It was observed in all previous cases that switches in AMI infrastructure were contributing to increased power consumption for the customer base being served by that AMI infrastructure. It seemed very clear that the switches being used in the AMI infrastructure were contributing to the increased power consumption for the customer base.

To prove this point that the switches were contributing to the extra power consumption for the customer base, we conducted further experiment where we used the switch as a load in place of the bulb.

(Figure 2.10) shows the setup configuration for the experiment used under this scenario with the CISCO switch SRW2024 v1.2 being used as a load.

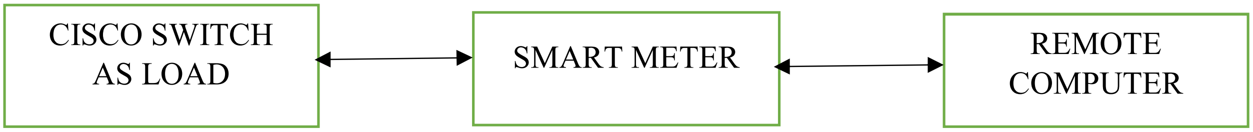


Figure 2.10: Experimental set up to monitor WH consumption of switch as a load

Table 2.5: Average Watt Hours consumption of switch as a load

Days	Watt hours measured when CISCO Ethernet switch was used as the load
1	115.44
2	118.32
3	104.64
4	115.44
5	127.44
6	126.80
7	129.44

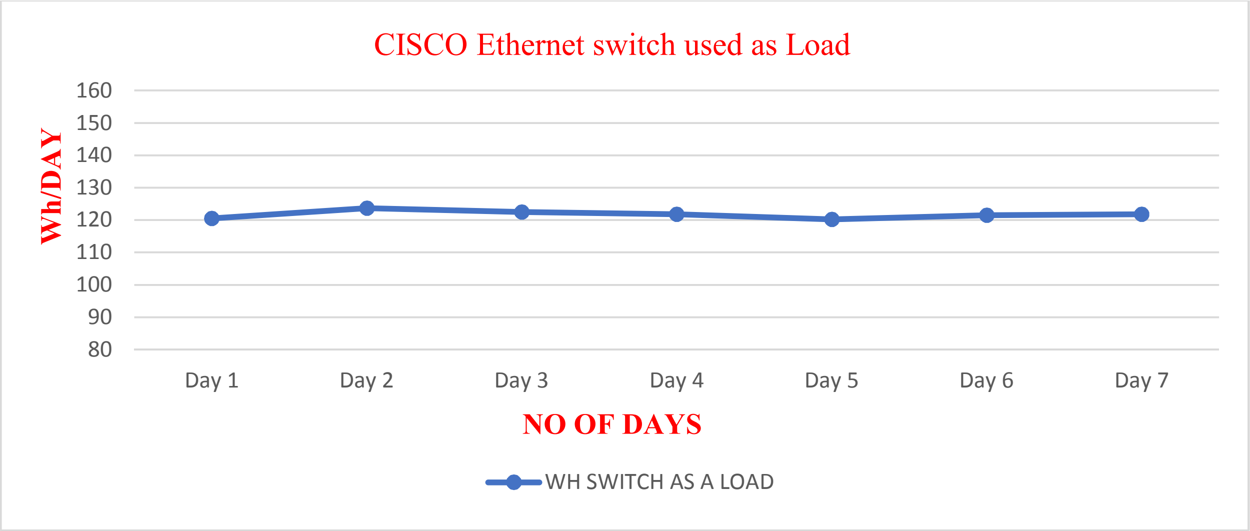


Figure 2.11: Watt hours consumption of CISCO Ethernet switch when used as a load.

It can be concluded that Ethernet switches act as a resistive load while communicating energy consumption data via AMI to the remote monitoring computer from smart meters. They contribute to the increase in watt hour consumption for the customer base they are serving via the AMI used by the smart grid infrastructure.

2.3 OBSERVATION

To understand the relation with power and resistive load, we use the following mathematical relation.

Average Power dissipated in R:

$$\mathbf{P} = \frac{\mathbf{1}}{\boldsymbol{T}}\int_{\mathbf{0}}^{\boldsymbol{T}} \mathbf{p(t)dt} = \frac{\mathbf{1}}{\boldsymbol{R}} \times \frac{\mathbf{1}}{\boldsymbol{T}}\int_{\mathbf{0}}^{\boldsymbol{T}} \boldsymbol{V}^{\mathbf{2}}\,\mathbf{(t)dt} = \frac{<\boldsymbol{V}^{\mathbf{2}}\mathbf{(t)}>}{\boldsymbol{R}}$$

$\frac{<V^2(t)>}{R}$ **is the value of** $\frac{V^2(t)}{R}$ **average over time**

This shows that the average power P is inversely proportional to the resistance R with respect to change in time. So, whenever resistance R increases average power will be on the lower side and vice versa. To show it with mathematical calculation we calculated the resistance for the given power and voltage value measured in our experiments for baseline and for the Cisco switch SRW2024.

Case I When no switch was used (Baseline)

P= Power average over 24 hours (calculated from Table 2.3)

P= 267.60-Watt hour and measured V= 119.43 volts

$$Pavg(24hrs) = \frac{V^2(\mathrm{t})}{R}$$

$$R = \frac{V^2(\mathrm{t})}{P} = \frac{119.43^2}{267.60} = 53.30$$

Case II When Cisco2024 switch was used

P= Power averaged over 24 hours (calculated from Table 2.3)

P= 274.34-Watt hour and measured V= 120.53 volts

$$Pavg(24hrs) = \frac{V^2(\mathrm{t})}{R}$$

$$R = \frac{V^2(\mathrm{t})}{P} = \frac{120.33^2}{274.34} = 52.77$$

These calculations show that the resultant resistive load decreases when the switches are added, which also implies that the switches were added in a shunt fashion to the load. As the intermediate network devices connected in shunt configuration to the load, they contribute to increase in overall power consumption contributed by the AMI infrastructure which gets added to the electric charges to be paid by the customer base being served by the AMI used in a smart grid. The estimation of revenue loss or increase in power consumption charges to a customer base being served by the AMI infrastructure is depicted in section 2.5.

2.4 ESTIMATION OF EXTRA CHARGES TO A CUSTOMER BASE IF SERVED BY THE ETHERNET BASED AMI

In this calculation, we consider one experimental data from CISCO switch with 270-Watt load (Table 2.3). In this section, we calculate cumulative difference in power consumption as follows:

$$\%\ \boldsymbol{Cumulative\ difference\ in\ power\ consumption} =$$

$$\frac{\boldsymbol{power\ consumption(\ with\ switch) - power\ consumption(no\ switch)}}{\boldsymbol{Power\ consumption(\ no\ switch)}} =$$

$$\frac{92910-89914}{89914} * 100 = 3.33\%$$

Many utility companies are deploying smart meters on mass scale via Advanced Metering Infrastructure in their Smart Grid. In this sample calculation, we consider deployment numbers from Pacific Gas and Electric [53]. Here we estimate how much of extra charges that can be levied to customer base if their smart meters are served by Ethernet based AMI, where Cisco switches are being used to transfer power consumption data to remote monitoring computers at the utility company.

How much of additional power consumption charges will be added to the customer base being served by this scenario of Ethernet switch-based AMI (Table 2.3).

- Name of the company: Pacific Gas & Electric
- Company data obtained from Ref [53] in 2015
- No of customer= 5,069,189
- Total power consumption per month= 6,040,152,083 KWH
- Average price [53] = 17.41 cents per KWH
- Increase in Watt hour due to intermediate network devices in AMI based on our experimental result of average increase of 3.33 % (as in Equation 1) = 201,137, 064 KWH
- Extra charges billed to the customer base due to intermediate devices in AMI and hence contributing to the increased power consumption charges = 35 million USD per month.

(PS: here we assumed for simplicity that only one Ethernet based AMI is serving all the customers. There may be different AMIs being used for a typical smart grid infrastructure).

2.5 Chapter Summary

In this chapter, we investigated the impact of intermediate network systems in the design of Advanced Metering network which is an essential component of the overall Smart Meter Infrastructure. We discovered that the deployment of Ethernet based Advanced Metering Infrastructure (AMI) can contribute to the increase in power consumption for overall customer base served by the AMIs. Customers have no way of knowing that the AMI deployment would cause their electric bill to go higher because the power consumption is higher due to the intermediate systems used in AMI. And the additional power consumption charges may be unfairly passed on to the customers to pay for deploying the AMI network comprising of intermediate network systems, which may be wireline or wireless equipment.

CHAPTER III

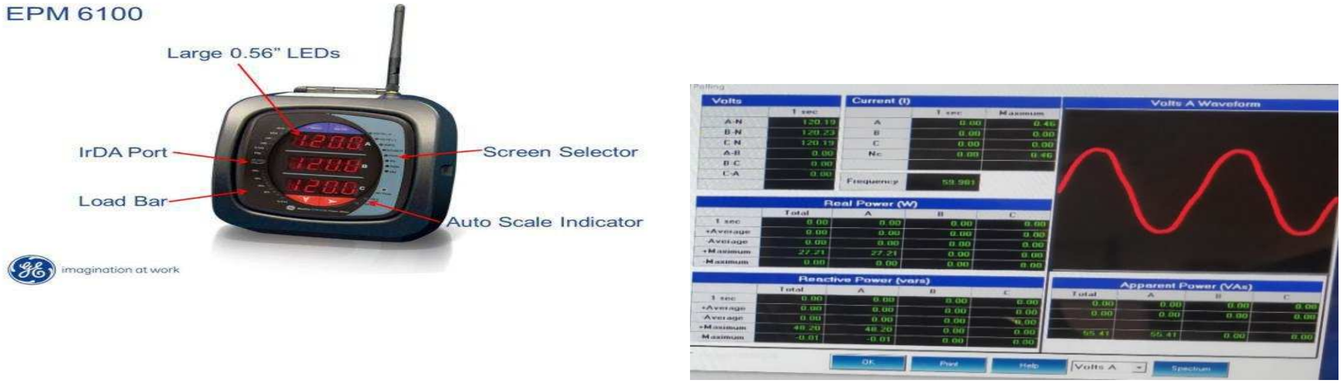
EVALUATION OF SECURITY INTEGRITY OF DATA COLLECTION FOR GE'S EPM 6100 POWER QUALITY SMART ELECTRIC METER UNDER A CYBER ATTACK

Cyber security has been a top concern for electric power companies deploying smart meters and smart grid technology. Despite the well-known advantages of smart grid technology and the smart meters, it is not yet very clear how and to what extent, the Cyber-attacks can hamper the operation of the smart meters, and remote data collections regarding the power usage from the customer sites. To understand these questions, we conducted experiments in a controlled lab environment of our cyber security lab to test a commercial grade smart meter. In this chapter, we present results of our investigation for EPM 6100 a commercial grade power quality smart meter from General Electric and measure the operation integrity of the smart meter under indirect and direct cyber-attack conditions.

3.1 EPM 6100 Power Quality Smart Electric Meter from GE

The EPM 6100 shown in (Figure 3.1) is one of the smart meters manufactured by GE [54], which allows service providers to monitor and manage their energy usage within factories, businesses and campuses. The EPM 6100 is a multifunction meter that features ANSI C12.20 (0.2% class) accuracy and provides several interfaces such as RS485, RJ45 Ethernet and IEEE 802.11 for WIFI communication, making the smart meter easy to deploy in new or preexisting communications systems. Early detection of power problems is facilitated through THD and the alarming capabilities of the EPM 6100. The units use standard 5 or 1-amp CTs.

EPM 6100 smart multifunction meters can be easily programmed and configured as stated in the manuals [54]. The key benefits of this smart multifunction meter are that it provides a variety of voltage, current and energy measurements. It can also allocate energy usage in multi-tenant settings such as apartment complexes, university campus towers, and shopping malls.



Volts	1 sec
A-N	120.19
B-N	120.23
C-N	120.19
A-B	0.00
B-C	0.00
C-A	0.00

Current (I)	1 sec	Maximum
A	0.00	0.46
B	0.00	0.00
C	0.00	0.00
Nc	0.00	0.46

Frequency 59.981

Real Power (W)	Total	A	B	C
1 sec	0.00	0.00	0.00	0.00
+Average	0.00	0.00	0.00	0.00
-Average	0.00	0.00	0.00	0.00
+Maximum	27.21	27.21	0.00	0.00
-Maximum	0.00	0.00	0.00	0.00

Reactive Power (vars)	Total	A	B	C
1 sec	0.00	0.00	0.00	0.00
+Average	0.00	0.00	0.00	0.00
-Average	0.00	0.00	0.00	0.00
+Maximum	48.20	48.20	0.00	0.00
-Maximum	-0.01	-0.01	0.00	0.00

Apparent Power (VAs) Total	A	B	C
0.00	0.00	0.00	0.00
0.00	0.00	0.00	0.00
55.41	55.41	0.00	0.00

Figure 3.1: Smart Multifunction Meter (EPM 6100) with Ener Vista Software for remote power recording from GE [54]

EnerVista Software from GE [54] shown in (Figure 3.1) provides service providers a platform to remotely access all setup and support tools needed for configuration and maintenance of GE smart meters. This software can remotely configure devices in real-time over network connections, and it can remotely read metered power usage data, and monitor status of the smart meters.

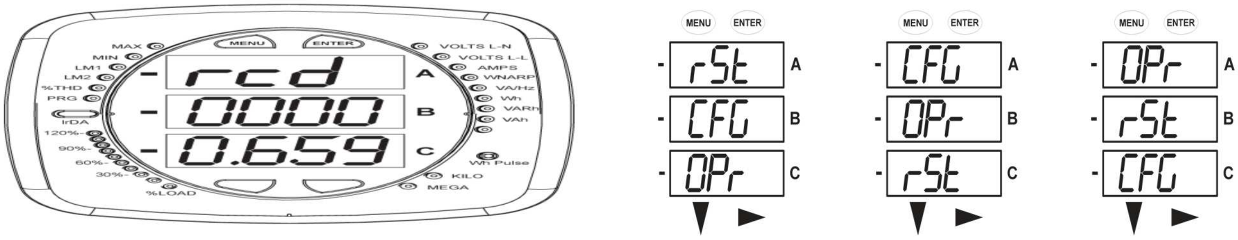


Figure 3.2: Manual Reading Parameters Setting from smart meter [54].

It can be observed from the (figure 3.2) that from the front panel of the meter we can read out several parameters when meter is in use like voltage between phases, phase to neutral, current, Watt-hour, active, reactive and apparent power, baud rate, percentage total harmonic distortion etc. One can also configure the parameters from the front panel buttons like menu and left-right arrow. One can configure the smart meter for the parameters from the meter front panel as well as through software installed in computer at remote location. In this research focus was to configure and read out from the meter from its front panel and to configure it manually for WH recording to be done. Front panel has four buttons for the navigation including up and down arrow for scrolling up and down for the options. Then it has menu button for going to the configuration options. From the front panel of the meter one can configure Potential Transformer (PT) ratio, Current Transformer (CT) ratio, reset the meter, adjust baud rate, configure address, see the value of voltage, current, Watt Hour (WH), and power, adjust the electrical connection etc.

3.2 Experimental Setup

In this chapter, we evaluated the security performance of Smart Meter namely General Electric (GE) company’s Multilin EPM 6100 Power Quality Meter with Ethernet port installed and 60Hz of operating frequency. EPM 6100 power quality meter is connected to the remote computer and attacker network as shown in the Figure 3.4. In this experiment, we used “3 EL WYE” in Meter Programming Setup as provided by General Electric Company [54]. For the experiments, a 400- Watt load (in the form of two light bulbs) is connected to the smart meter at the LOAD end shown in (Figure 3.3).

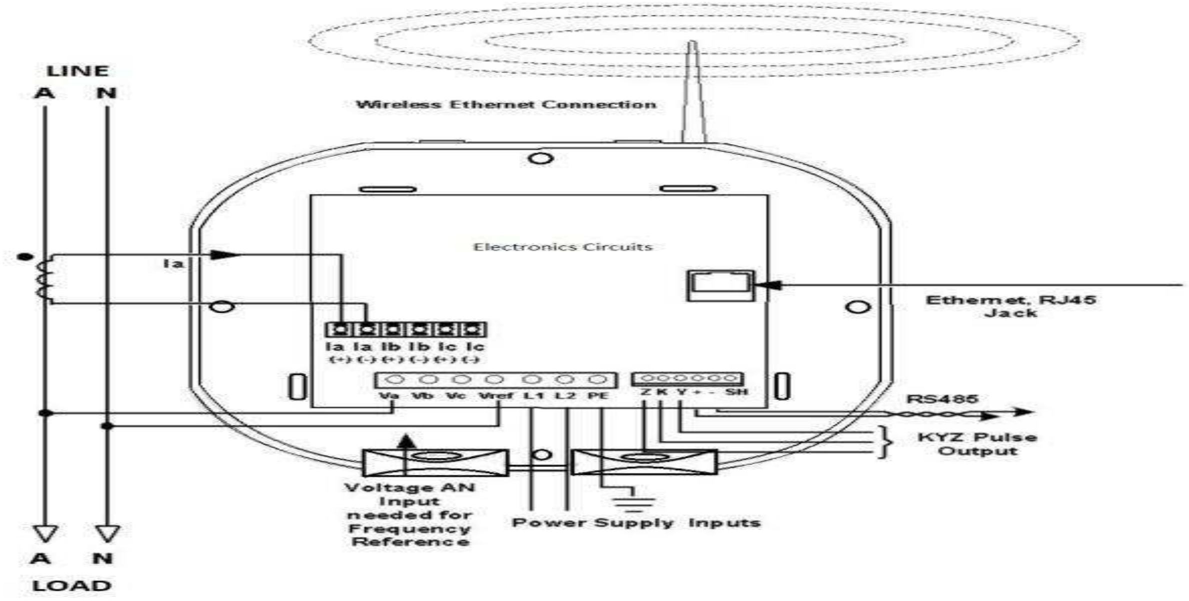


Figure 3.3**:** “3 EL WYE” in Meter Programming Setup [58].

By using monitoring computer, power consumption data is obtained remotely from the smart meter. Simulated Ping based security attack traffic was sent to the smart meter. The schematics of the experimental set up is shown in (Figure 3.4). We used simulated traffic in the protected environment of the Network Research Laboratory (NRL) at UTRGV.

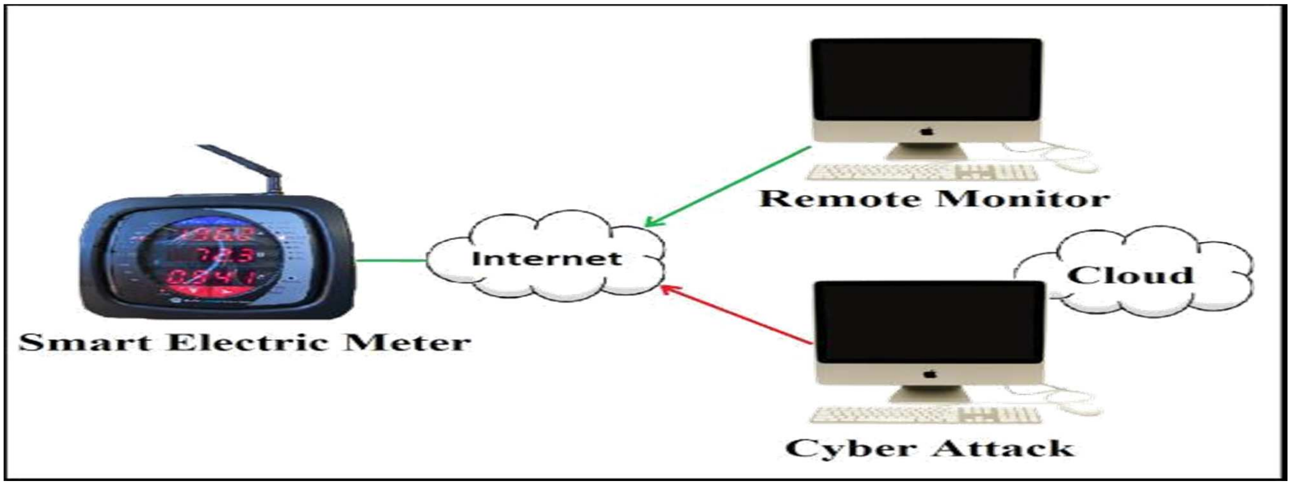


Figure 3.4: Experimental setup for Cyber-Attack [41]

For experiments, we used General Electric's EPM 6100 Power Quality Meter as the Smart meter under test. It was remotely accessed for power usage data reading over Ethernet utilizing GE communicator software EnerVista, which was installed on a remote monitoring computer (Figure 3.5).

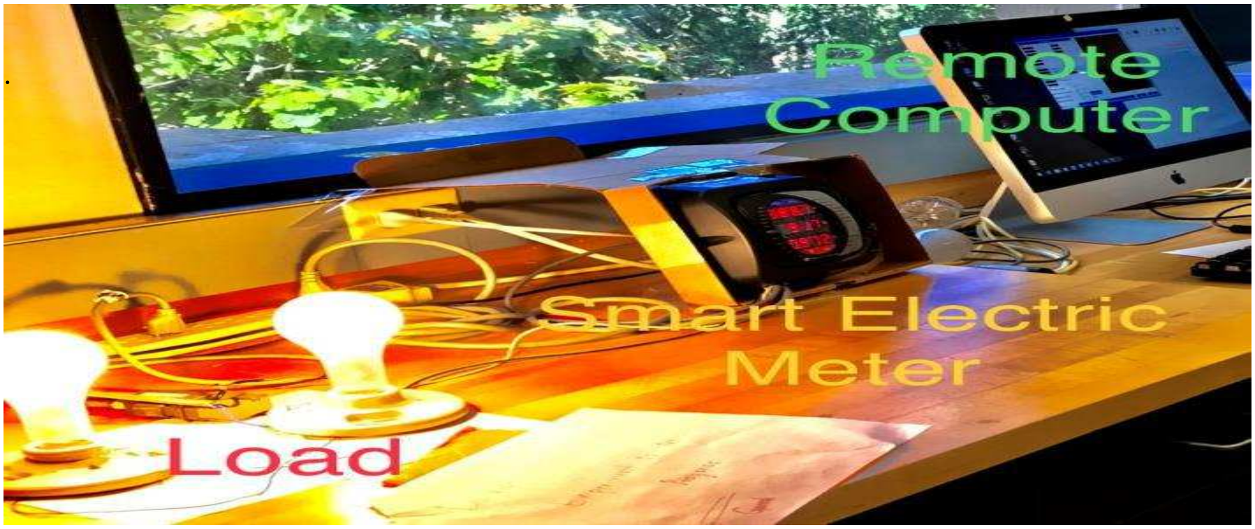


Figure 3.5: Lab set up used in Experiments showing Load, Smart meter and monitoring remote computer [41]

We conducted five independent experiments to observe the impact of a Cyber Security Attack on the Watt Hour reporting over several days and its deviation from the baseline Watt Hour reporting when there was no attack.

3.3 Performance Parameters for Evaluation

3.3.1 Experiment I Under Indirect Attack for 4-days

For Experiment I, we used two incandescent light bulbs which together measured a 400-Watt of load for this smart meter. We used this load as the baseline load (in the absence of any attack traffic going to the smart electric meter). We used this baseline load for the smart meter operation for 4 days (96 hours).

We remotely collected the power usage data to confirm the stability of the data collected (for the baseline load in the absence of any Cyber-attack) which is (shown in the 2nd column of Table 3.1). And then we repeated the same experiment under the conditions of indirect Cyber-attack. We remotely collected power consumption data (shown in 3rd column of Table 3.1) again for the next 4 days (96 hours) from the smart meter under conditions of the Ping based indirect Cyber-attack. Ping attack traffic experienced by the smart meter was measured to be a continuous 50 Mbps, which is considered rather a low intensity Cyber-attack these days.

3.3.2 Experiment II Under Indirect Attack for 7-days

For Experiment II, we used two incandescent light bulbs which together measured a 400-Watt of load for this smart meter. We used this load as the baseline load (in the absence of any attack traffic going to the smart electric meter). We used this baseline load for the smart meter operation for 7 days (168 hours). We remotely collected the power usage data to confirm the stability of the data collected (for the baseline load in the absence of any Cyber-attack) which is shown in the 2nd column of (Table 3. 2). And then we repeated the same experiment under the conditions of indirect Cyber-attack. We remotely collected power consumption data (shown in 3rd column of Table 3.2) again for the next 7 days (168 hours) from the smart meter under conditions of the Ping based indirect Cyber-attack. Ping attack traffic experienced by the smart meter was measured to be a continuous 50 Mbps, which is considered rather a low intensity Cyber-attack these days.

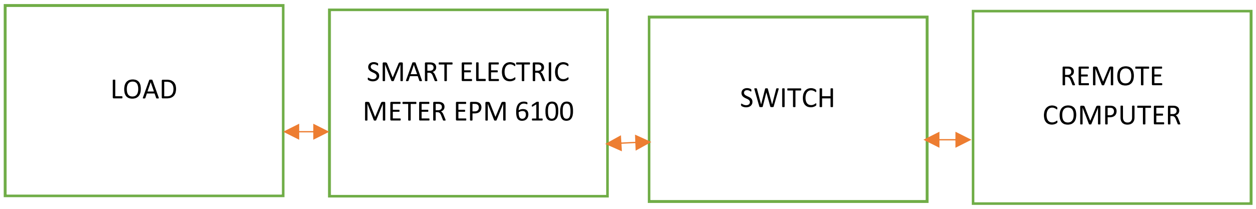


Figure 3.6: Experimental setup for Experiments

3.3.3 Experiment III Under Indirect Attack for 15-days

For Experiment-III, we used one incandescent light bulb which measured a 200-Watt of load for this smart meter. We used this load as the baseline load (in the absence of any attack traffic going to the smart electric meter). We used this baseline load for the smart meter operation for 15 days (360 hours). We remotely collected the power usage data to confirm the stability of the data collected (for the baseline load in the absence of any Cyber-attack) which is shown in the 2nd column of Table 3.3. And then we repeated the same experiment under the conditions of indirect Cyber-attack. We remotely collected power consumption data (shown in 3rd column of Table 3.3) again for the next 15 days (360 hours) from the smart meter under conditions of the Ping based indirect Cyber-attack. Ping attack traffic experienced by the smart meter was measured to be a continuous 50 Mbps, which is considered as low intensity of Cyber-attack these days.

3.3.4 Experiment IV Under Indirect Attack for 30-days

For Experiment-IV, we used one incandescent light bulb which measured a 200-Watt of load for this smart meter. We used this load as the baseline load (in the absence of any attack traffic going to the smart electric meter). We used this baseline load for the smart meter operation for 30 days (720 hours). We remotely collected the power usage data to confirm the stability of the data collected (for the baseline load in the absence of any Cyber-attack) which is shown in the 2nd column of (Table 3.4). And then we repeated the same experiment under the conditions of indirect Cyber-attack. We remotely collected power consumption data (shown in 3rd column of Table 3.4) again for the next 30 days (720 hours) from the smart meter under conditions of the Ping based indirect Cyber-attack.

Ping attack traffic experienced by the smart meter was measured to be a continuous 50 Mbps, which is considered rather a low intensity Cyber-attack these days.

3.3.5 Experiment V Under Direct Attack

In further investigation smart meter was experimented under direct cyber-attack. Smart meter was experimented for one entire day under no attack, one entire day under direct cyber-attack and one final day after attack being removed. The same experimental set up was used as shown in (Figure 3.6). This experiment was done to check the connectivity issue of smart meter under cyber-attack while communicating data from smart meter to remote monitoring computer at utility.

3.4 Experimental Results and discussion

3.4.1 Results from Experiment I

We observed (Figure.3.7) that for the first 24 hours of the Cyber-attack there was no significant impact on the power readings however after 24 hours, the smart meter reported declining power consumption data. Table 1 shows average power consumption for 96 hours (4 days), shown as a running average Power consumption after 1st day, 2nd day, 3rd day and 4th day in the third column of the Table-3.1.

Table 3.1: Average power consumption with and without the Cyber-attack on the smart meter measured for 4-days

Time (in Days)	Baseline-Average power consumption (in watt hours)	Average power consumption under cyber-attack (in watt hours)	% loss of power consumption reported
1	202.62	202.3	0.16
2	201.62	201.2	0.21
3	201.10	200.6	0.25
4	200.84	200.2	0.32

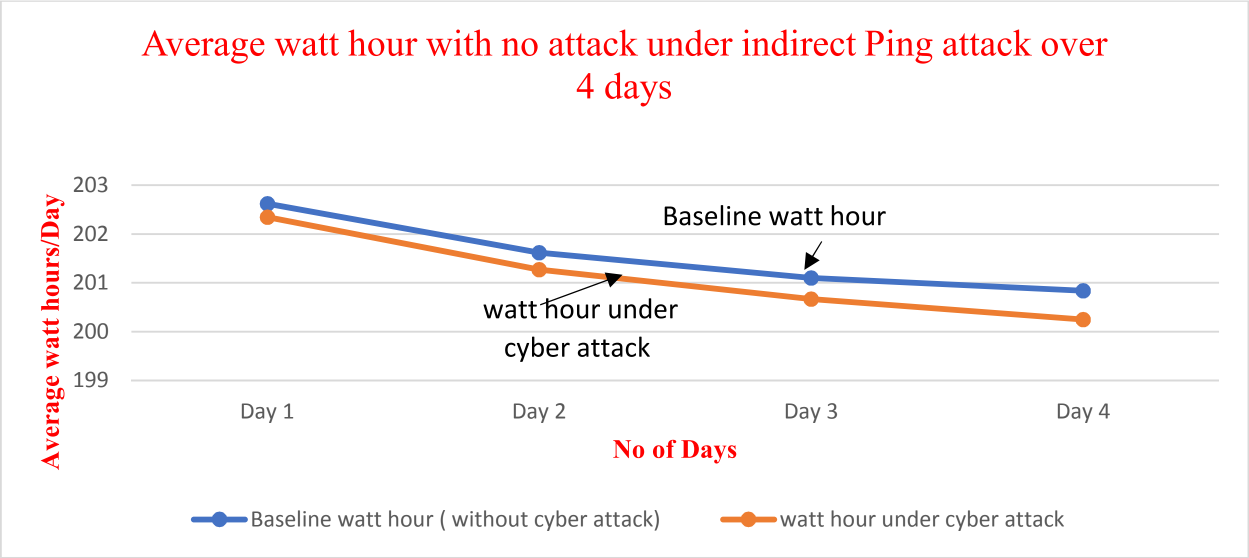


Figure 3.7**:** Average Power Consumption Measured in Average Watt Hour for Experiment I without Cyber-Attack (baseline shown in blue) and with Indirect Cyber-Attack (shown in orange)

Loss of Power Consumption reported under Cyber attack

% Loss of Power reported (after 4 days) =

$$\frac{Power\ Consumption\ (Baseline) - Power\ Consumption\ (Cyber\ Attack)}{Power\ Consumption\ (Baseline)} \quad * \ 100$$

=[(200.84 – 200.2) / 200.84] *100= 0.32 %

In Experiment I, by the end of Day 4, the smart meter reported a cumulative power loss of 0.32% (compared to the baseline values) because of security attack on the smart meter. Power consumption reporting for baseline (blue) and power consumption reporting under Cyber-attack conditions (red) is shown for four consecutive days in (Figure 3.7). There seems to be a trend in the continued decline in the average power consumption as reported by the smart meter to the remote computer under the influence of the Cyber-attack. Power loss of 0.32% may seem little, but it makes a big difference when it comes to a large commercial deployment of smart meters by a large Electric company and an example is shown below.

Financial loss estimation due to the Cyber-attack for a large Electric Company's deployment under Experiment I setup

Here we estimate how this type of Cyber-attack on Smart meters will affect revenue of a large electric company assuming they use this type of smart meters in their deployments. Some of the power consumption data has been obtained for the Pacific Gas & Electric in 2015 from [53] and are given below:

Name of Company: Pacific Gas & Electric.

Number of Customers (Residential and Commercial)=5,069,189

Total power consumption per month = 6,040,152,083 kWh

Average price from ref [53] = 17.41 cents per kWh

Loss of power due to security attack on Smart Meter/Smart Grid = 19,328,487 kWh per month based on our experimental result of 0.32 % reported loss.

Total Loss of revenue due to Cyber-attack on Smart Meter/Smart Grid network = $3.4 Million per month.

3.4.2 Results from Experiment II

We observed (Figure 3.8) that for the first 24 hours of the Cyber-attack there was no significant impact on the power readings however after 24 hours, the smart meter reported declining power consumption data. (Table 3.2) shows average power consumption for 168 hours (7 days), shown as a running average Power consumption after 1st day to 7th day in the third column of the (Table-3.2).

Table 3.2: Average power consumption with and without the Cyber-attack on the smart meter measured for 7-days

Time (in days)	Baseline-Average power consumption reported without attack (in watt hours)	Average power consumption under cyber-attack (in watt hours)	% loss of power consumption reported
1	202.62	202.3	0.16
2	201.62	201.2	0.21
3	201.10	200.6	0.25
4	200.84	200.2	0.32
5	200.54	199.7	0.41
6	200.73	199.4	0.66
7	200.95	199.1	0.92

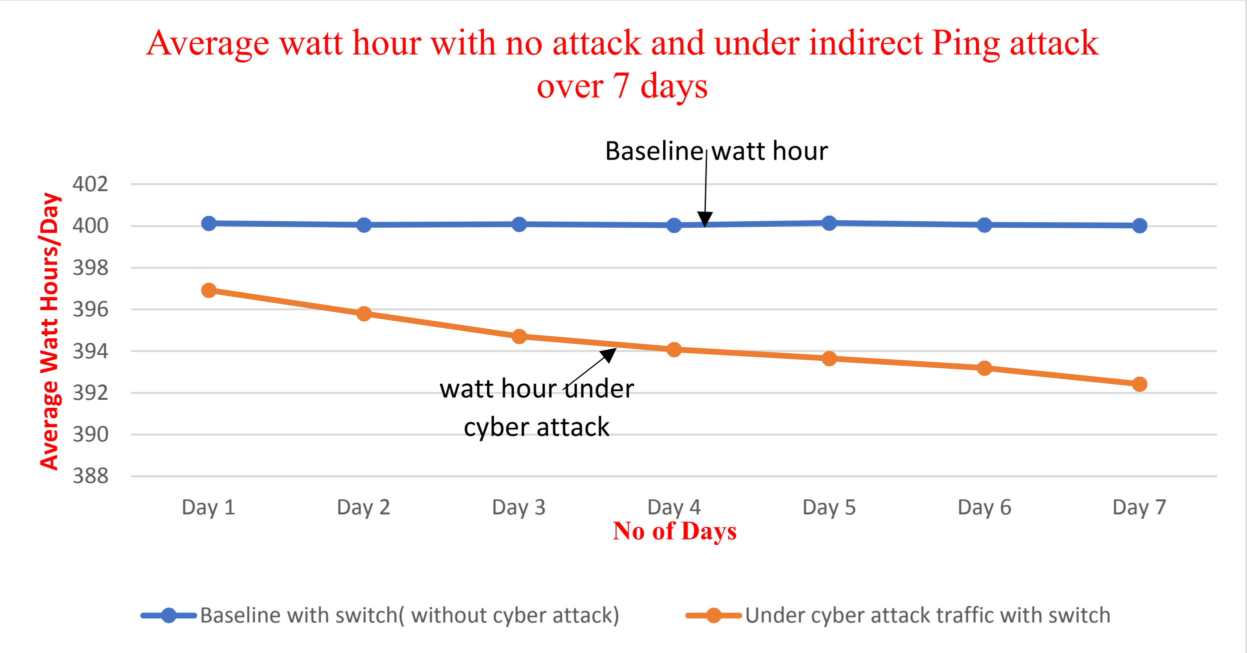


Figure 3.8: Average Power Consumption measured in Average Watt hour for Experiment II without cyber-attack (baseline shown in blue) and with indirect cyber-attack (shown in orange)

Loss of Power Consumption reported under Cyber attack

% Loss of Power reported (after 7 days) =

$$\frac{Power\,Consumption\,(Baseline) - Power\,Consumption\,(Cyber\,Attack)}{Power\,Consumption\,(Baseline)} * 100$$

= [(200.95-199.1) / 200.95] *100= 0.92%

In Experiment II, by the end of Day 7, the smart meter reported a cumulative power loss of 0.92% (compared to the baseline values) because of security attack on the smart meter. Power consumption reporting for baseline (blue) and power consumption reporting under Cyber-attack conditions (orange) is shown for 7 consecutive days in (Figure 3.8). There seems to be a trend in the continued decline in the average power consumption as reported by the smart meter to the remote computer under the influence of the Cyber-attack same as experiment I. Power loss of 0.92 % may seem little, but it makes a big difference when it comes to a large commercial deployment of smart meters by a large Electric company and an example is shown below.

Financial loss estimation due to the Cyber-attack for a large Electric Company's deployment under Experiment II setup

Here we estimate how this type of Cyber-attack on Smart meters will affect revenue of a large electric company assuming they use this type of smart meters in their deployments. Some of the power consumption data has been obtained for the Pacific Gas & Electric in 2015 from [53] and are given below:

- Name of the company: Pacific Gas & Electric
- Company data obtained from Ref [53] in 2015
- No of customer (Residential and Commercial) = 5,069,189
- Total power consumption per month= 6,040,152,083 KWH
- Average price [53] = 17.41 cents per kWh
- Loss of power due to security attack on smart meter/smart grid per month based on our experimental result of 0.92 % loss = 55,569,399 kWh
- Loss of revenue to the utility company due to cyber-attack on smart meter /smart grid = 9.7 million USD per month.

3.4.3 Result for Experiment III

We observed (Figure 3.9) that for the first 24 hours of the Cyber-attack there was no significant impact on the power readings however after 24 hours, the smart meter reported declining power consumption data. (Table 3.3) shows average power consumption for 360 hours (15 days), shown as a running average Power consumption after 1st day to 15th day in the third column of the (Table-3.3).

Table 3.3: Average power consumption with and without the Cyber-attack on the smart meter measured for 15-days

Time (in days)	Baseline-Average power consumption reported without attack (in watt hours)	Average power consumption under cyber-attack (in watt hours)	% loss of power consumption reported
1	202.62	202.3	0.16
2	201.62	201.2	0.21
3	201.10	200.6	0.25
4	200.84	200.2	0.32
5	200.54	199.7	0.41
6	200.73	199.4	0.66
7	200.95	199.1	0.92
8	200.87	198.8	1.03
9	200.94	198.5	1.21
10	201.12	198.3	1.4
11	201.35	198.1	1.61
12	201.26	197.8	1.72
13	201.33	197.6	1.85
14	201.34	197.3	2.00
15	201.70	197.1	2.28

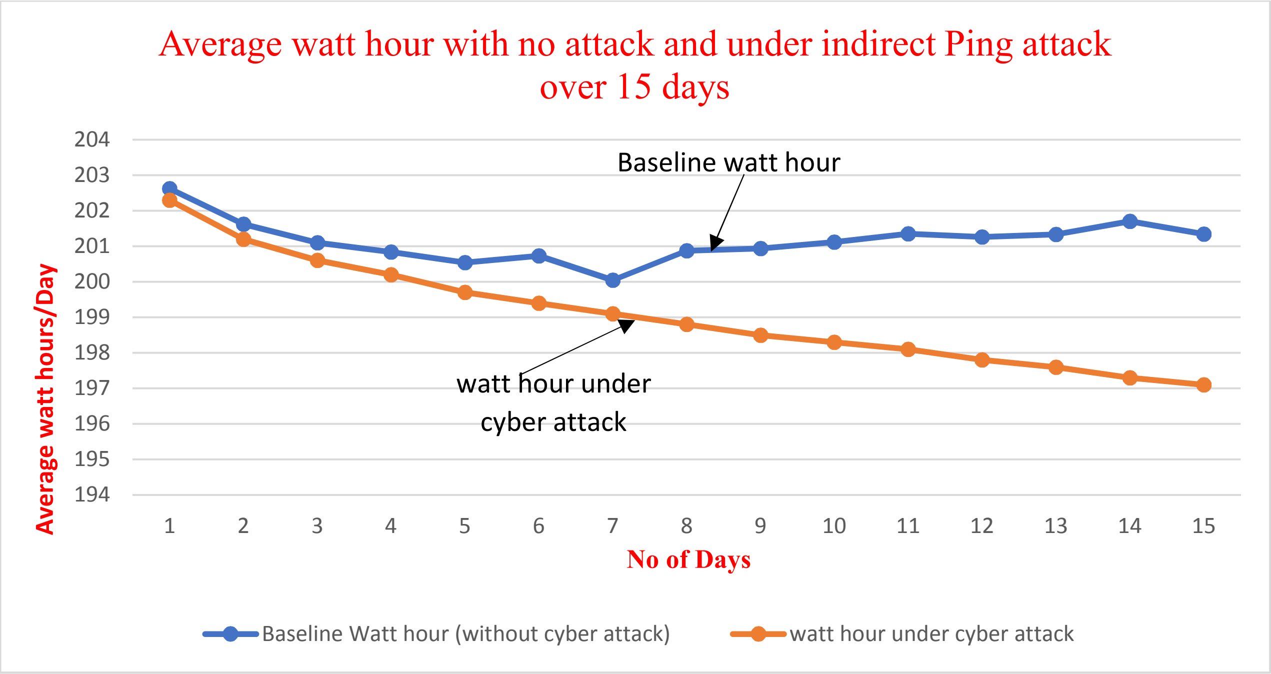


Figure 3.9: Average Power Consumption measured in Average Watt hour for Experiment III without cyber-attack (baseline shown in blue) and with indirect cyber-attack (shown in orange)

Loss of Power reported under Cyber attack

% Loss of Power reported (after 15 days) =

$$\frac{Power\ Consumption\,(Baseline) - Power\ Consumption\,(Cyber\ Attack)}{Power\ Consumption\,(Baseline)} * 100$$

= [(201.7 – 197.1) / 201.7] *100= 2.28 %

In Experiment-III, by the end of Day 15, the smart meter recorded a cumulative power loss of 2.28 % (compared to the baseline watt hours) because of security attack on the smart meter. Power usage recorded for baseline and power usage recorded under Cyber-attack conditions is shown for 15 consecutive days in (Figure 3.9). There seems a trend in the continued decline in the average power consumption as reported by the smart meter to the remote computer under the influence of the Cyber-attack.

Power loss of 2.28 % may looks a little, but it can make a big difference when it comes to a large commercial deployment of smart meters by a large Electric company and an example is shown below.

Financial loss estimation due to the Cyber-attack for a large Electric Company's deployment under Experiment III setup

Here we estimate how this type of Cyber-attack on Smart meters will affect revenue of a large electric company assuming they use this type of smart meters in their deployments. Some of the power consumption data has been obtained for the Pacific Gas & Electric in 2015 from [53] and are given below:

- Name of Company: Pacific Gas & Electric.
- Number of Customers (Residential and Commercial) = 5,069,189
- Total power consumption per month = 6,040,152,083 KWh. Average price from ref [53] = 17.41 cents per KWh
- Loss of power due to security attack on Smart Meter/Smart Grid = 169,124,258 KWh per month based on our experimental result of 2.28 % reported loss.
- Total Loss of revenue due to Cyber-attack on Smart Meter/Smart Grid network = $29.4 Million per month.

3.4.4 Results from Experiment IV

We observed (figure.3.10) that for the first 24 hours of the Cyber-attack there was no significant impact on the power readings however after 24 hours, the smart meter reported declining power consumption data. (Table 3.4) shows average power consumption for 720 hours (30 days), shown as a running average Power consumption after 1st day to 30th day in the third column of the (Table-3.4).

Table 3.4: Average power consumption with and without the Cyber-attack on the smart meter measured for 30-days

Time (in days)	Average WH with No attack	Average WH under cyber attack	% deviation or WH decline under attack from baseline WH
1	202.62	202.3	0.16
2	201.62	201.2	0.21
3	201.10	200.6	0.25
4	200.84	200.2	0.32
5	200.54	199.7	0.41
6	200.73	199.4	0.66
7	200.95	199.1	0.92
8	200.87	198.8	1.03
9	200.94	198.5	1.21
10	201.12	198.3	1.4
11	201.35	198.1	1.61
12	201.26	197.8	1.72
13	201.33	197.6	1.85
14	201.34	197.3	2.00
15	201.70	197.1	2.28
16	201.76	196.8	2.45
17	201.57	196.5	2,51
18	201.51	196.1	2.67
19	201.44	195.9	2.75
20	201.53	195.6	2.94
21	201.43	195.3	3.04
22	201.63	195.1	3.23
23	201.47	194.8	3.45
24	201.77	194.5	3,60
25	201.54	194.3	3.58
26	201.67	194.3	3.71
27	201.50	194.2	3.70
28	201.70	194.2	3,72
29	201.68	194.2	3.71
30	201.70	194.2	3.72
31	200.54	199.7	0.41
32	201.20	200.7	0.24

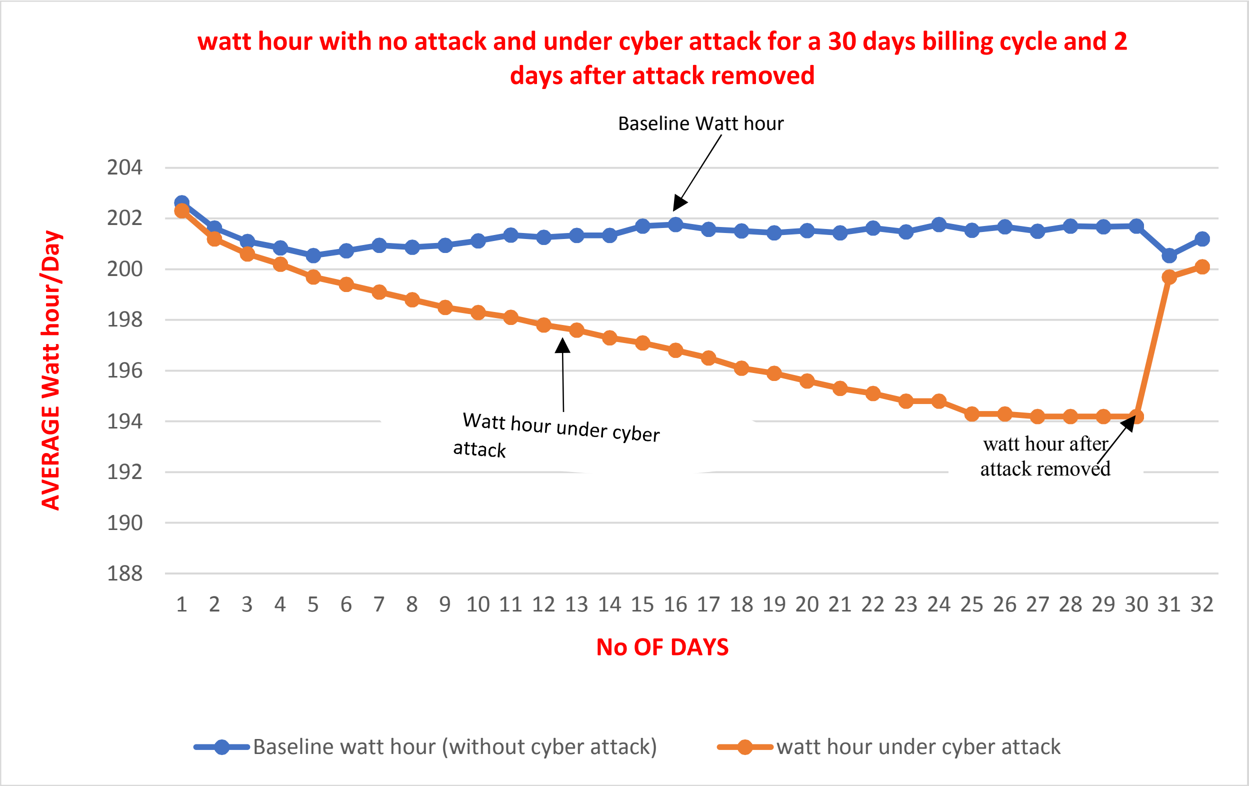


Figure 3.10: Average Power Consumption measured in Average Watt hour for Experiment IV without cyber-attack (baseline shown in blue) and with indirect cyber-attack (shown in orange)

Loss of Power reported under Cyber attack

% Loss of Power reported (after 30 days) =

$$\frac{Power\ Consumption\,(Baseline) - Power\ Consumption\,(Cyber\ Attack)}{Power\ Consumption\ (Baseline)} * 100$$

= [(201.7 – 194.2) / 201.7] *100= 3.72 %

In Experiment-IV, by the end of Day 30, the smart meter recorded a cumulative power loss of 3.72 % (compared to the baseline watt hours) because of security attack on the smart meter. Power usage recorded for baseline and power usage recorded under Cyber-attack conditions is shown for 30 consecutive days and 2 days after attack was removed in (figure 3.10).

There seems no further decline in the average power consumption as reported by the smart meter to the remote computer under the influence of the Cyber-attack at the end of the 30 days typical customer billing cycle. Power loss of 3.72 % may looks a little, but it can make a big difference when it comes to a large commercial deployment of smart meters by a large Electric company and an example is shown below.

Financial loss estimation due to the Cyber-attack for a large Electric Company's deployment under Experiment IV setup

Here we estimate how this type of Cyber-attack on Smart meters will affect revenue of a large electric company assuming they use this type of smart meters in their deployments. Some of the power consumption data has been obtained for the Pacific Gas & Electric in 2015 from [53] and are given below:

- Name of Company: Pacific Gas & Electric.
- Number of Customers (Residential and Commercial) = 5,069,189
- Total power consumption per month = 6,040,152,083 KWh. Average price from ref [53] = 17.41 cents per KWh
- Loss of power due to security attack on Smart Meter/Smart Grid = 224,693,657 KWh per month based on our experimental result of 3.72 % reported loss.
- Total Loss of revenue due to Cyber-attack on Smart Meter/Smart Grid network = $39.11 Million per month.

Based on these different experiments and the measured results it is evident that the Cyber-attacks can adversely affect the operation of smart meters, which in turn can result in a significant financial loss for a large electric company deployment of smart meters.

3.4.5 Results from Experiment V

On day 1 without attack there was no impact on data recording for this smart meter. On day 2 it shows that there is problem with communication as only old repeated data was communicated to the remote monitoring computer for the power usage under direct attack which was recorded just before the attack has started. GE meter still seems connected to the network because GE smart meter uses intel core duo 1.8 GHZ processor or even faster and under attack it has not lost all its processing power and connectivity options needed to implement most of functions such as consumption analysis, dynamic pricing, and other demand response features After the attacked being removed on day three the data started being recoded as usual which can be observed in (Figure 3.11). As the intensity of the attack was increased beyond 50 Mbps there was no communication at all by the meter. This means this the minimum attack bandwidth required to create problem for meter while usage data communication.

Table 3.5: Watt hour with and without direct attack

Time (in Hours)	WH with no direct attack day 1
1	21.33
2	42.89
3	64.33
4	85.56
5	106.95
6	128.52
7	150.14
8	171.41
9	192.74
10	214.21
11	235.63
12	256.99
13	278.52

14	299.97
15	321.29
16	342.84
17	364.43
18	385.85
19	407.18
20	428.54
21	449.85
22	471.44
23	492.81
24	514.16
Time (in Hours)	**WH with direct attack day 2**
25	514.16
26	514.16
27	514.16
28	514.16
29	514.16
30	514.16
31	514.16
32	514.16
33	514.16
34	514.16
35	514.16
36	514.16
37	514.16
38	514.16
39	514.16
40	514.16
41	514.16
42	514.16
43	514.16
44	514.16
45	514.16
46	514.16
48	514.16
Time (in Hours)	**WH after attack removed**
49	1009.3
50	1029.87
51	1050.49
52	1070.93
53	1091.46
54	1112.23
55	1133.04
56	1153.68
57	1174.25

58	1194.91
59	1215.8
60	1236.67
61	1257.58
62	1278.63
63	1299.7
64	1320.79
64	1341.83
65	1362.95
66	1384.14
67	1405.31
68	1426.46
69	1447.45
70	1468.38
71	1489.23
72	1509.90

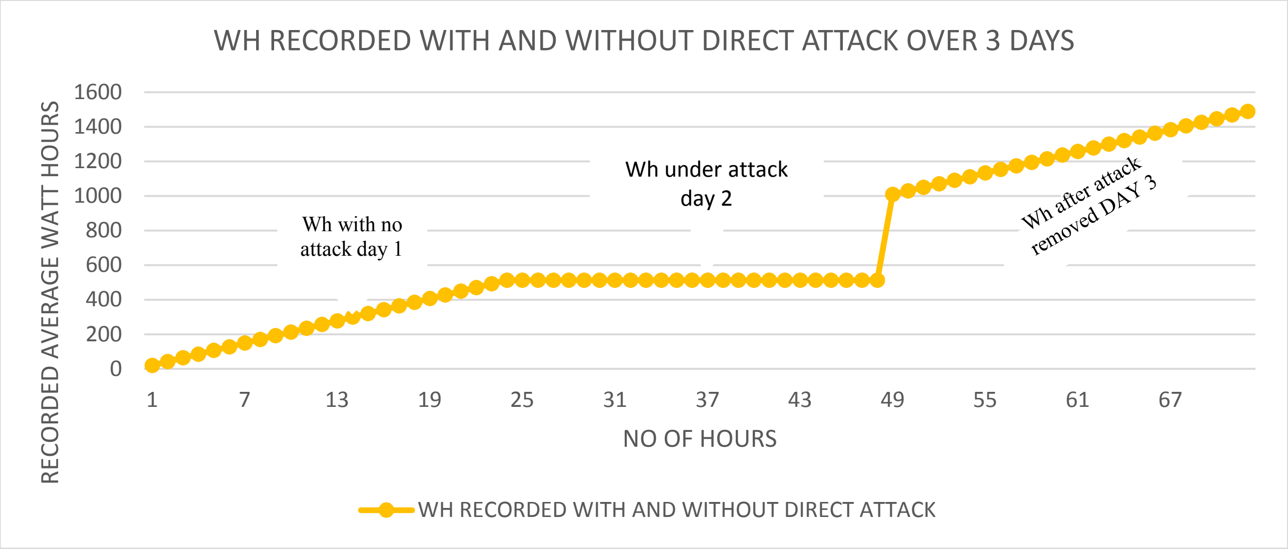


Figure 3.11: Data Connectivity to remote monitoring computer from smart meter under direct attack

3.5 Chapter Summary

In this chapter EPM 6100 smart electric meter has been exposed and evaluated under a real indirect and direct Cyber security attack to understand its effect on its operation and data communication to remote location. Smart meters are very handy for customers as well as utilities in their smart grid infrastructure implementation and to provide uninterrupted power monitoring and easy trouble shooting related to electric Smart meters in a smart grid. But the actual problem is security and the effect of security attacks was not known until this experiment was done. In this experiment, we found that even a very common indirect and direct Cyber security attack such as Ping based ICMP flood attack can have big impact on operation of a smart electric meter in smart grid infrastructure. While experimenting under indirect cyber-attack for customer billing cycle i.e. 30 days, starting day 1 there was not much significant impact but there was significant impact at the end of billing cycle. While experimenting under direct attack there was immediate impact as there was complete loss of data communication. These cyber security attacks can result in significant financial loss in millions of dollars for the power company's deployment in a large-scale smart grid infrastructure.

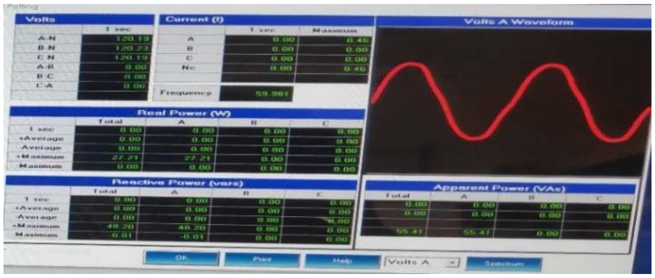
CHAPTER IV

EVALUATION OF SECURITY INTEGRITY OF DATA COLLECTION FOR GE'S EPM 7000 POWER QUALITY SMART ELECTRIC METER UNDER A CYBER ATTACK

Cyber security must be utmost priority and matter of top concern for companies manufacturing and installing smart meters to keep system data secure and to maintain system's reliability and integrity. With implementation of internet of things (IoT), digital system and internet-based data communication in smart electric meters used in the electric power networks there comes the threat of cyber-attacks. With all the additional features and merits of smart meter still there is no significant research done and not enough research data published out which infers how and to what extent, the cyber-attacks can affect the smart electric meters operation and remote data collections of the power usage to remote monitoring sites from smart electric meters. Moving ahead with these questions, we conducted different experiments in a controlled and stabilized lab environment of our network research lab to testify actual impact of direct and indirect cyber-attack on different smart electric meters. In this chapter, we are going to present results from our different investigations done on EPM 7000 commercial grade power quality smart meter from General Electric and how its operation got affected under a cyber-attack.

4.1. EPM 7000 Power Quality Smart Electric Meter from GE

The EPM 7000 shown in (Figure.4.1) is one of the smart meters manufactured by GE [55], which allows service providers to monitor and manage their energy usage within factories, businesses and campuses. The EPM 7000 is a multifunction meter that features ANSI C12.20 (0.2% class) accuracy and provides several interfaces such as RS485 and RJ45 Ethernet, making the smart meter easy to deploy in new or preexisting communications systems. Early detection of power problems is facilitated through THD and the alarming capabilities of the EPM 7000. The units use standard 5 or 1-amp CTs (either split or donut), surface mount to any wall. EPM 7000 smart multifunction meters can be easily programmed and configured as stated in the manuals [55]. The key benefits of this smart multifunction meter are that it provides a variety of voltage, current and energy measurements. It can also allocate energy usage in multi-tenant settings such as apartment complexes, university campus towers, and shopping malls.



Volts

	1 sec
A-N	120.19
B-N	120.23
C-N	120.19
A-B	0.00
B-C	0.00
C-A	0.00

Current (I)

	1 sec	Maximum
A	0.00	0.46
B	0.00	0.00
C	0.00	0.00
Nc	0.00	0.46

Frequency 59.981

Real Power (W)

	Total	A	B	C
1 sec	0.00	0.00	0.00	0.00
+Average	0.00	0.00	0.00	0.00
-Average	0.00	0.00	0.00	0.00
+Maximum	27.21	27.21	0.00	0.00
-Maximum	0.00	0.00	0.00	0.00

Reactive Power (vars)

	Total	A	B	C
1 sec	0.00	0.00	0.00	0.00
+Average	0.00	0.00	0.00	0.00
-Average	0.00	0.00	0.00	0.00
+Maximum	48.20	48.20	0.00	0.00
-Maximum	-0.01	-0.01	0.00	0.00

Apparent Power (VAs)

Total	A	B	C
0.00	0.00	0.00	0.00
0.00	0.00	0.00	0.00
55.41	55.41	0.00	0.00

Figure 4.1. Smart Multifunction Meter (EPM 7000) with Ener Vista Software for remote power recording from GE [55]

EnerVista Software from GE [55] shown in (figure 4.1) provides service providers a platform to remotely access all setup and support tools needed for configuration and maintenance of GE smart meters. This software can remotely configure devices in real-time over network connections, and it can remotely read metered power usage data, and monitor status of the smart meters.

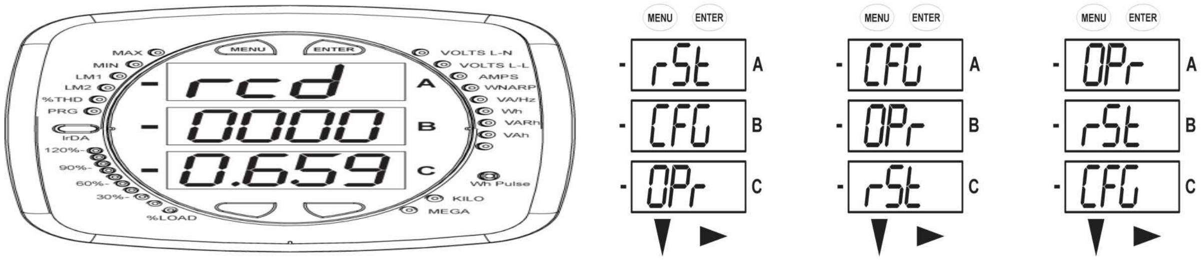


Figure 4.2: Manual Reading Parameters Setting from smart meter [55]

It can be observed from the (Figure 4.2) that from the front panel of the meter we can read out several parameters when meter is in use like voltage between phases, phase to neutral, current, Watt-hour, active, reactive and apparent power, baud rate, percentage total harmonic distortion etc. One can also configure the parameters from the front panel buttons like menu and left-right arrow. One can configure the smart meter for the parameters from the meter front panel as well as through software installed in computer at remote location. In this research focus was to configure and read out from the meter from its front panel and to configure it manually for WH recording to be done. Front panel has four buttons for the navigation including up and down arrow for scrolling up and down for the options. Then it has menu button for going to the configuration options. From the front panel of the meter one can configure Potential Transformer (PT) ratio, Current Transformer (CT) ratio, reset the meter, adjust baud rate, configure address, see the value of voltage, current, Watt Hour (WH), and power, adjust the electrical connection etc. .

4.2 Experimental Setup

In this chapter, we evaluated the security in Smart Meter Namely General Electric (GE) company's Multilin EPM 7000 Power Quality Meter with Ethernet port installed and 60Hz of operating frequency.

EPM 7000 power quality meter is connected to the remote computer and attacker network as shown in the (Figure.4.4). In this experiment, we used “3 EL WYE” in Meter Programming Setup as provided by General Electric Company [55].

For the experiments, a 200- Watt load (in the form of two light bulbs) is connected to the smart meter at the LOAD end (figure.4.3).

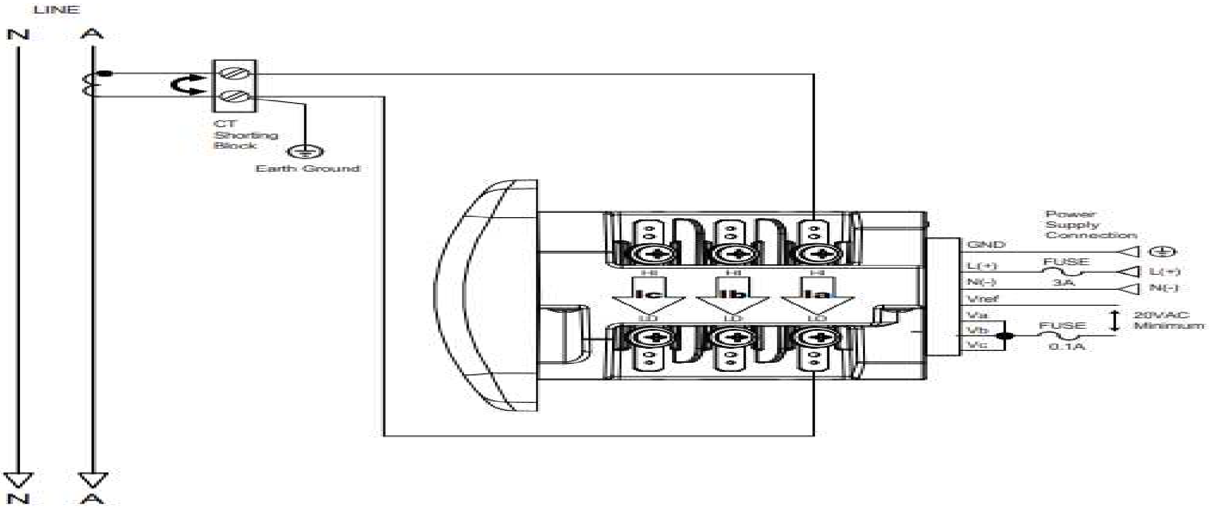


Figure 4.3: “3 EL WYE” in Meter Programming Setup [55]

By using monitoring computer, power consumption data is obtained remotely from the smart meter. Simulated Ping based security attack traffic was sent to the smart meter. The schematics of the experimental set up is shown in (Figure 4.4). We used simulated traffic in the protected environment of the Network Research Laboratory (NRL) at UTRGV.

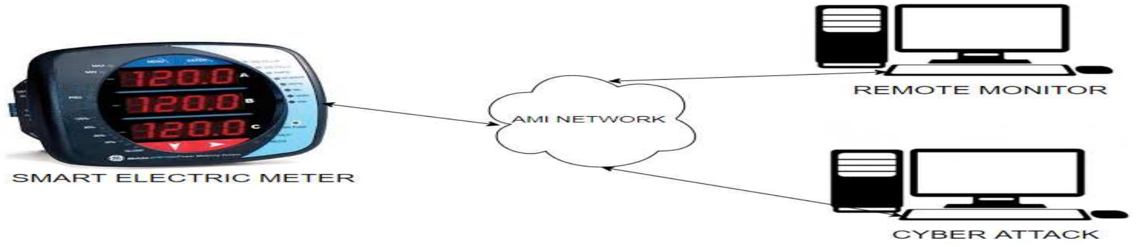


Figure 4.4: Experimental setup for cyber-attack

For experiments, we used General Electric's EPM 7000 Power Quality Meter as the Smart meter under test. It was remotely accessed for power usage data reading over Ethernet utilizing GE communicator software EnerVista, which was installed on a remote monitoring computer (Figure 4.5)

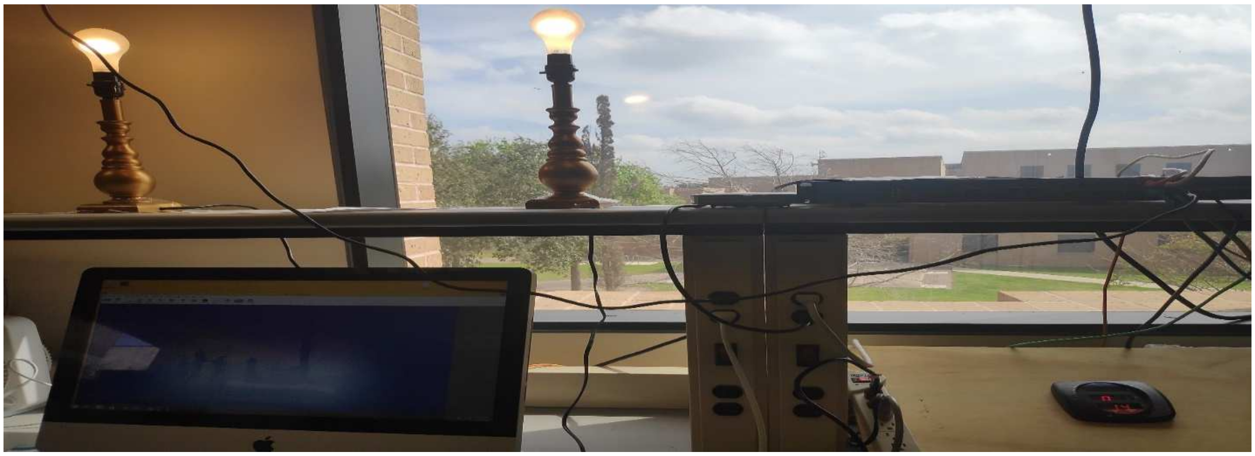


Figure 4.5: Lab set up used in Experiments showing Load, Smart meter and monitoring remote computer

We conducted five independent experiments to observe the impact of a Cyber Security Attack on the Watt Hour reporting over several days and its deviation from the baseline Watt Hour reporting when there was no attack.

4.3 Performance Parameters for Evaluation

4.3.1 Experiment I Under Indirect Attack for 4-days

For Experiment I, we used two incandescent light bulbs which together measured a 200-Watt of load for this smart meter. We used this load as the baseline load (in the absence of any attack traffic going to the smart electric meter). We used this baseline load for the smart meter operation for 4 days (96 hours). We remotely collected the power usage data to confirm the stability of the data collected (for the baseline load in the absence of any Cyber-attack) which is shown in the 2nd column of Table 4.1.

And then we repeated the same experiment under the conditions of indirect Cyber-attack. We remotely collected power consumption data (shown in 3rd column of Table 4.1) again for the next 4 days (96 hours) from the smart meter under conditions of the Ping based indirect Cyber-attack. Ping attack traffic experienced by the smart meter was measured to be a continuous 50 Mbps, which is considered rather a low intensity Cyber-attack these days.

4.3.2. Experiment II Under Indirect Attack for 7-days

For Experiment II, we used two incandescent light bulbs which together measured a 200-Watt of load for this smart meter. We used this load as the baseline load (in the absence of any attack traffic going to the smart electric meter). We used this baseline load for the smart meter operation for 7 days (168 hours). We remotely collected the power usage data to confirm the stability of the data collected (for the baseline load in the absence of any Cyber-attack) which is shown in the 2nd column of (Table 4.2). And then we repeated the same experiment under the conditions of indirect Cyber-attack. We remotely collected power consumption data (shown in 3rd column of Table 4.2) again for the next 7 days (168 hours) from the smart meter under conditions of the Ping based indirect Cyber-attack. Ping attack traffic experienced by the smart meter was measured to be a continuous 50 Mbps, which is considered rather a low intensity Cyber-attack these days.

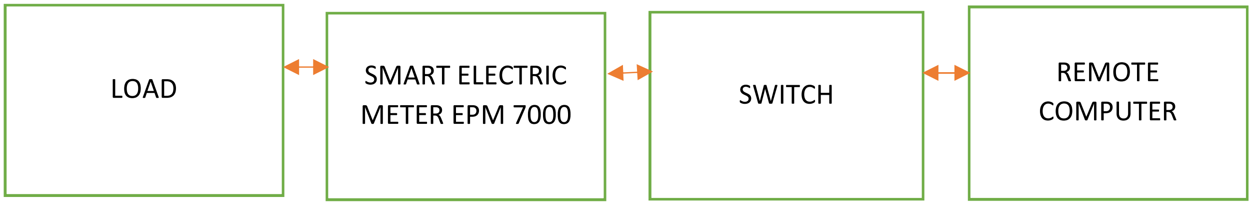


Figure 4.6: Experimental setup for Experiments

4.3.3 Experiment III Under Indirect Attack for 15-days

For Experiment III, we used one incandescent light bulb which measured a 200-Watt of load for this smart meter. We used this load as the baseline load (in the absence of any attack traffic going to the smart electric meter). We used this baseline load for the smart meter operation for 15 days (360 hours).

We remotely collected the power usage data to confirm the stability of the data collected (for the baseline load in the absence of any Cyber-attack) which is (shown in the 2nd column of Table 4.3). And then we repeated the same experiment under the conditions of indirect Cyber-attack. We remotely collected power consumption data (shown in 3rd column of Table 4.3) again for the next 15 days (360 hours) from the smart meter under conditions of the Ping based indirect Cyber-attack. Ping attack traffic experienced by the smart meter was measured to be a continuous 50 Mbps, which is considered rather a low intensity Cyber-attack these days.

4.3.4 Experiment IV Under Indirect Attack for 30-days

For Experiment-IV, we used one incandescent light bulb which measured a 200-Watt of load for this smart meter. We used this load as the baseline load (in the absence of any attack traffic going to the smart electric meter). We used this baseline load for the smart meter operation for 30 days (720 hours). We remotely collected the power usage data to confirm the stability of the data collected (for the baseline load in the absence of any Cyber-attack) which is (shown in the 2nd column of Table 4.4). And then we repeated the same experiment under the conditions of indirect Cyber-attack. We remotely collected power consumption data (shown in 3rd column of Table 4.4) again for the next 30 days (720 hours) from the smart meter under conditions of the Ping based indirect Cyber-attack.

Ping attack traffic experienced by the smart meter was measured to be a continuous 50 Mbps, which is considered rather a low intensity Cyber-attack these days.

4.3.5 Experiment V Under Direct Attack

In further investigation smart meter was experimented under direct cyber-attack. Smart meter was experimented for one entire day under no attack, one entire day under direct cyber-attack and one final day after attack being removed. The same experimental set up was used as shown in (Figure 4.6). This experiment was done to check the connectivity issue of smart meter under cyber-attack while communicating data from smart meter to remote monitoring computer at utility.

4.4 Results and discussion

4.4.1 Results from Experiment I

We observed (figure 4.7) that for the first 24 hours of the Cyber-attack there was no significant impact on the power readings however after 24 hours, the smart meter reported declining power consumption data. (Table 4.1) shows average power consumption for 96 hours (4 days), shown as a running average Power consumption after 1st day, 2nd day, 3rd day and 4th day in the third column of the (Table-4.1).

Table 4.1: Average power consumption with and without the Cyber-attack on the smart meter measured for 4-days

Time (in Days)	Baseline-Average power consumption (in watt hours)	Average power consumption under cyber-attack (in watt hours)	% loss of power consumption reported
1	202.62	202.35	0.13
2	201.62	201.27	0.17
3	201.10	200.67	0.21
4	200.84	200.25	0.29

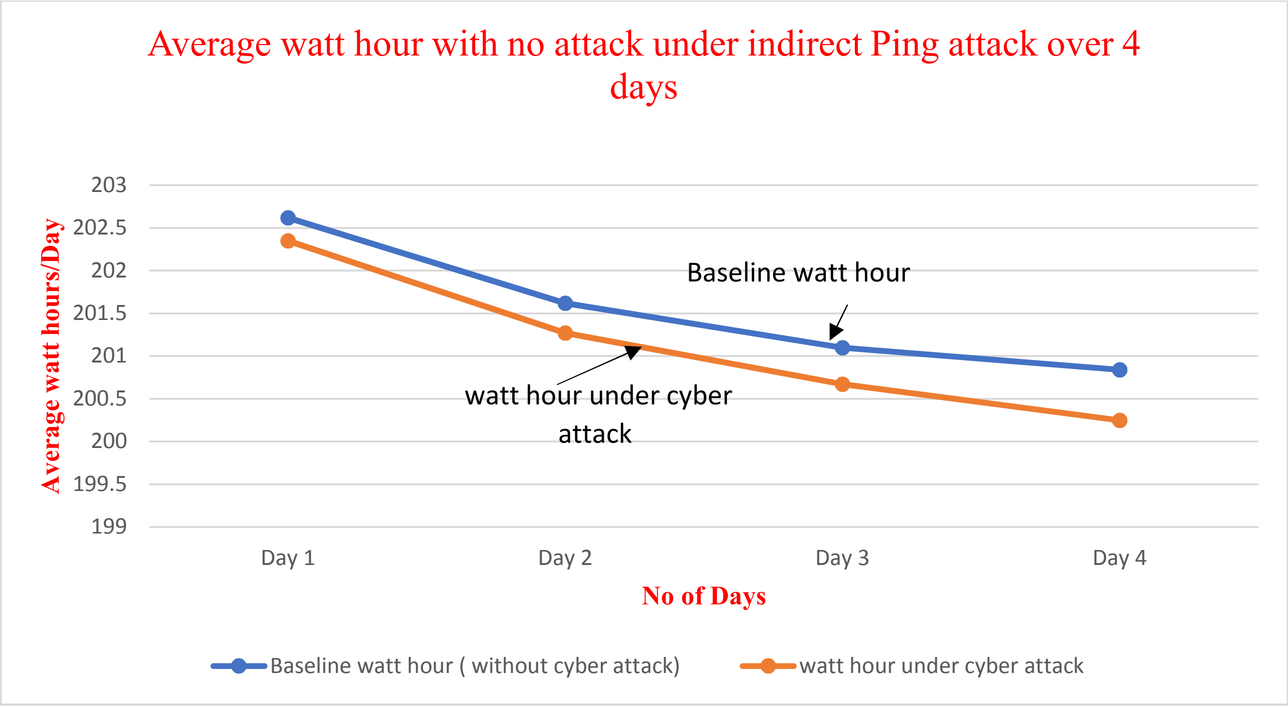


Figure 4.7**:** Average Power Consumption measured in Average Watt hour for Experiment-I without cyber-attack (baseline shown in blue) and with indirect cyber-attack (shown in orange)

Loss of Power Consumption reported under Cyber attack

% Loss of Power reported (after 4 days) =

$$\frac{Power\,Consumption\,(Baseline) - Power\,Consumption\,(Cyber\,Attack)}{Power\,Consumption\,(Baseline)} * 100$$

=[(200.84 – 200.25) / 200.84] *100= 0.29 %

In Experiment-I, by the end of Day 4, the smart meter reported a cumulative power loss of 0.29 % (compared to the baseline values) because of security attack on the smart meter. Power consumption reporting for baseline (blue) and power consumption reporting under Cyber-attack conditions (red) is shown for four consecutive days in (figure 4.7). There seems to be a trend in the continued decline in the average power consumption as reported by the smart meter to the remote computer under the influence of the Cyber-attack.

Power loss of 0.29 % may seem little, but it makes a big difference when it comes to a large commercial deployment of smart meters by a large Electric company and an example is shown below.

Financial loss estimation due to the Cyber-attack for a large Electric Company's deployment under Experiment I setup

Here we estimate how this type of Cyber-attack on Smart meters will affect revenue of a large electric company assuming they use this type of smart meters in their deployments. Some of the power consumption data has been obtained for the Pacific Gas & Electric in 2015 from [53] and are given below:

Name of Company: Pacific Gas & Electric.

Number of Customers (Residential and Commercial)=5,069,189

Total power consumption per month = 6,040,152,083 kWh

Average price from ref [53] = 17.41 cents per kWh

Loss of power due to security attack on Smart Meter/Smart Grid = 17,526,343 kWh per month based on our experimental result of 0.29 % reported loss.

Total Loss of revenue due to Cyber-attack on Smart Meter/Smart Grid network = $3.04 Million per month.

4.4.2 Results from Experiment-II

We observed (Figure 4.8) that for the first 24 hours of the Cyber-attack there was no significant impact on the power readings however after 24 hours, the smart meter reported declining power consumption data.

(Table 4.2) shows average power consumption for 168 hours (7 days), shown as a running average Power consumption after 1st day to 7th day in the third column of the Table 4.2.

Table 4.2: Average power consumption with and without the Cyber-attack on the smart meter measured for 7-days

Time (in days)	Baseline-Average power consumption reported without attack (in watt hours)	Average power consumption under cyber-attack (in watt hours)	% loss of power consumption reported
1	202.62	202.35	0.13
2	201.62	201.27	0.17
3	201.10	200.67	0.21
4	200.84	200.25	0.29
5	200.54	199.8	0.37
6	200.73	199.53	0.60
7	200.95	199.35	0.79

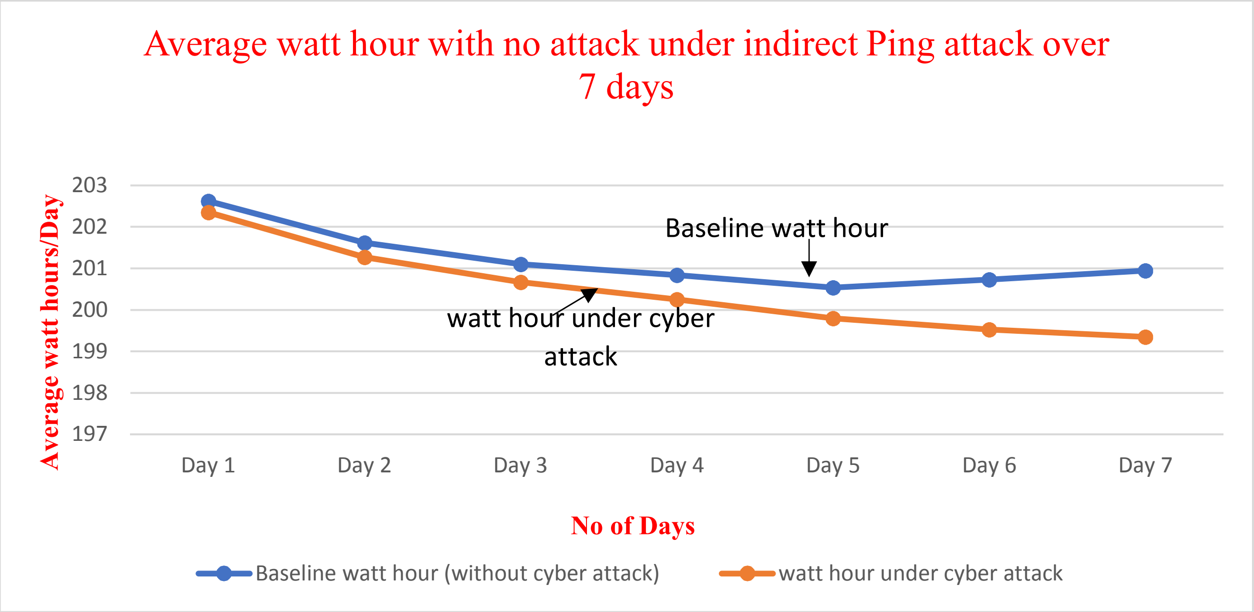


Figure 4.8: Average Power Consumption measured in Average Watt hour for Experiment II without cyber-attack (baseline shown in blue) and with indirect cyber-attack (shown in orange)

Loss of Power Consumption reported under Cyber attack

% Loss of Power reported (after 7 days)

$$\frac{Power\ Consumption\ (Baseline) - Power\ Consumption\ (Cyber\ Attack)}{Power\ Consumption\ (Baseline)} * 100$$

= [(200.95-199.35) / 200.95] *100 = 0.79%

In Experiment-II, by the end of Day 7, the smart meter reported a cumulative power loss of 0.79 % (compared to the baseline values) because of security attack on the smart meter. Power consumption reporting for baseline (blue) and power consumption reporting under Cyber-attack conditions (orange) is shown for 7 consecutive days in (figure 4.8). There seems to be a trend in the continued decline in the average power consumption as reported by the smart meter to the remote computer under the influence of the Cyber-attack same as experiment I. Power loss of 0.79 % may seem little, but it makes a big difference when it comes to a large commercial deployment of smart meters by a large Electric company and an example is shown below.

Financial loss estimation due to the Cyber-attack for a large Electric Company's deployment under Experiment II setup

Here we Estimate how this type of Cyber-attack on Smart meters will affect revenue of a large electric company assuming they use this type of smart meters in their deployments. Some of the power consumption data has been obtained for the Pacific Gas & Electric in 2015 from [53] and are given below:

- Name of the company: Pacific Gas & Electric
- Company data obtained from Ref [53] in 2015
- No of customer (Residential and Commercial) = 5,069,189
- Total power consumption per month= 6,040,152,083 KWH
- Average price [53] = 17.41 cents per kWh
- Loss of power due to security attack on smart meter/smart grid per month based on our experimental result of 0.79 % loss = 46,019,382 kWh
- Loss of revenue to the utility company due to cyber-attack on smart meter /smart grid = 7.87 million USD per month.

4.4.3 Result for Experiment III

We observed (Figure 4.9) that for the first 24 hours of the Cyber-attack there was no significant impact on the power readings however after 24 hours, the smart meter reported declining power consumption data. (Table 4.3) shows average power consumption for 360 hours (15 days), shown as a running average Power consumption after 1st day to 15th day in the third column of the (Table 4.3).

Table 4.3: Average power consumption with and without the Cyber-attack on the smart meter measured for 15-days

Time (in days)	Baseline-Average power consumption reported without attack (in watt hours)	Average power consumption under cyber-attack (in watt hours)	% loss of power consumption reported
1	202.62	202.35	0.13
2	201.62	201.27	0.17
3	201.10	200.67	0.21
4	200.84	200.25	0.29
5	200.54	199.8	0.37
6	200.73	199.53	0.60
7	200.95	199.35	0.79
8	200.87	199.04	0.91
9	200.94	198.79	1.06
10	201.12	198.57	1.27
11	201.35	198.39	1.47
12	201.26	198.08	1.58
13	201.33	197.79	1.76
14	201.34	197.53	1.90
15	201.70	197.34	2.16

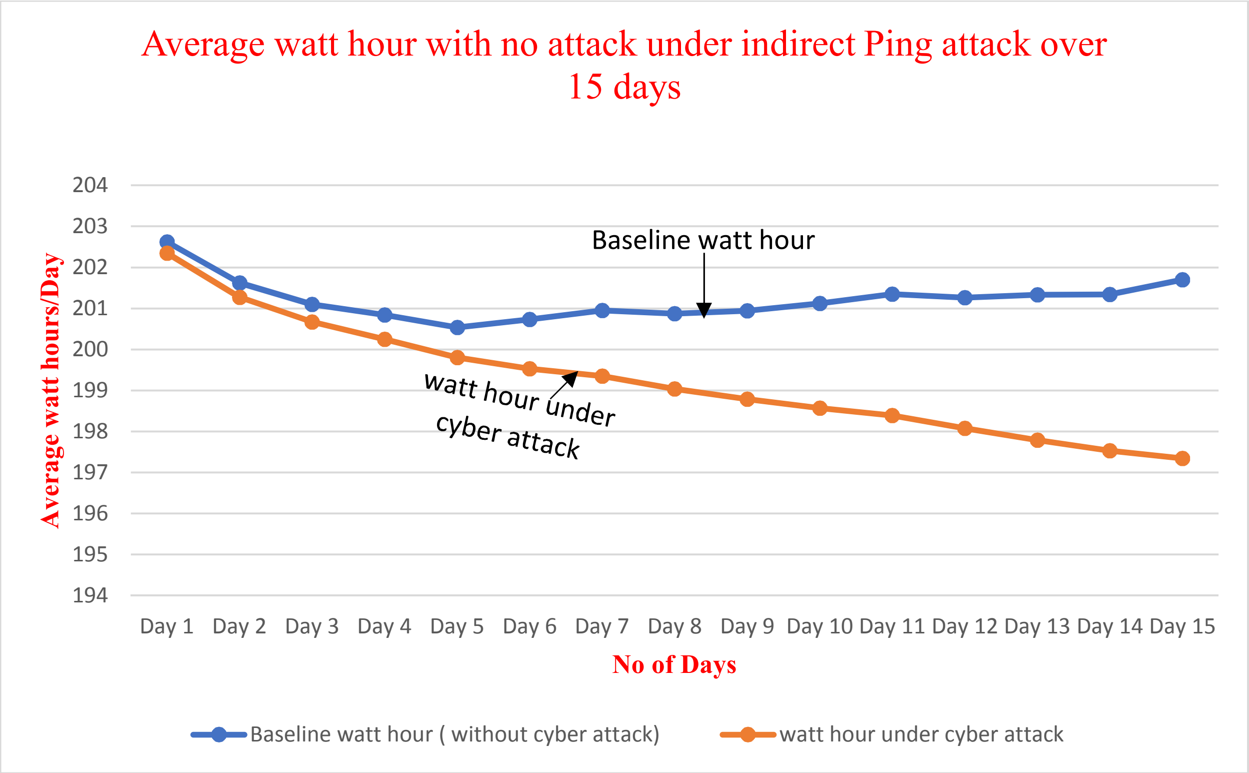


Figure 4.9: Average Power Consumption measured in Average Watt hour for Experiment III without cyber-attack (baseline shown in blue) and with indirect cyber-attack (shown in orange)

Loss of Power reported under Cyber attack

% Loss of Power reported (after 15 days) =

$$\frac{Power\ Consumption\,(Baseline) - Power\ Consumption\,(Cyber\ Attack)}{Power\ Consumption\,(Baseline)} * 100$$

= [(201.7 – 197.34) / 201.7] *100 = 2.16%

In Experiment-III, by the end of Day 15, the smart meter recorded a cumulative power loss of 2.16 % (compared to the baseline watt hours) because of security attack on the smart meter. Power usage recorded for baseline and power usage recorded under Cyber-attack conditions is shown for 15 consecutive days in (Figure 4.9). There seems a trend in the continued decline in the average power consumption as reported by the smart meter to the remote computer under the influence of the Cyber-attack. Power loss of 2.16 % may looks a little, but it can make a big difference when it comes to a large commercial deployment of smart meters by a large Electric company and an example is shown below.

Financial loss estimation due to the Cyber-attack for a large Electric Company’s deployment under Experiment III setup

Here we estimate how this type of Cyber-attack on Smart meters will affect revenue of a large electric company assuming they use this type of smart meters in their deployments. Some of the power consumption data has been obtained for the Pacific Gas & Electric in 2015 from [53] and are given below:

- Name of Company: Pacific Gas & Electric.
- Number of Customers (Residential and Commercial) = 5,069,189
- Total power consumption per month = 6,040,152,083 KWh. Average price from ref [53] = 17.41 cents per KWh
- Loss of power due to security attack on Smart Meter/Smart Grid = 130,467,285 KWh per month based on our experimental result of 2.16 % reported loss.
- Total Loss of revenue due to Cyber-attack on Smart Meter/Smart Grid network = $22.71 Million per month.

4.4.4 Results from Experiment IV

We observed (Figure 4.10) that for the first 24 hours of the Cyber-attack there was no significant impact on the power readings however after 24 hours, the smart meter reported declining power consumption data. (Table 4.4) shows average power consumption for 720 hours (30 days), shown as a running average Power consumption after 1st day to 30th day in the third column of the (Table-4.4).

Table 4.4: Average power consumption with and without the Cyber-attack on the smart meter measured for 30-days

Time (in days)	Average WH with No attack	Average WH under cyber attack	% deviation or WH decline under attack from baseline WH
1	202.62	202.35	0.13
2	201.62	201.27	0.17
3	201.10	200.67	0.21
4	200.84	200.25	0.29
5	200.54	199.8	0.37
6	200.73	199.53	0.60
7	200.95	199.35	0.79
8	200.87	199.04	0.91
9	200.94	198.79	1.06
10	201.12	198.57	1.27
11	201.35	198.39	1.47
12	201.26	198.08	1.58
13	201.33	197.79	1.76
14	201.34	197.53	1.90
15	201.70	197.34	2.16
16	201.76	197.06	2.33
17	201.57	196.61	2.46
18	201.51	196.33	2.57
19	201.44	195.98	2.71
20	201.53	195.75	2.87
21	201.43	195.43	2.98
22	201.63	195.36	3.11
23	201.47	194.9	3.26
24	201.77	194.65	3.53
25	201.54	194.12	3.68
26	201.67	194.3	3.71
27	201.50	194.2	3.70
28	201.70	194.2	3.72
29	201.68	194.2	3.71
30	201.70	194.2	3.72
31	200.54	199.7	0.41
32	201.20	200.7	0.24

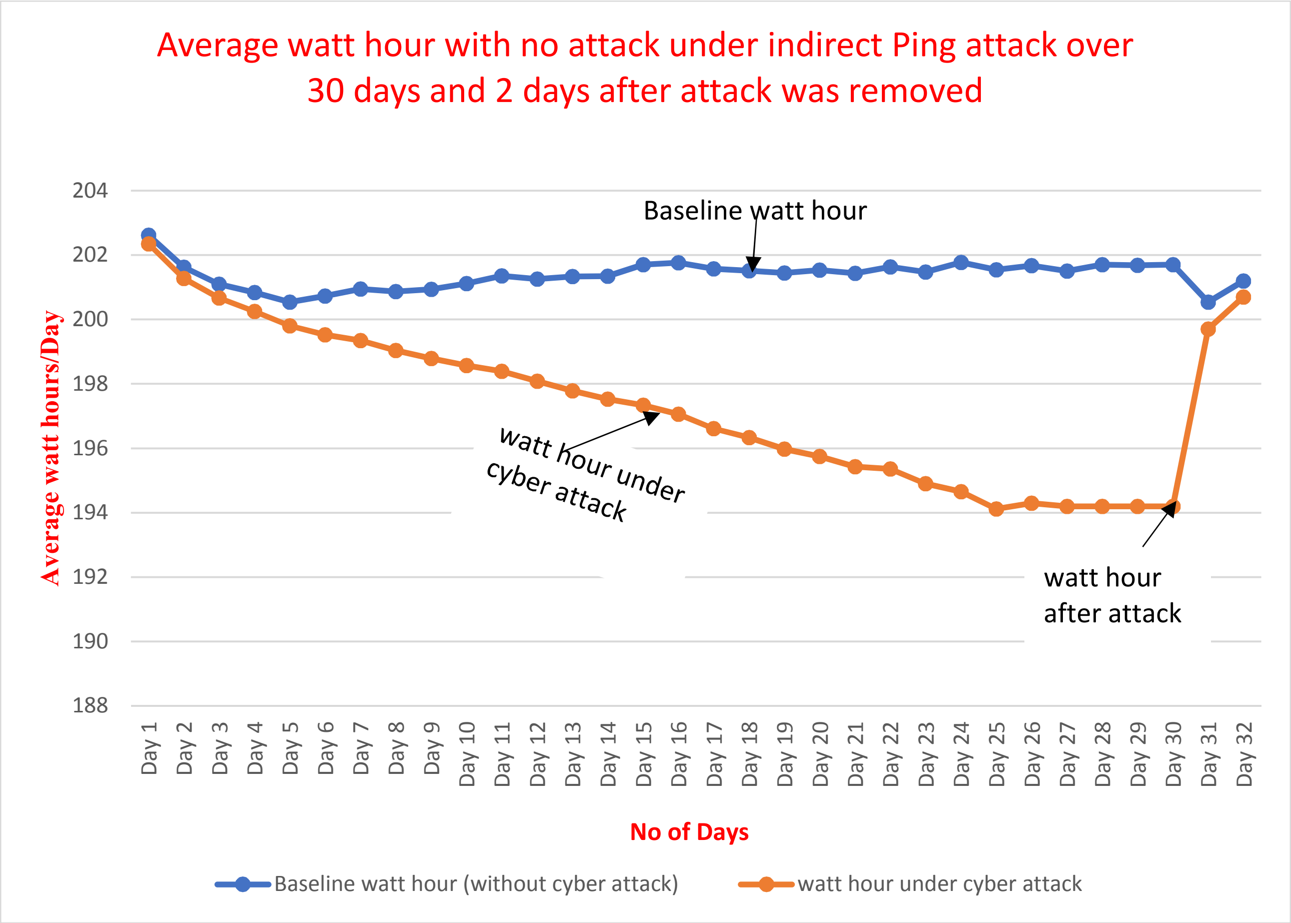


Figure 4.10: Average Power Consumption measured in Average Watt hour for Experiment IV without cyber-attack (baseline shown in blue) and with indirect cyber-attack (shown in orange)

Loss of Power reported under Cyber attack

% Loss of Power reported (after 30 days) =

$$\frac{Power\ Consumption\left(Baseline\right) - Power\ Consumption\left(Cyber\ Attack\right)}{Power\ Consumption\ (Baseline)} \quad * \ 100$$

= [(201.7 – 194.2) / 201.7] *100 = 3.72 %

In Experiment-IV, by the end of Day 30, the smart meter recorded a cumulative power loss of 3.72 % (compared to the baseline watt hours) because of security attack on the smart meter.

Power usage recorded for baseline and power usage recorded under Cyber-attack conditions is shown for 30 consecutive days and 2 days after attack was removed in (figure.4.10). There seems no further decline in the average power consumption as reported by the smart meter to the remote computer under the influence of the Cyber-attack at the end of the 30 days typical customer billing cycle. Power loss of 3.72 % may looks a little, but it can make a big difference when it comes to a large commercial deployment of smart meters by a large Electric company and an example is shown below.

Financial loss estimation due to the Cyber-attack for a large Electric Company's deployment under Experiment IV setup

Here we estimate how this type of Cyber-attack on Smart meters will affect revenue of a large electric company assuming they use this type of smart meters in their deployments. Some of the power consumption data has been obtained for the Pacific Gas & Electric in 2015 from [53] and are given below:

- Name of Company: Pacific Gas & Electric.
- Number of Customers (Residential and Commercial) = 5,069,189
- Total power consumption per month = 6,040,152,083 KWh. Average price from ref [53] = 17.41 cents per KWh
- Loss of power due to security attack on Smart Meter/Smart Grid = 224,693,657 KWh per month based on our experimental result of 3.72 % reported loss.
- Total Loss of revenue due to Cyber-attack on Smart Meter/Smart Grid network = $39.11 Million per month.

Based on these different experiments and the measured results it is evident that the Cyber-attacks can adversely affect the operation of smart meters, which in turn can result in a significant financial loss for a large electric company deployment of smart meters.

4.4.5 Results from Experiment V

On day 1 without attack there was no impact on data recording for this smart meter. On day 2 it shows that there is problem with communication as only old repeated data was communicated to the remote monitoring computer for the power usage under direct attack which was recorded just before the attack has started. GE meter still seems connected to the network because GE smart meter uses intel core duo 1.8 GHZ processor or even faster and under attack it has not lost all its processing power and connectivity options needed to implement most of functions such as consumption analysis, dynamic pricing, and other demand response features After the attacked being removed on day three the data started being recoded as usual which can be observed in (figure 4.11). As the intensity of the attack was increased beyond 50 Mbps there was no communication at all by the meter. This means this the minimum attack bandwidth required to create problem for meter while usage data communication.

Table 4.5: Watt hour with and without direct attack

Time (in Hours)	WH with no direct attack day 1
1	21.33
2	42.89
3	64.33
4	85.56
5	106.95
6	128.52
7	150.14
8	171.41
9	192.74
10	214.21
11	235.63
12	256.99
13	278.52

14	299.97
15	321.29
16	342.84
17	364.43
18	385.85
19	407.18
20	428.54
21	449.85
22	471.44
23	492.81
24	514.16
Time (in Hours)	**WH with direct attack day 2**
25	0
26	0
27	0
28	0
29	0
30	0
31	0
32	0
33	0
34	0
35	0
36	0
37	0
38	0
39	0
40	0
41	0
42	0
43	0
44	0
45	0
46	0
48	0
Time (in Hours)	**WH after attack removed**
49	1009.3
50	1029.87
51	1050.49
52	1070.93
53	1091.46
54	1112.23
55	1133.04
56	1153.68
57	1174.25

58	1194.91
59	1215.8
60	1236.67
61	1257.58
62	1278.63
63	1299.7
64	1320.79
64	1341.83
65	1362.95
66	1384.14
67	1405.31
68	1426.46
69	1447.45
70	1468.38
71	1489.23
72	1509.90

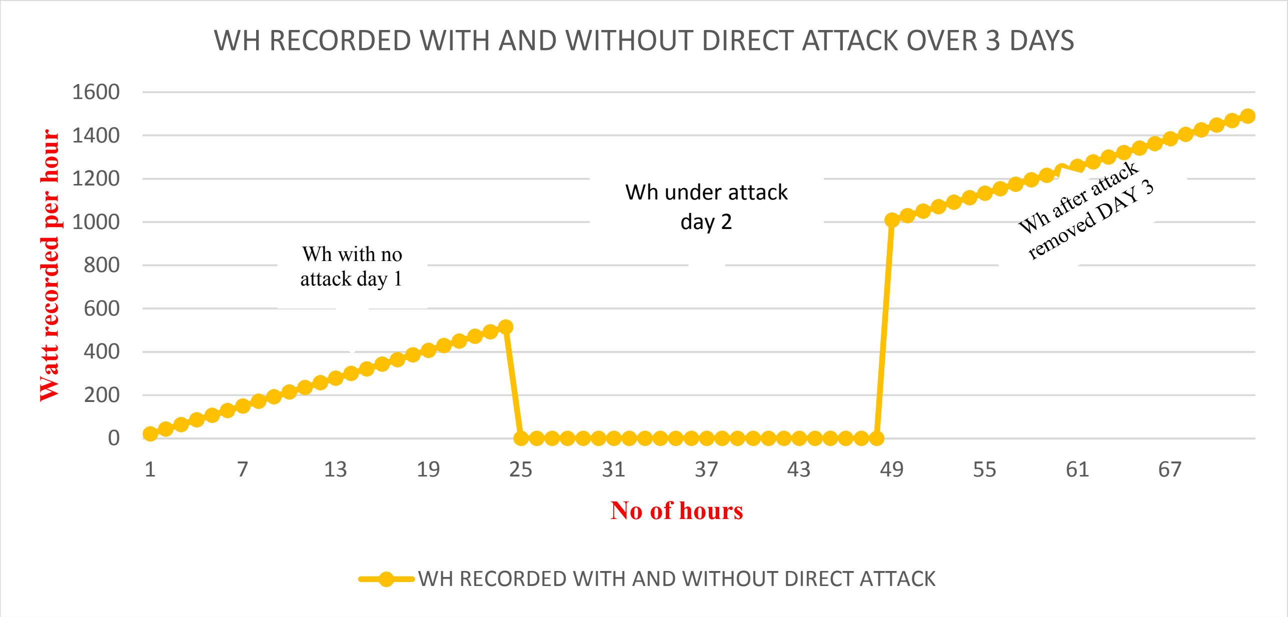


Figure 4.11: Data Communication to remote monitoring computer from smart meter under direct attack

4.5 Chapter Summary

In this chapter EPM 7000 smart electric meter has been exposed and evaluated under a real indirect and direct Cyber security attack to understand its effect on its operation and data communication to remote location. Smart meters are very handy for customers as well as utilities in their smart grid infrastructure implementation and to provide uninterrupted power monitoring and easy trouble shooting related to electric Smart meters in a smart grid. But the actual problem is security and the effect of security attacks was not known until this experiment was done. In this experiment, we found that even a very common indirect and direct Cyber security attack such as Ping based ICMP flood attack can have big impact on operation of a smart electric meter in smart grid infrastructure. While experimenting under indirect cyber-attack for customer billing cycle i.e. 30 days, starting day 1 there was not much significant impact but there was significant impact at the end of billing cycle. While experimenting under direct attack there was immediate impact as there was complete loss of data communication. These cyber security attacks can result in significant financial loss in millions of dollars for the power company's deployment in a large-scale smart grid infrastructure.

CHAPTER V

EVALUATION OF SMART METERING DATA COMMUNICATION FOR GE'S EPM 6100 AND EPM 7000 POWER QUALITY SMART ELECTRIC METER UNDER DIFFERENT CYBER-ATTACKS

The data transmission or communication process is the key characteristics of a smart electric meter in AMI system, because it introduces the "two-way communication" for energy measurement. Being the smart meters are the indispensable tool in AMI system, the goal of smart metering communication is to ensure a secure and reliable transmission of information to their data collectors that can only be accessed by the end user and the utility company. However, given that the possibility of compromising the information transmitted is real, efforts to ensure the security must be done. Cyber security in smart meter is the field of research that must secure the information from all the aspects of the security triad (confidentiality, integrity, and availability). As such, this research evaluates a scenario where a smart meter is subjected under cyber-attacks. This chapter showcases a series of experiments performed on smart meters with ethernet-based communication using a small-scale simulation of the process done by one of the utility companies. In order to achieve this simulation, a properly laboratory setup was designed along with specialized software developed by the department of electrical engineering at the University of Texas at Rio Grande Valley (UTRGV). The purpose of this chapter is to evaluate the security of smart meter to prevent third party actions and, therefore, improve the user experience.

5.1 Experimental Set Up

For research purposes, we used two different smart meters i.e. EPM 6100 and EPM 7000 power quality meter. For all our experiments, we used a fan as a load. Given that there was need to connect our smart meters to a data collector to transmit the information to the remote monitoring computer and to simulate the flooding cyber-attacks to the respective meters for evaluating their performance, we used ethernet network switch. Here is where the meters were connected on different ports as well as a remote monitoring computer used to monitor all the data gathered by the meters (this is the command center, or utility company). Therefore, our laboratory used the following diagram shown in (figure 5.1 and 5.2) respectively.

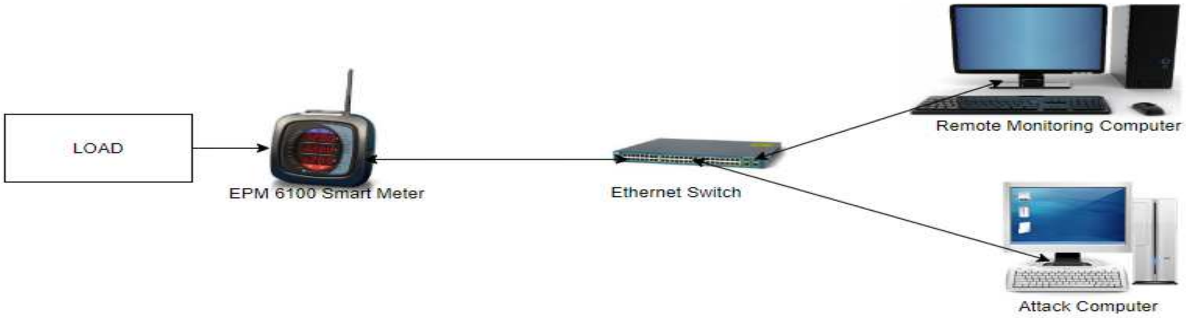


Figure 5.1: Experimental set up for evaluating EPM 6100 smart meter data communication performance under cyber-attack

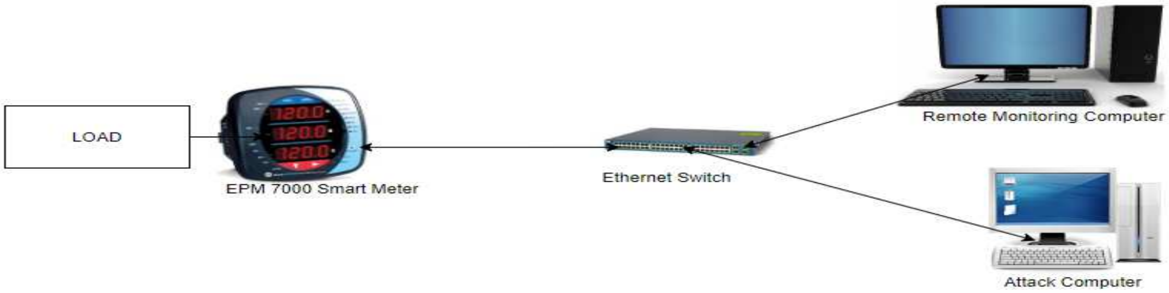
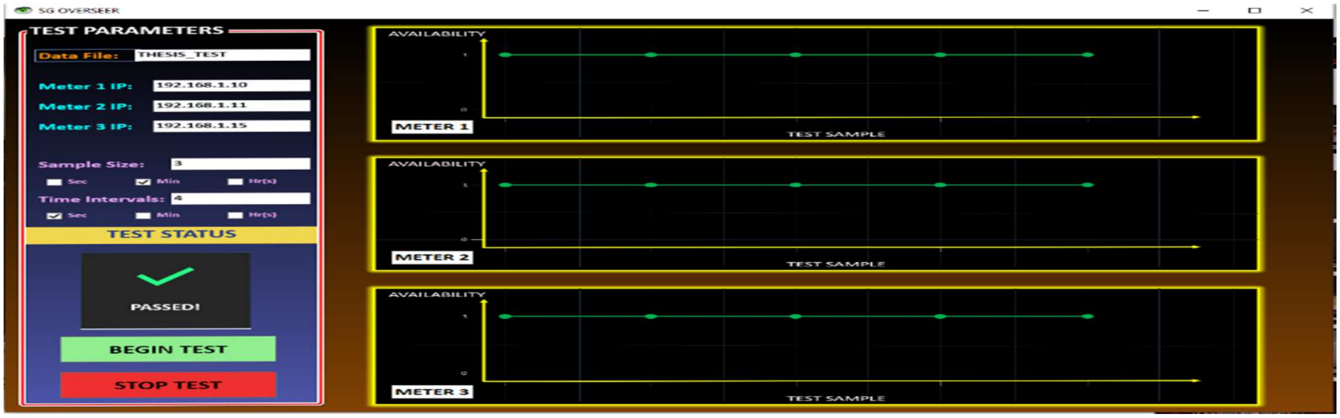


Figure 5.2: Experimental set up for evaluating EPM 7000 smart meter data communication performance under cyber-attack.

For every device connected and communicating data through ethernet switch were assigned with different IP address i.e. 192.1.15 and 192.1.11 for EPM 6100 and EPM 7000 respectively. Meters used for evaluation comes with a specialized software provided by the manufacturing company to display all concerning information to the user. In order to study the performance of the ethernet-based communication system, an attacking computer was introduced to the systems as if it were one more element. The idea behind the experiments is to attack the communication lines and observe the effect that it could bring to the information retrieved from the smart meters. Out of all the known cyber-attacks, three were used in the experiments which are the most practical to apply i.e. the Ping, Smurf attack and TCP/SYN attack respectively. In order to create an environment where an attacker floods the system, the use of the mentioned attacking computer becomes the key which play the role of the cyber attacker in this system. Since it was already stated that cyber-attacks has an effect on data communication, we wanted to evaluate how much minimum bandwidth of cyber-attack is required to break the communication, how much is the recovery time of the meter after attack is removed, if different attack has different effect on recovery time and is there any trend with the duration of attack on recovery time of meter. Having the integrity aspect compromised in a smart meter refers to any modification made to the information transferred from the meters to the monitoring computer, or when the information that comes out of the meter does not reflect the expected one (meter physically reports x watthour consumed, yet, the information that the monitoring computer receives is y).The other aspect to investigate is the information availability. During the attack, it must be observed if every meter used in the experiments remains available, meaning that the remote monitoring computer must always be able to access the information from respective connected meters.

A new software was developed Smart Meter Overseer (SM Overseer) shown in (figure 5.3). SM Overseer does not record the watthour consumption but only focuses on the connectivity status of the meters. 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 this means that 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 were under attack, there is no communication, and any ping request done by the monitoring computer resulted in a request timeout, and hence, the communication was considered as 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.



SG OVERSEER

TEST PARAMETERS

Data File: THESIS_TEST

Meter 1 IP: 192.168.1.10

Meter 2 IP: 192.168.1.11

Meter 3 IP: 192.168.1.15

Sample Size: 3

□ Sec ☑ Min □ Hr(s)

Time Intervals: 4

☑ Sec □ Min □ Hr(s)

TEST STATUS

PASSED!

Figure 5.3: SM Overseer Software for checking connectivity status of meters

5.2 Experimental Results and Discussion from EPM 6100 Smart Electric Meter

Several experiments were made attempting to study the connectivity behavior of the smart meters during data communication. The research focused on short time experiments to determine how fast the communication would break and how much time does the smart meter take to recover. Initially Experiment started with recording the baseline without attack for a brief period of 30 minutes which will acts as baseline for all the experiments. Then we repeated the experiment under attack for 30 seconds and then attack was removed checking for time of recovery under Ping, Smurf and TCP/SYN attack respectively. Maximum bandwidth capacity of ethernet port of this is given as 100 Mbps as per meter manufacturing company so CAT 5 cable was used which has maximum data transmission capacity of 100 Mbps. Attacker computer has maximum capacity to send flooding at the rate of 1Gbps so that means 10% of the total flooding capacity is enough for these experiments. We started sending flooding from 1% and kept on increasing. We observed that until 5% there was no effect on communication performance of this meter. So, we found out the minimum bandwidth to break the communication of this meter was 6%.

Table 5.1: Experiment Result of Performance of smart Metering Data Communication for EPM 6100 Power Quality Smart Electric Meter Under Different Flooding Cyber-Attacks

Time duration of cyber-attack in seconds	Disconnection time under ping attack in seconds	Recovery time after ping attack removed in seconds	Disconnection time under smurf attack in seconds	Recovery time after smurf attack removed in seconds	Disconnection time under TCP/SYN attack in seconds	Recovery time after TCP/SYN attack removed in seconds
30 sec	3	4	3	7	3	6
60 sec	3	7	3	14	3	10
120 sec	3	10	3	19	3	14
300 sec	3	14	3	23	3	19
600 sec	3	14	3	23	3	19
1200 sec	3	14	3	23	3	19

5.2.1 Experiment Results Under PING, SMURF and TCP/SYN Attack for 30 seconds

We observed that time to disconnection time under all kinds of attack was same and was 3 seconds which was almost immediate but the recovery time under all attacks was different and was 4 seconds in case of Ping attack, 7 seconds in case of Smurf attack and 6 seconds in case of TCP/SYN attack shown in (Figure 5.4, 5.5 and 5.6) respectively.

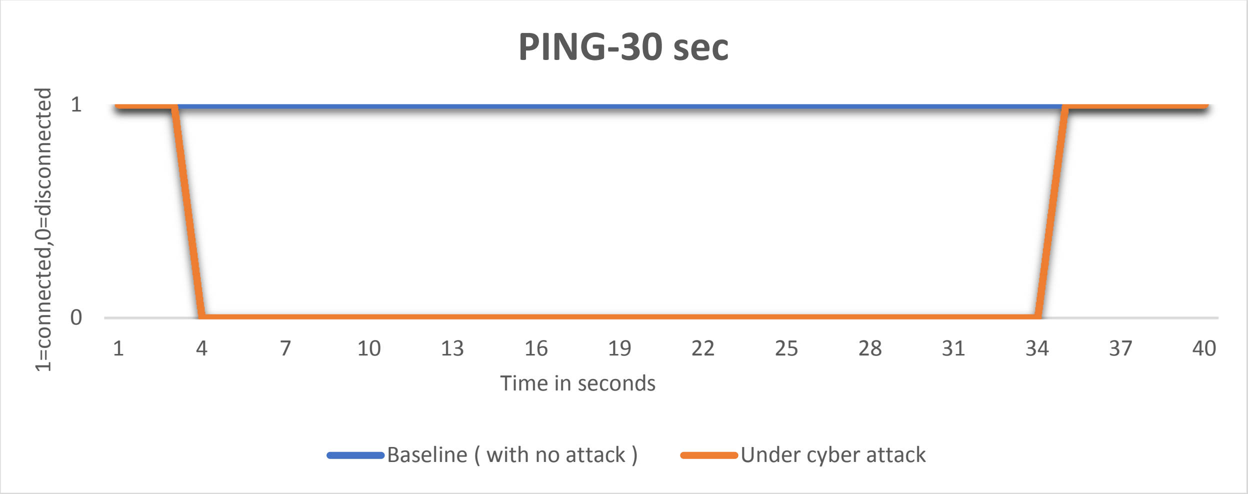


Figure 5.4: Observation under ping attack for 30 seconds

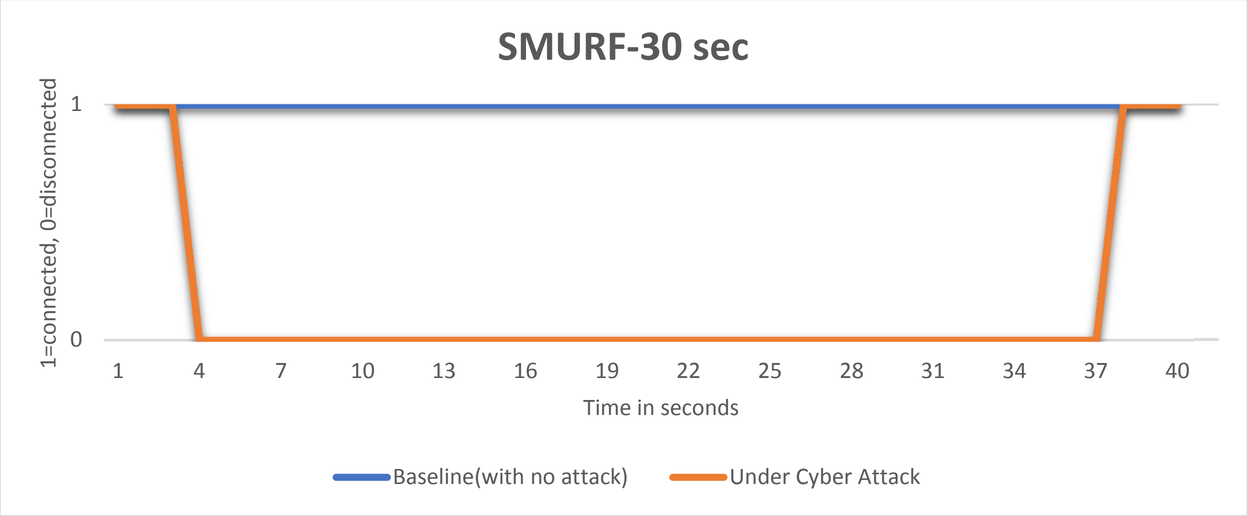


Figure 5.5: Observation under smurf attack for 30 seconds

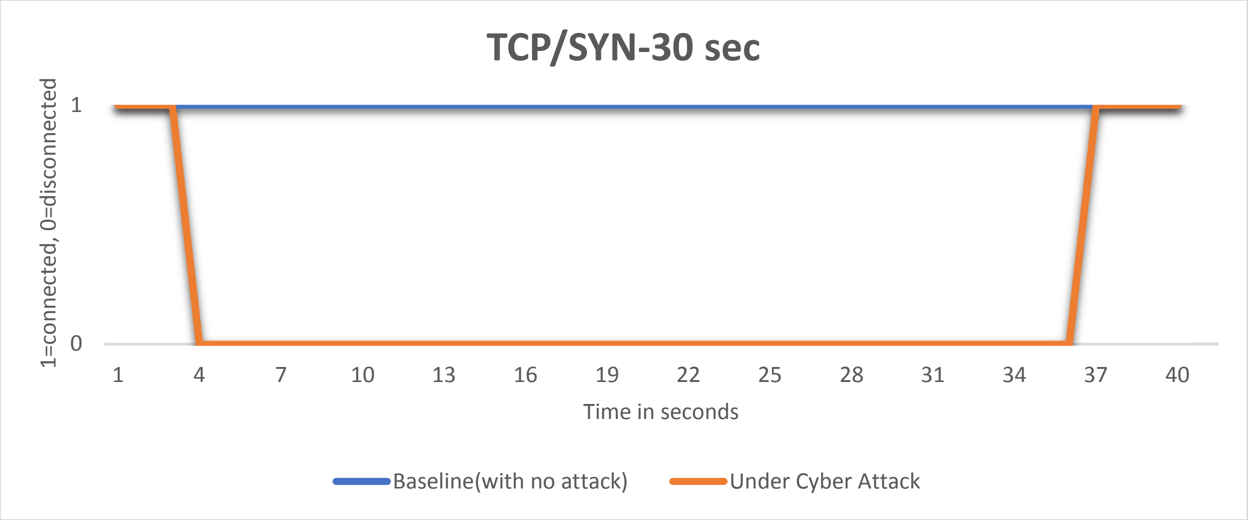


Figure 5.6: Observation under TCP/SYN attack for 30 seconds

5.2.2 Experiment Results Under PING, SMURF and TCP/SYN Attack for 60 seconds

To check on the trend of disconnection time and recovery time under attack we increased the attack duration to 60 seconds. We observed that time to disconnection time under all kinds of attack was same and was 3 seconds which was almost immediate but the recovery time under all attacks was different and was 7 seconds in case of Ping attack, 14 seconds in case of Smurf attack and 10 seconds in case of TCP/SYN attack shown in (Figure 5.7, 5.8 and 5.9) respectively.

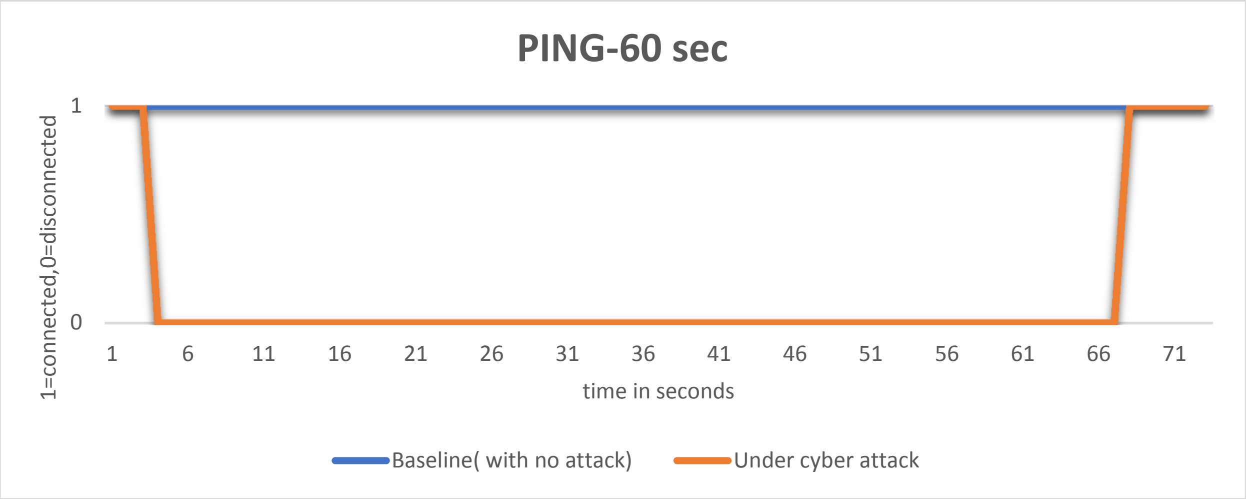


Figure 5.7 Observation under ping attack for 60 seconds

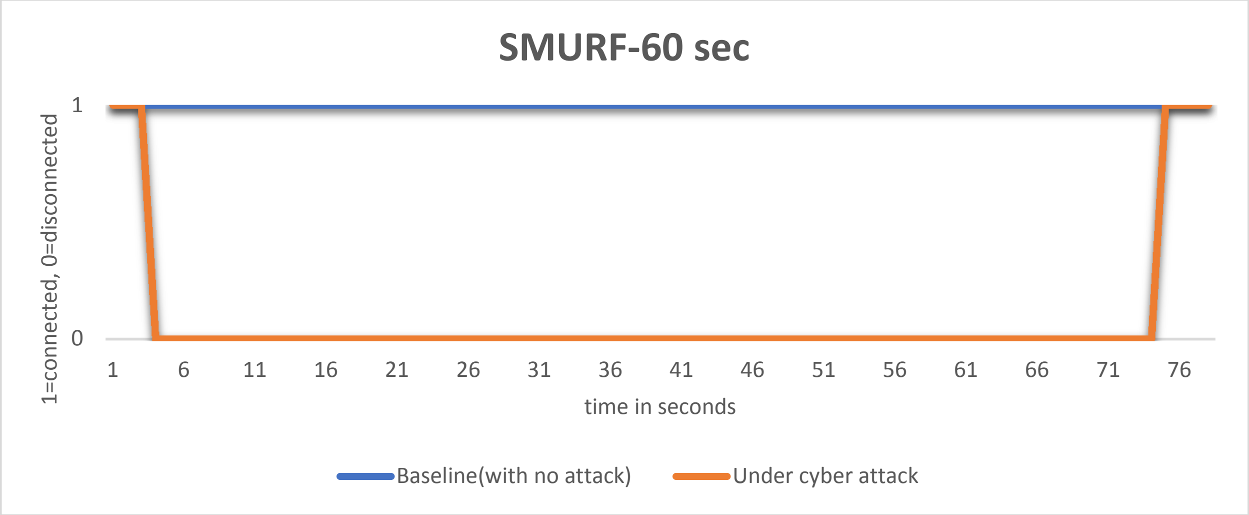


Figure 5.8: Observation under smurf attack for 60 seconds

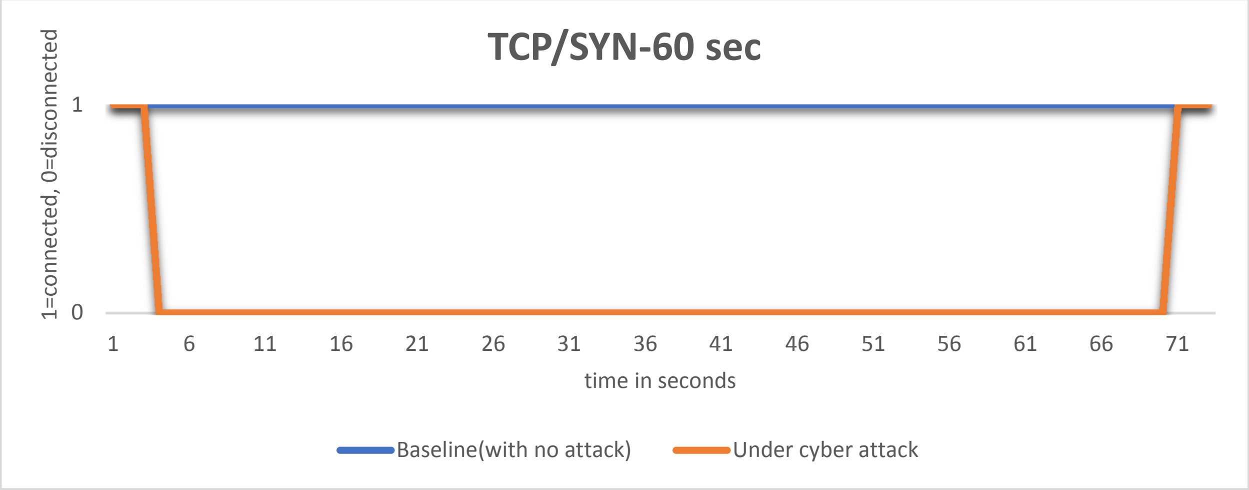


Figure 5.9 Observation under TCP/SYN attack for 60 seconds

5.2.3 Experiment Results Under PING, SMURF and TCP/SYN Attack for 120 seconds

To check on the trend of disconnection time and recovery time under attack we increased the attack duration to 120 seconds. We observed that time to disconnection time under all kinds of attack was same and was 3 seconds which was almost immediate but the recovery time under all attacks was different and was 10 seconds in case of Ping attack, 19 seconds in case of Smurf attack and 14 seconds in case of TCP/SYN attack shown in (Figure 5.10, 5.11and 5.12) respectively.

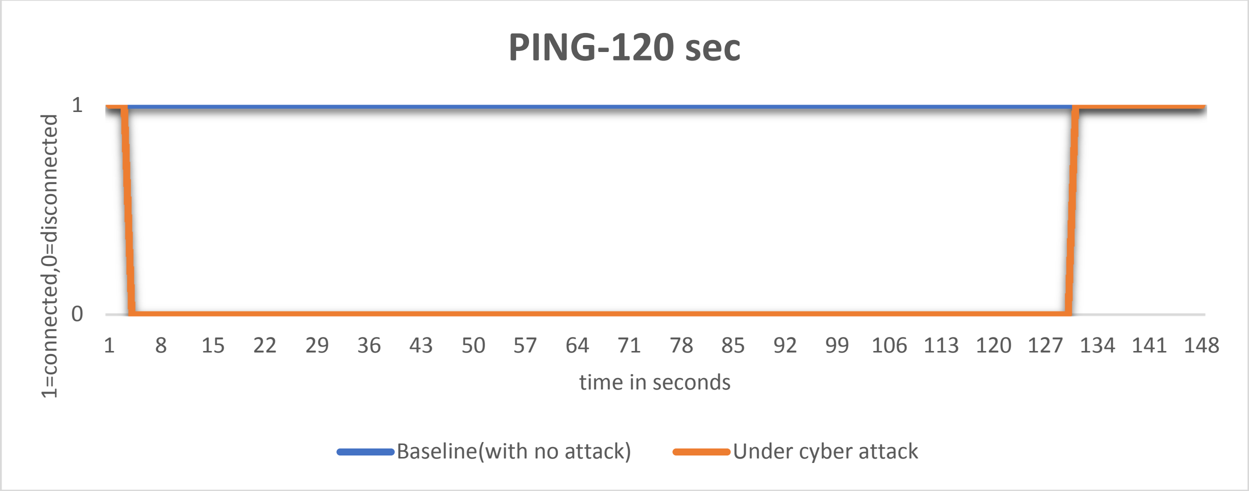


Figure 5.10: Observation under ping attack for 120 seconds

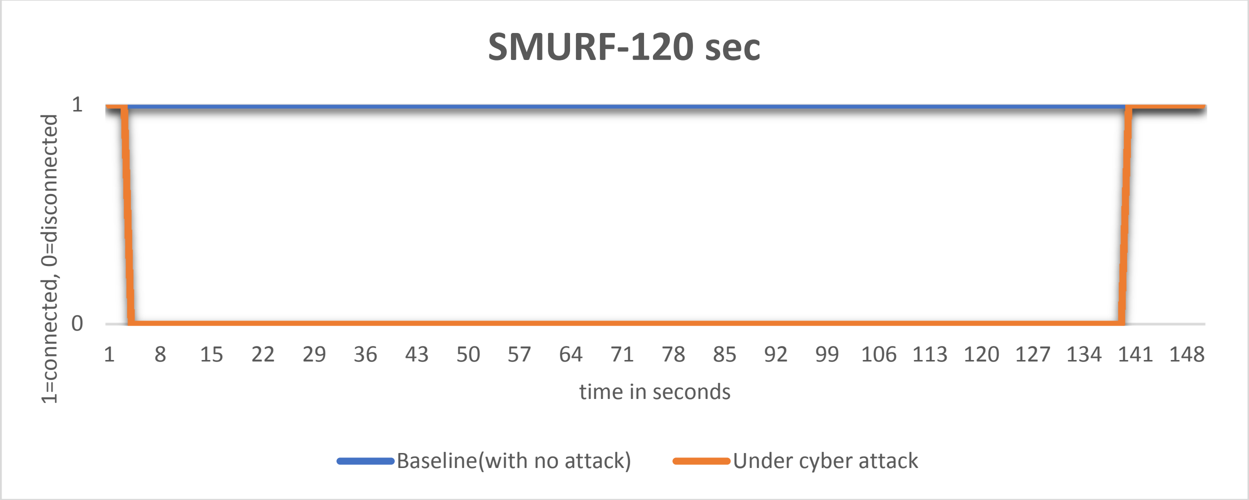


Figure 5.11: Observation under smurf attack for 120 seconds

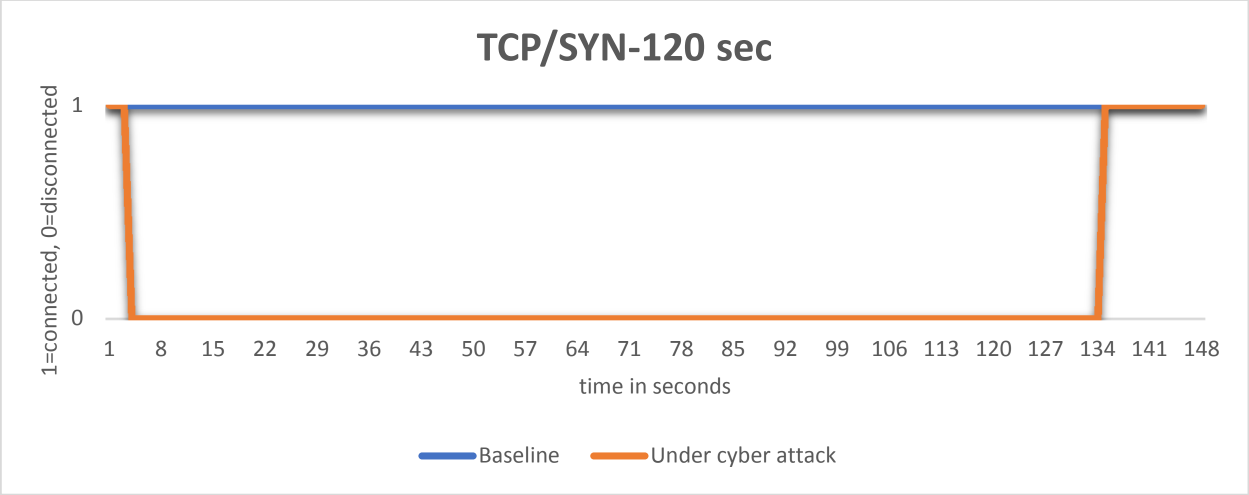


Figure 5.12: Observation under TCP/SYN attack for 120 seconds

5.2.4 Experiment Results Under PING, SMURF and TCP/SYN Attack for 300 seconds

To check on the trend of disconnection time and recovery time under attack we increased the attack duration to 300 seconds. We observed that time to disconnection time under all kinds of attack was same and was 3 seconds which was almost immediate but the recovery time under all attacks was different and was 14 seconds in case of Ping attack, 23 seconds in case of Smurf attack and 19 seconds in case of TCP/SYN attack shown in (Figure 5.13, 5.14 and 5.15) respectively.

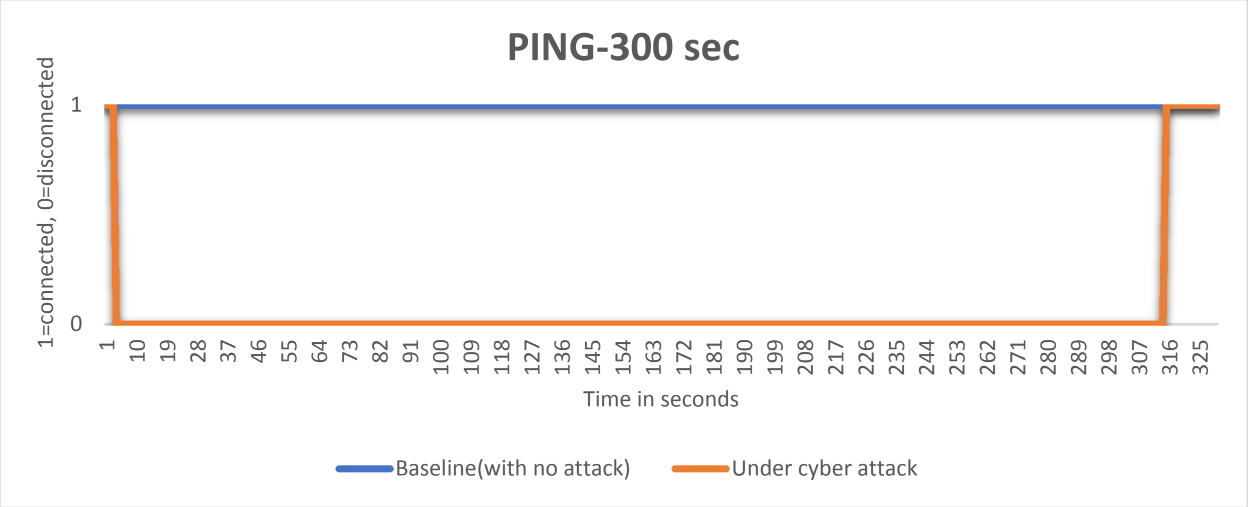


Figure 5.13: Observation under Ping attack for 300 seconds

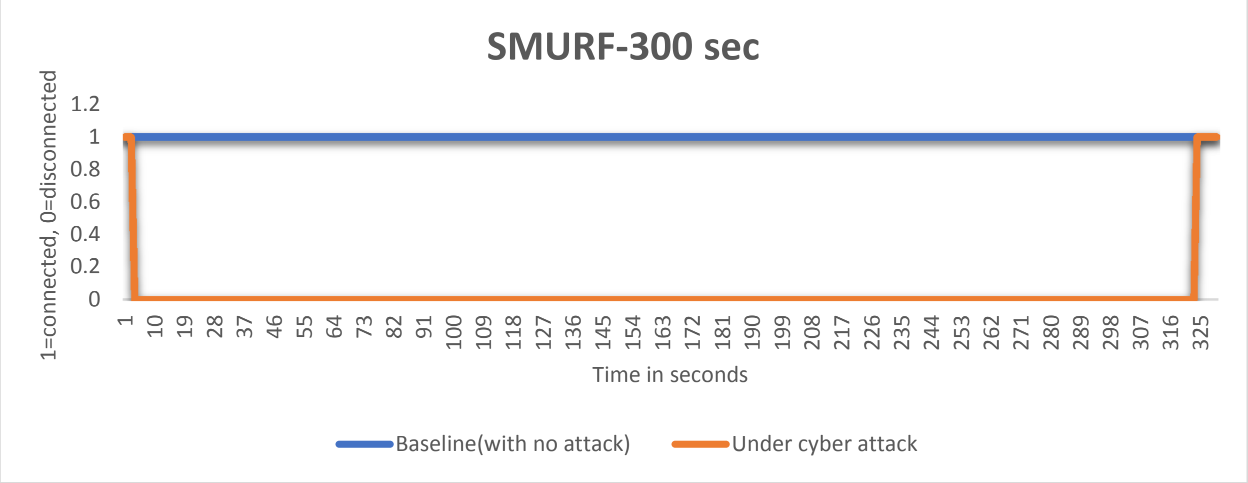


Figure 5.14: Observation under smurf attack for 300 seconds

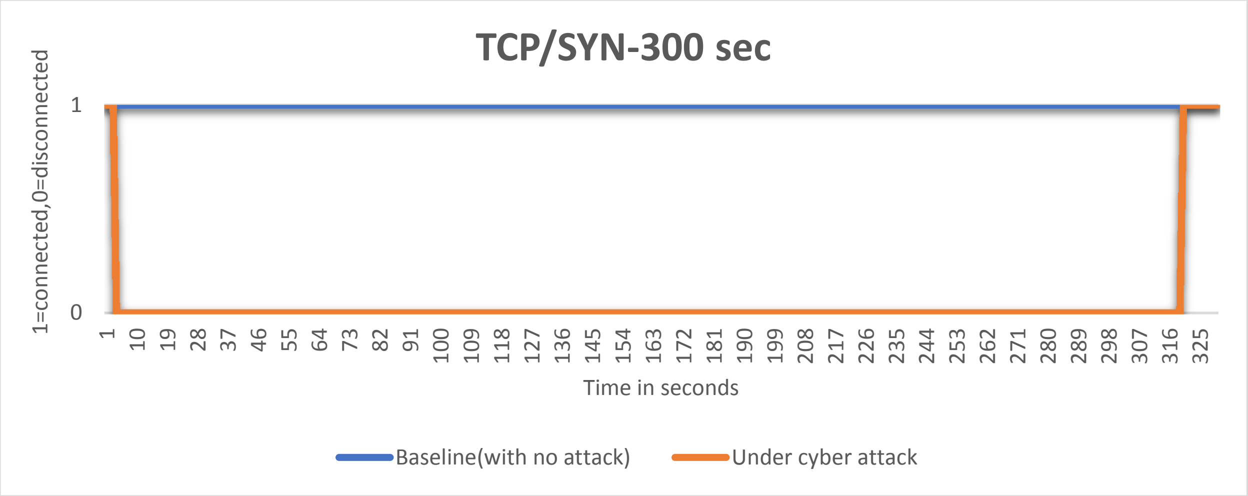


Figure 5.15: Observation under TCP/SYN attack for 300 seconds

5.2.5 Experiment Results Under PING, SMURF and TCP/SYN Attack for 600 seconds

To check on the trend of disconnection time and recovery time under attack we increased the attack duration to 600 seconds. We observed that time to disconnection time under all kinds of attack was same and was 3 seconds which was almost immediate but the recovery time under all attacks was different and was 14 seconds in case of Ping attack, 23 seconds in case of Smurf attack and 19 seconds in case of TCP/SYN attack shown in (Figure 5.16, 5.17 and 5.18) respectively.

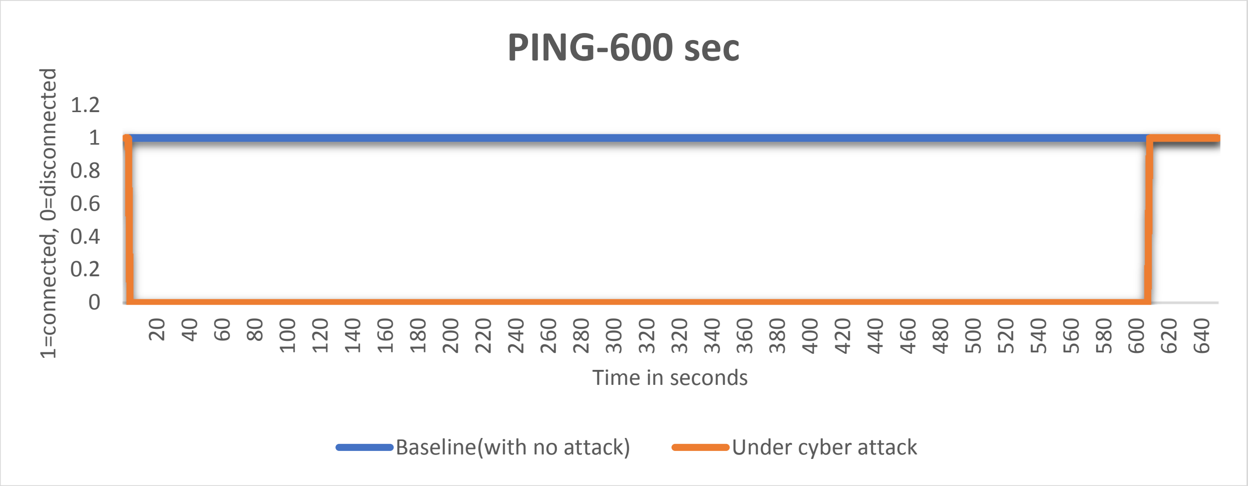


Figure 5.16: Observation under ping attack for 600 seconds

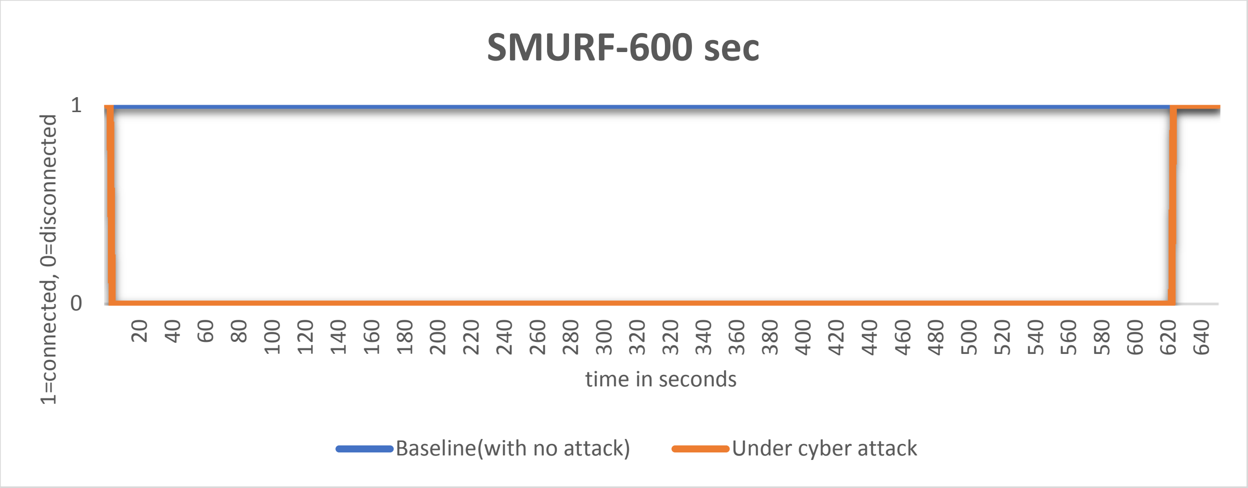


Figure 5.17: Observation under smurf attack for 600 seconds

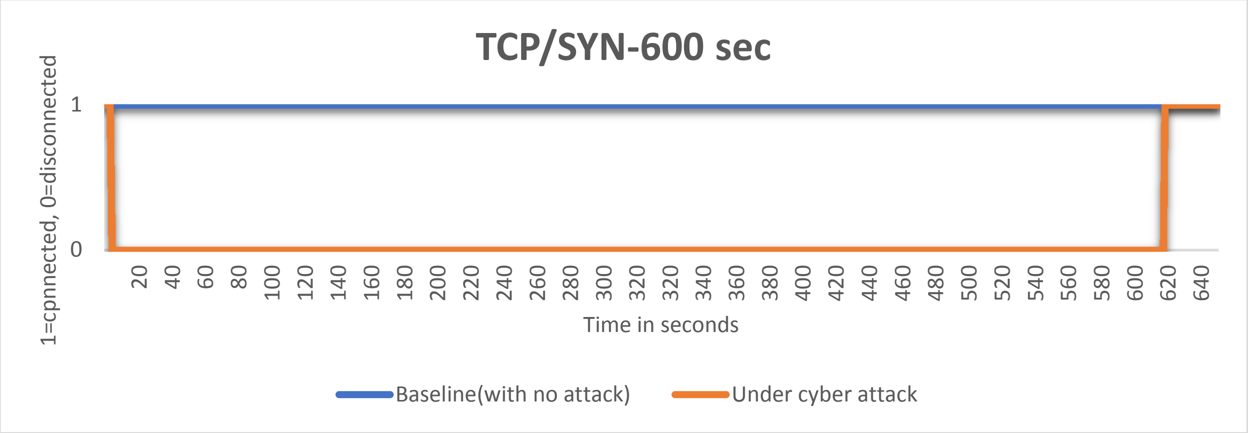


Figure 5.18: Observation under TCP/SYN attack for 600 seconds

5.2.6 Experiment Results Under PING, SMURF and TCP/SYN Attack for 1200 seconds

To check on the trend of disconnection time and recovery time under attack we increased the attack duration to 1200 seconds. We observed that time to disconnection time under all kinds of attack was same and was 3 seconds which was almost immediate but the recovery time under all attacks was different and was 14 seconds in case of Ping attack, 23 seconds in case of Smurf attack and 19 seconds in case of TCP/SYN attack shown in (Figure 5.19, 5.20 and 5.21) respectively.

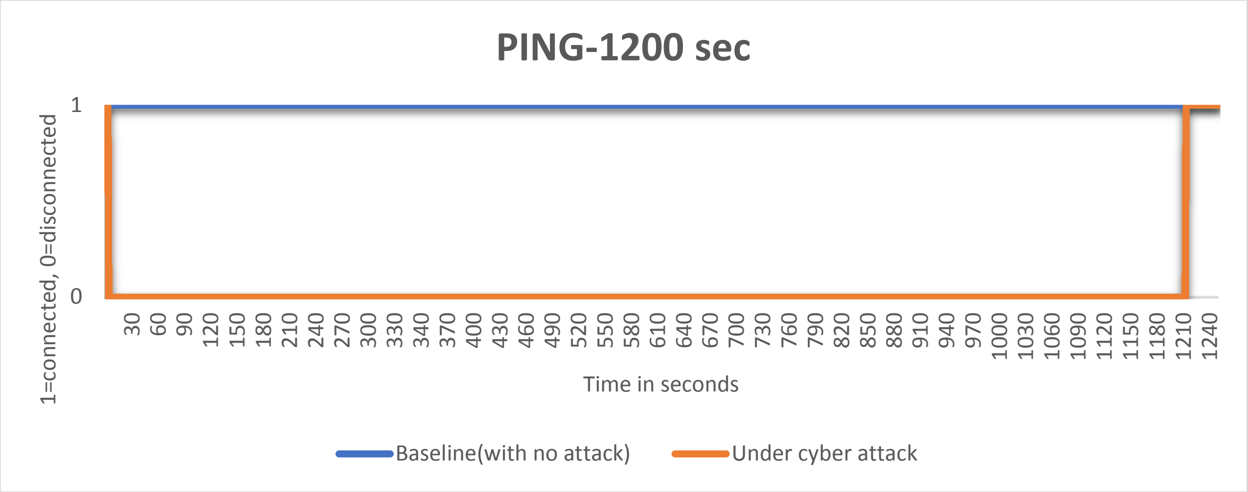


Figure 5.19: Observation under ping attack for 1200 seconds

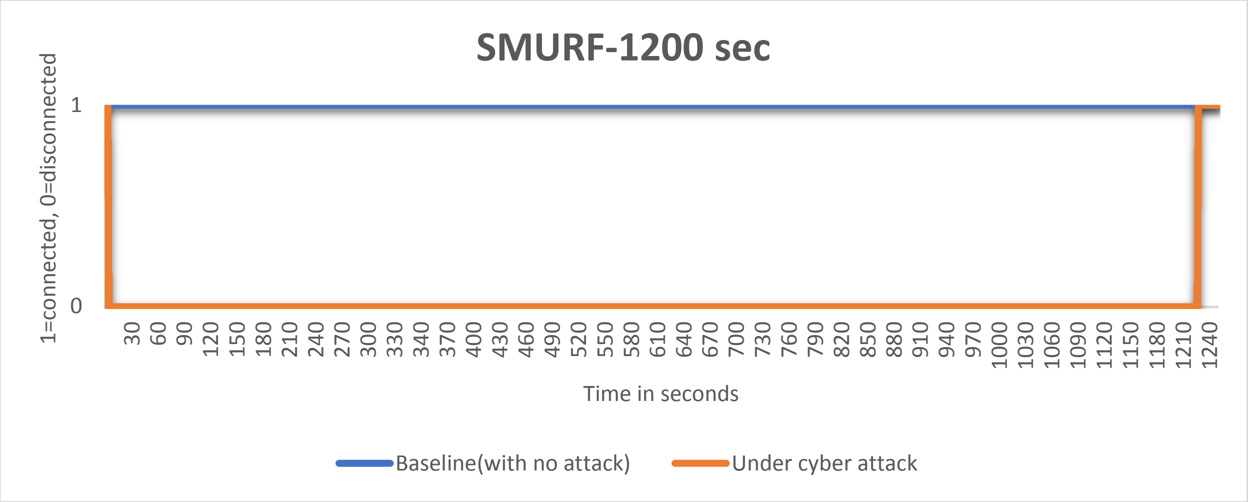


Figure 5.20: Observation under smurf attack for 1200 seconds

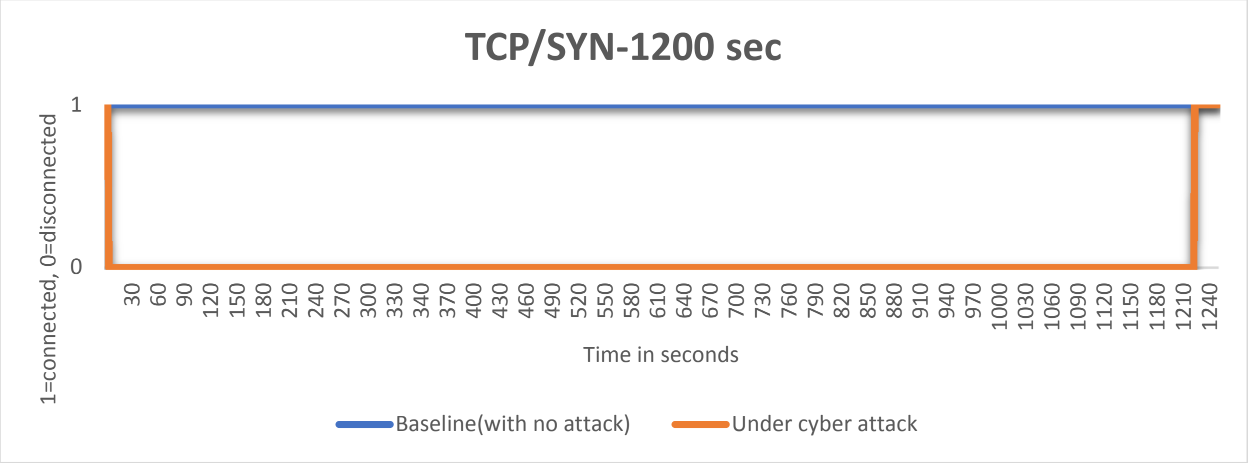


Figure 5.21: Observation under TCP/SYN attack for 1200 seconds

5.3 Experimental Results and Discussion from EPM 7000 smart meter

Several experiments were made attempting to study the connectivity behavior of the smart meters. The research focused on short time experiments to determine how fast the communication would break and how much time does the smart meter take to recover. Initially Experiment started with recording the baseline without attack for a brief period of 30 minutes which will acts as baseline for all the experiments. Then we repeated the experiment under attack for 30 seconds and then attack was removed checking for time of recovery under ping, smurf and TCP/SYN attack respectively. Maximum bandwidth capacity of ethernet port of this is given as 100 Mbps as per meter manufacturing company so CAT 5 cable was used which has maximum data transmission capacity of 100 Mbps. Attacker computer has maximum capacity to send flooding at the rate of 1Gbps so that means 10% of the total flooding capacity is enough for these experiments. We started sending flooding from 1% and kept on increasing. We observed that until 9% there was no effect on communication performance of this meter. So, we found out the minimum bandwidth to break the communication of this meter was 10%.

Table 5.2: Experiment Result of Performance of smart Metering Data Communication for EPM 7000 Power Quality Smart Electric Meter Under Different Flooding Cyber-Attacks

Time duration of cyber-attack in seconds	Disconnection time under ping attack in seconds	Recovery time after ping attack removed in seconds	Disconnection time under smurf attack in seconds	Recovery time after smurf attack removed in seconds	Disconnection time under TCP/SYN attack in seconds	Recovery time after TCP/SYN attack removed in seconds
30 sec	5	2	5	3	5	2
60 sec	5	3	5	5	5	3
120 sec	5	4	5	8	5	6
300 sec	5	7	5	12	5	9
600 sec	5	7	5	12	5	9
1200 sec	5	7	5	12	5	9

5.3.1 Experiment Results Under PING, SMURF and TCP/SYN Attack for 30 seconds

We observed that disconnection time all kinds of attack was same and was 5 seconds which was almost immediate but the recovery time under all attacks was different and was 2 seconds in case of ping attack, 3 seconds in case of smurf attack and 2 seconds in case of TCP/SYN attack shown in (Figure 5.22, 5.23 and 5.24) respectively.

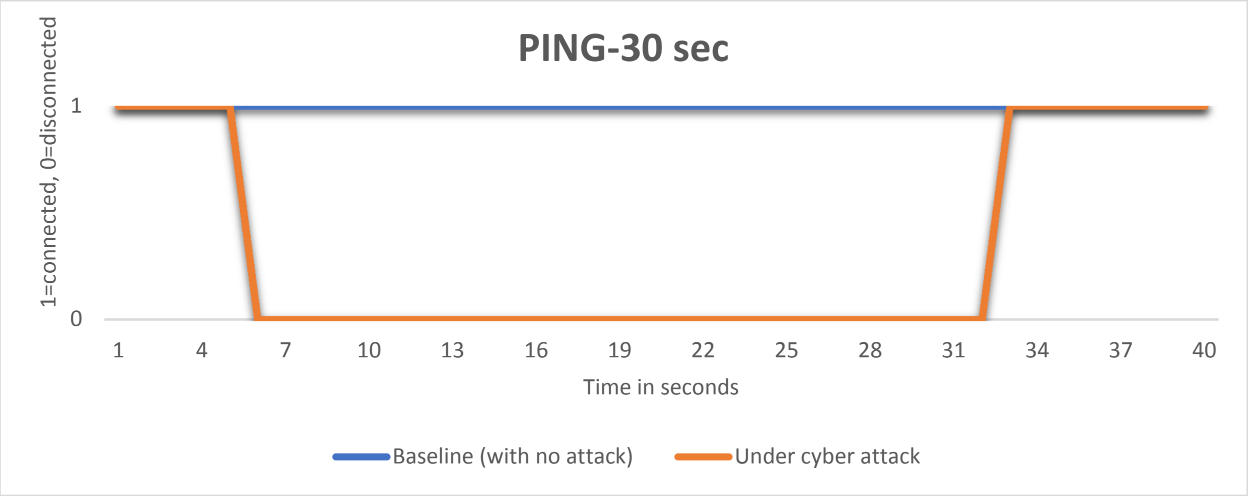


Figure 5.22: Observation under ping attack for 30 seconds

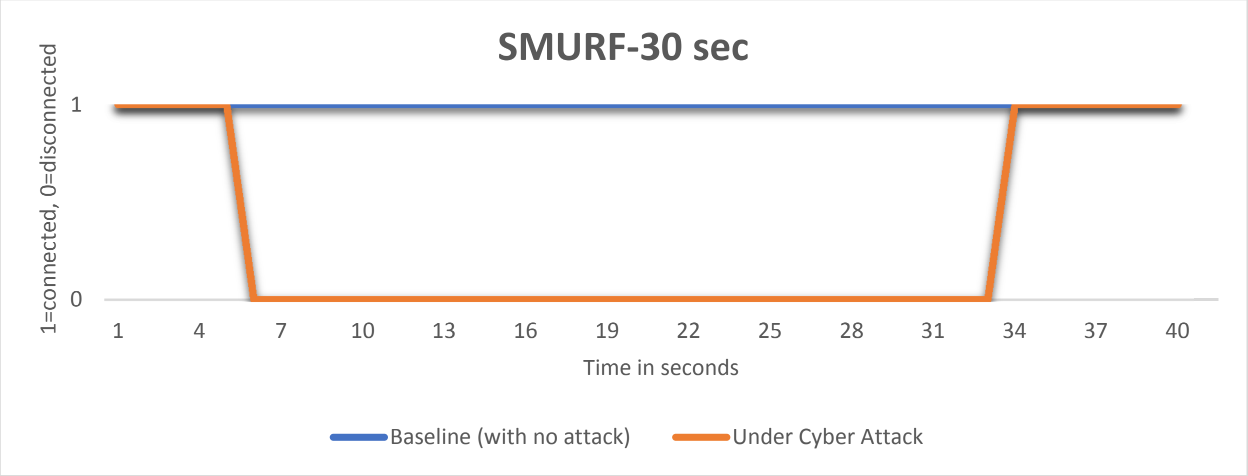


Figure 5.23: Observation under smurf attack for 30 seconds

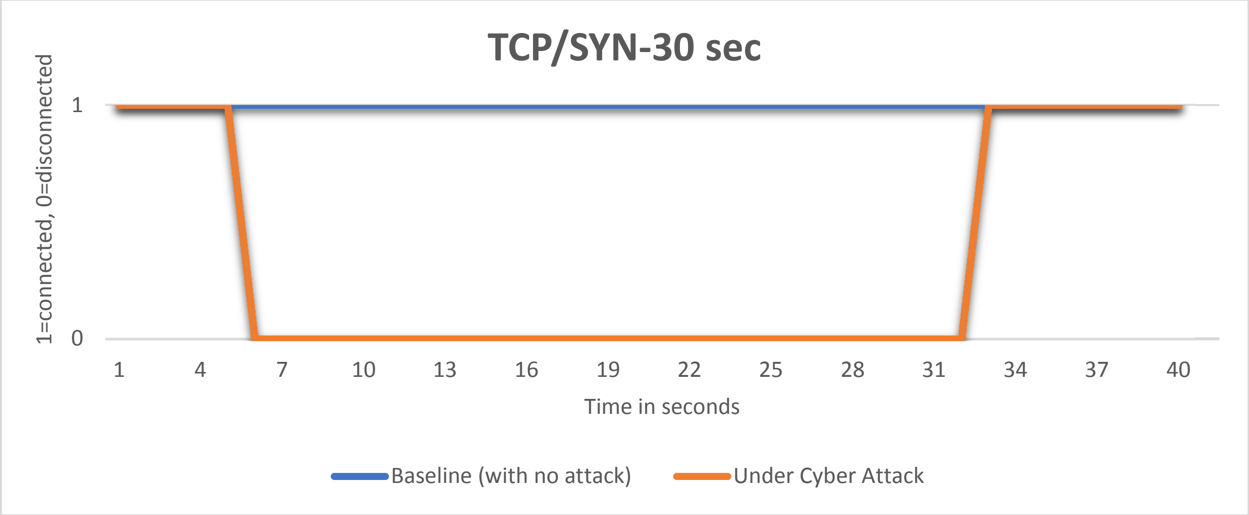


Figure 5.24: Observation under TCP/SYN attack for 30 seconds

5.3.2 Experiment Results Under PING, SMURF and TCP/SYN Attack for 60 seconds:

To check on the trend of attack duration and disconnection time and recovery time under attack we increased the attack duration to 60 seconds. We observed that time to break the communication under all kinds of attack was same and was 5 seconds which was almost immediate but the recovery time under all attacks was different and was 3 seconds in case of ping attack, 5 seconds in case of smurf attack and 3 seconds in case of TCP/SYN attack shown in (Figure 5.25, 5.26 and 5.27) respectively.

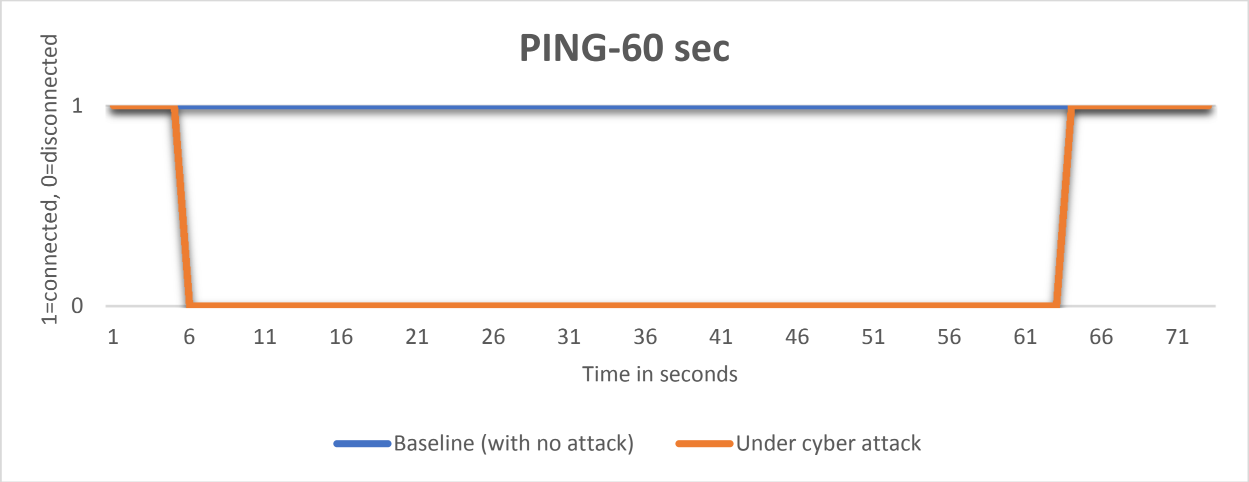


Figure 5.25: Observation under ping attack for 60 seconds

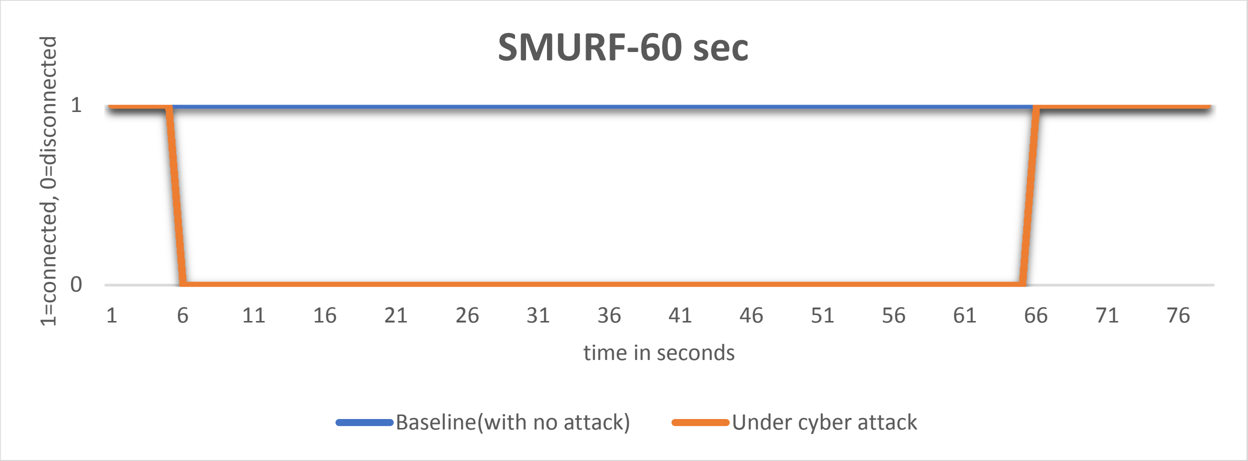


Figure 5.26: Observation under smurf attack for 60 seconds

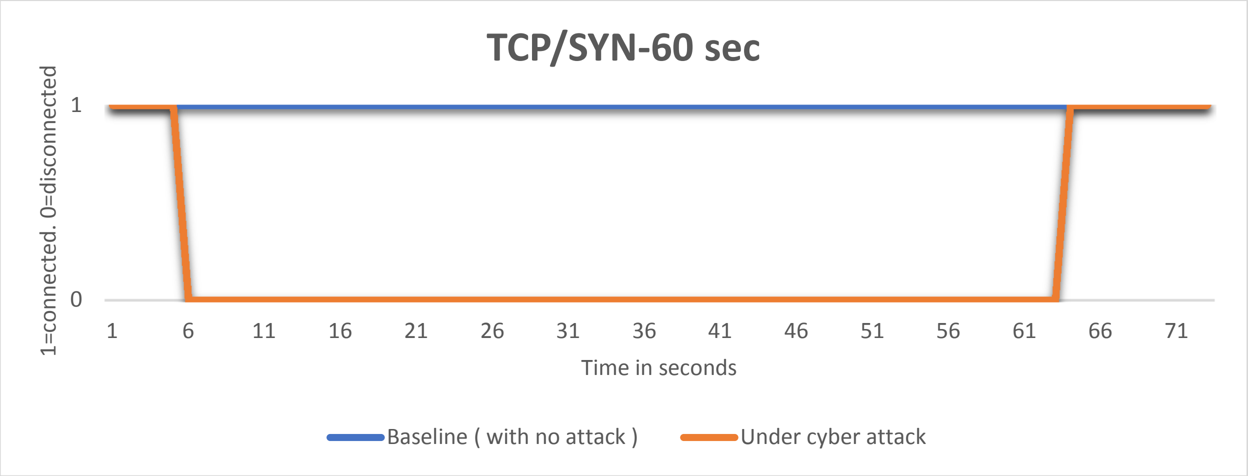


Figure 5.27: Observation under TCP/SYN attack for 60 seconds

5.3.3 Experiment Results Under PING, SMURF and TCP/SYN Attack for 120 seconds

To check on the trend of disconnection time and recovery time under attack, we increased the attack duration to 120 seconds. We observed that time to disconnection time under all kinds of attack was same and was 5 seconds which was almost immediate but the recovery time under all attacks was different and was 3 seconds in case of ping attack, 5 seconds in case of smurf attack and 3 seconds in case of TCP/SYN attack shown in (Figure 5.28, 5.29 and 5.30) respectively.

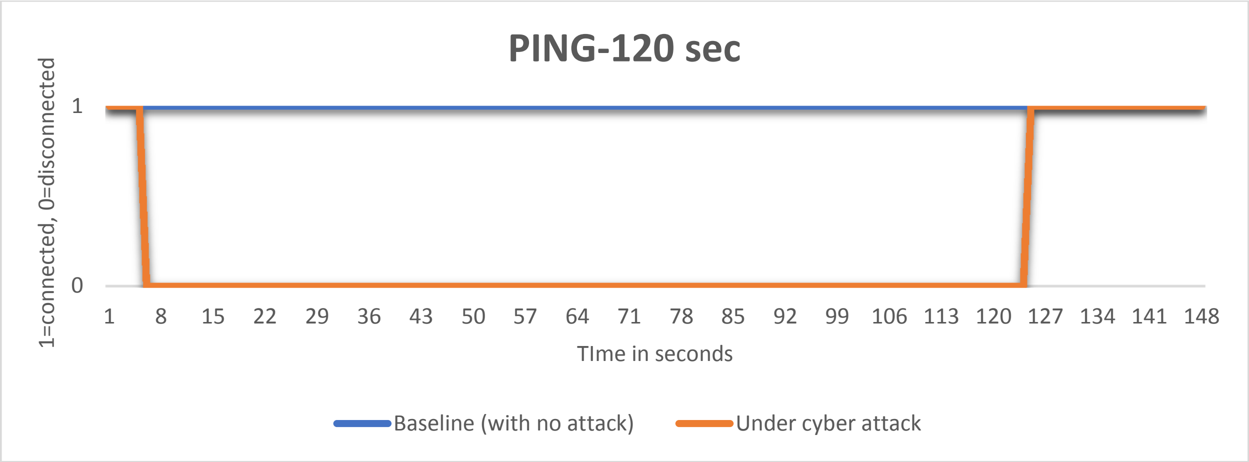


Figure 5.28: Observation under ping attack for 120 seconds

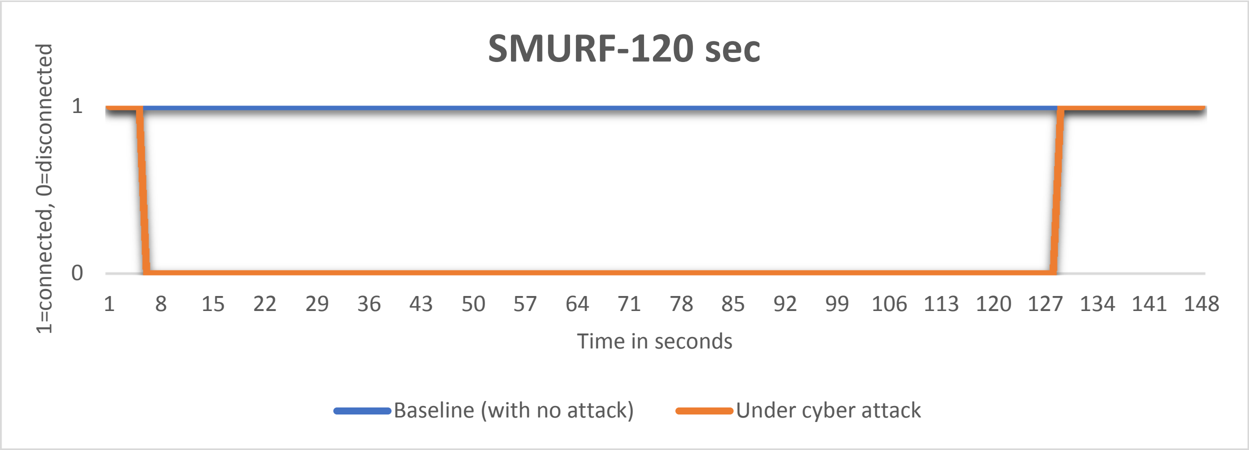


Figure 5.29: Observation under smurf attack for 120 seconds

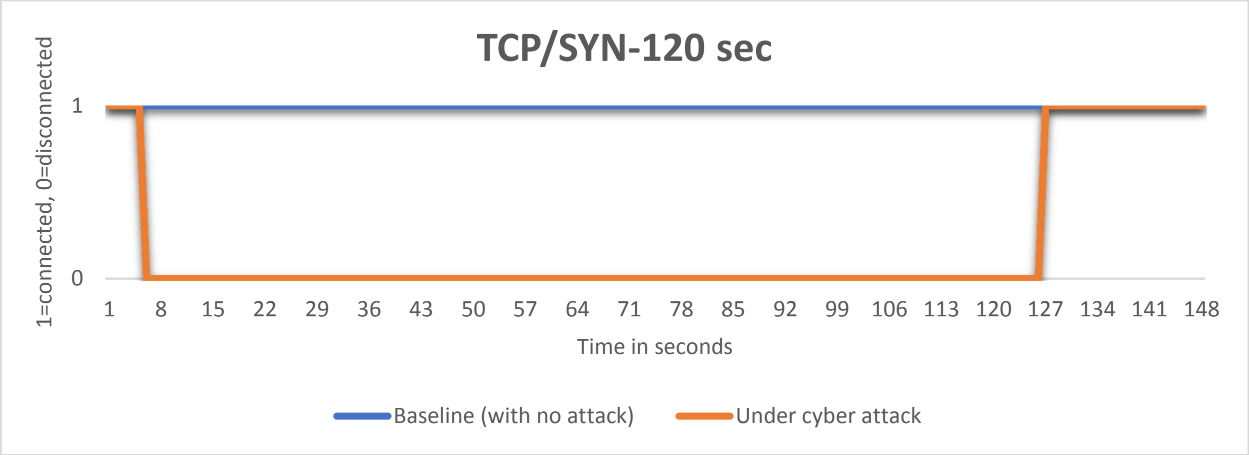


Figure 5.30: Observation under TCP/SYN attack for 120 seconds

5.3.4 Experiment Results Under PING, SMURF and TCP/SYN Attack for 300 seconds

To check on the trend of disconnection time and recovery time under attack we increased the attack duration to 300 seconds. We observed that time to disconnection time under all kinds of attack was same and was 5 seconds which was almost immediate but the recovery time under all attacks was different and was 4 seconds in case of ping attack, 8 seconds in case of smurf attack and 6 seconds in case of TCP/SYN attack shown in (Figure 5.31, 5.32and 5.33) respectively.

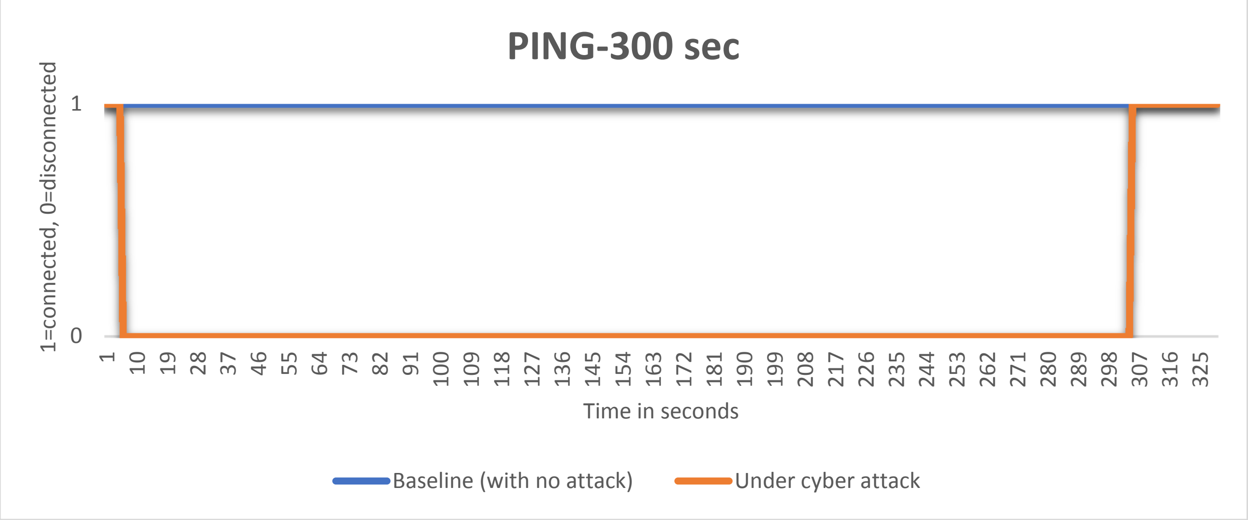


Figure 5.31: Observation under Ping attack for 300 seconds

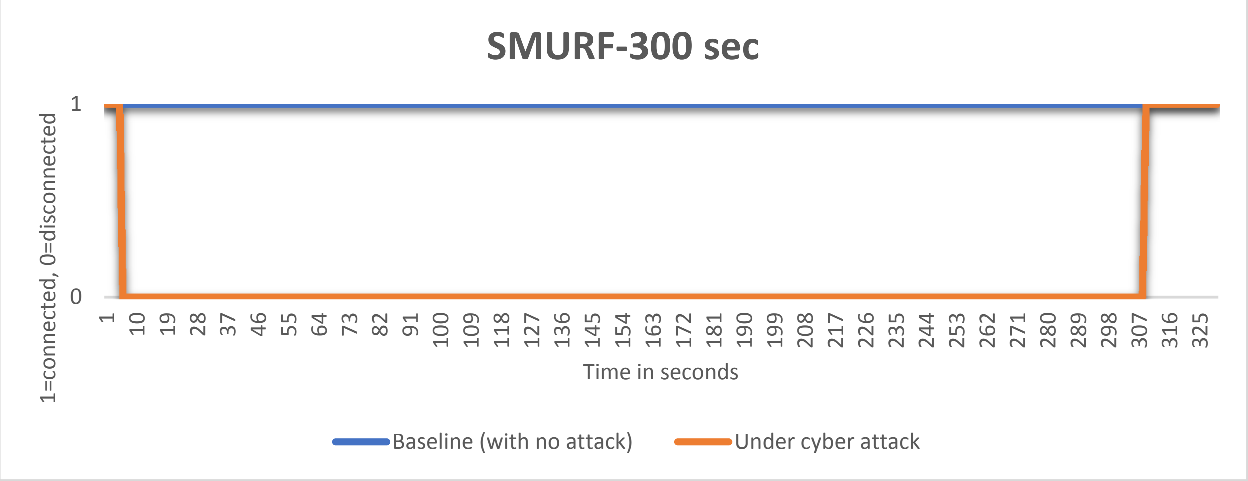


Figure 5.32: Observation under smurf attack for 300 seconds

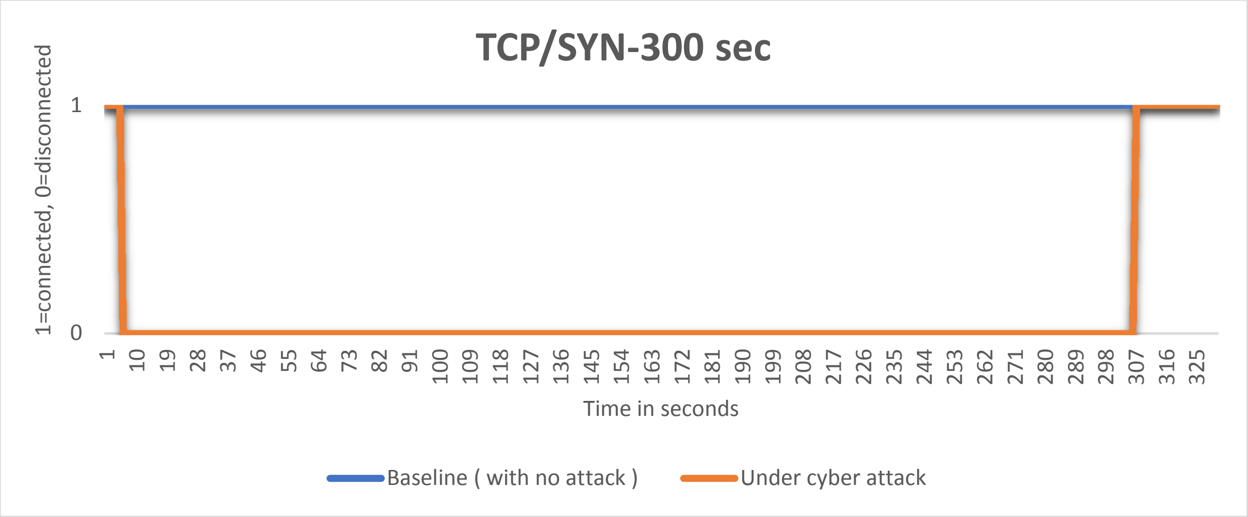


Fig 5.33 Observation under TCP/SYN attack for 300 seconds

5.3.5 Experiment Results Under PING, SMURF and TCP/SYN Attack for 600 seconds

To check on the trend of disconnection time and recovery time under attack we increased the attack duration to 600 seconds. We observed that time to disconnection time under all kinds of attack was same and was 5 seconds which was almost immediate but the recovery time under all attacks was different and was 7 seconds in case of ping attack, 12 seconds in case of smurf attack and 9 seconds in case of TCP/SYN attack shown in (Figure 5.34, 5.35and 5.36) respectively.

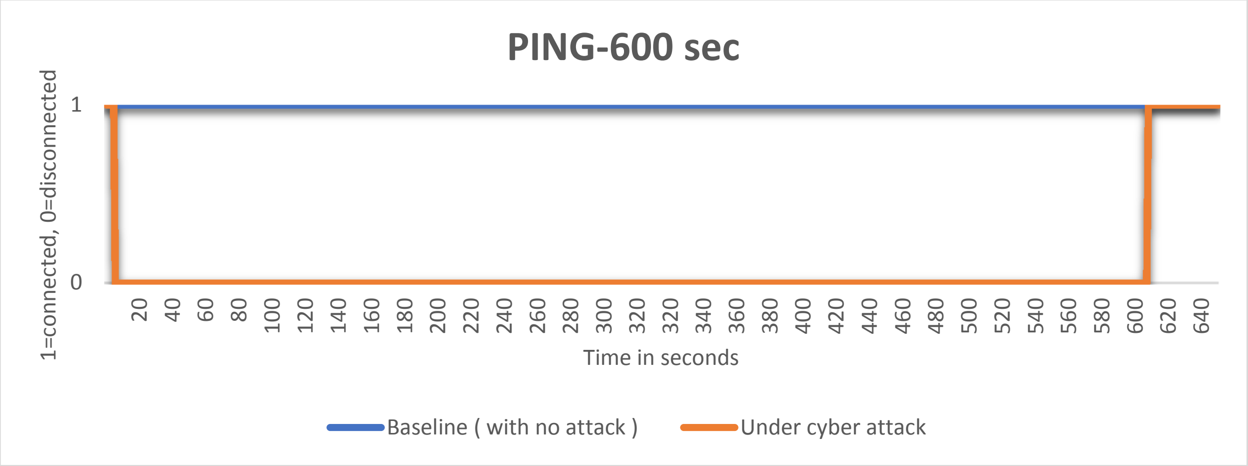


Figure 5.34: Observation under ping attack for 600 seconds

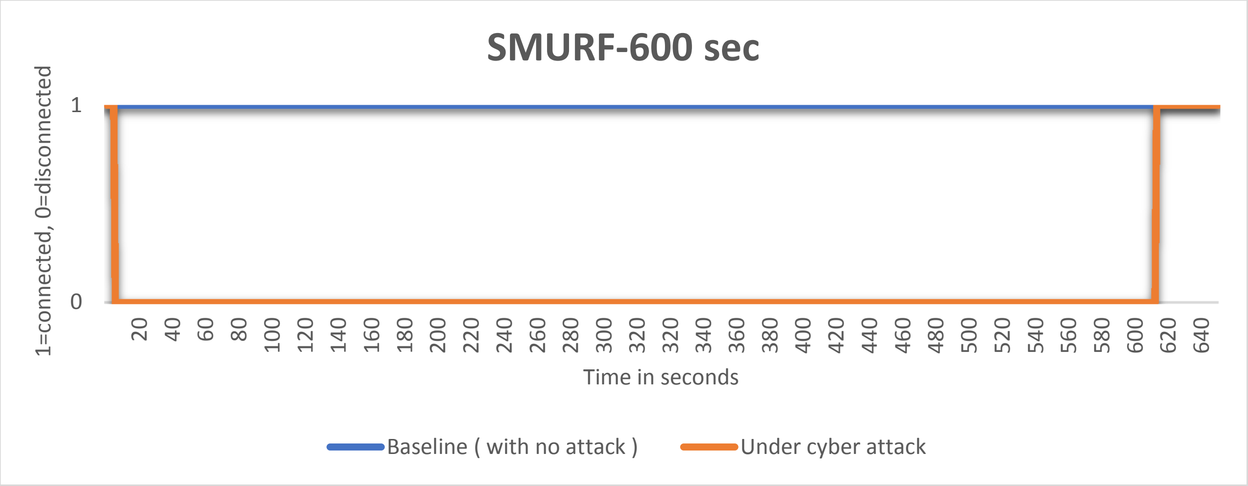


Figure 5.35: Observation under smurf attack for 600 seconds

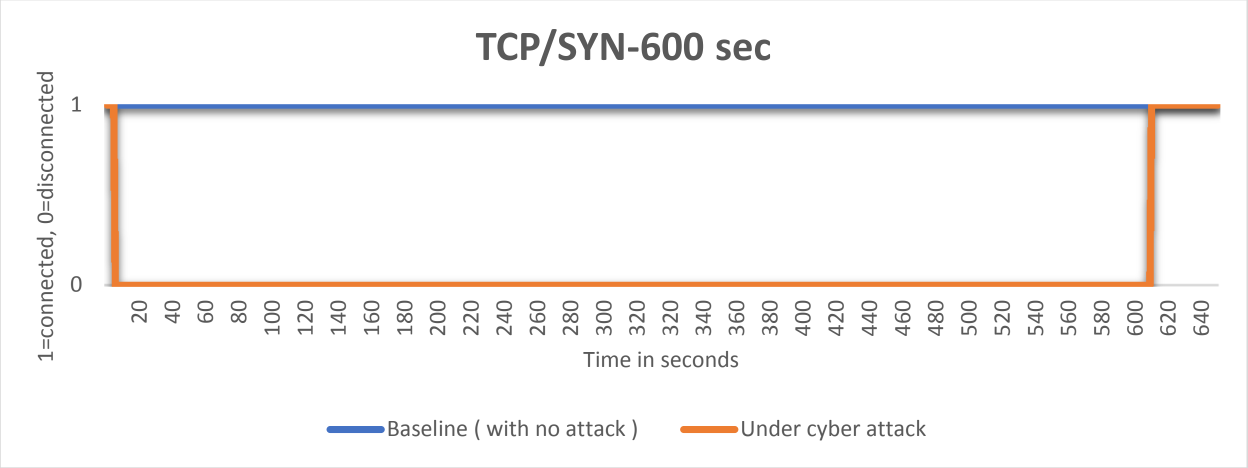


Figure 5.36: Observation under TCP/SYN attack for 600 seconds

5.3.6 Experiment Results Under PING, SMURF and TCP/SYN Attack for 1200 seconds

To check on the trend of disconnection time and recovery time under attack, we increased the attack duration to 1200 seconds. We observed that time to disconnection time under all kinds of attack was same and was 5 seconds which was almost immediate but the recovery time under all attacks was different and was 7 seconds in case of ping attack, 12 seconds in case of smurf attack and 9 seconds in case of TCP/SYN attack shown in (Figure 5.37, 5.38 and 5.39) respectively.

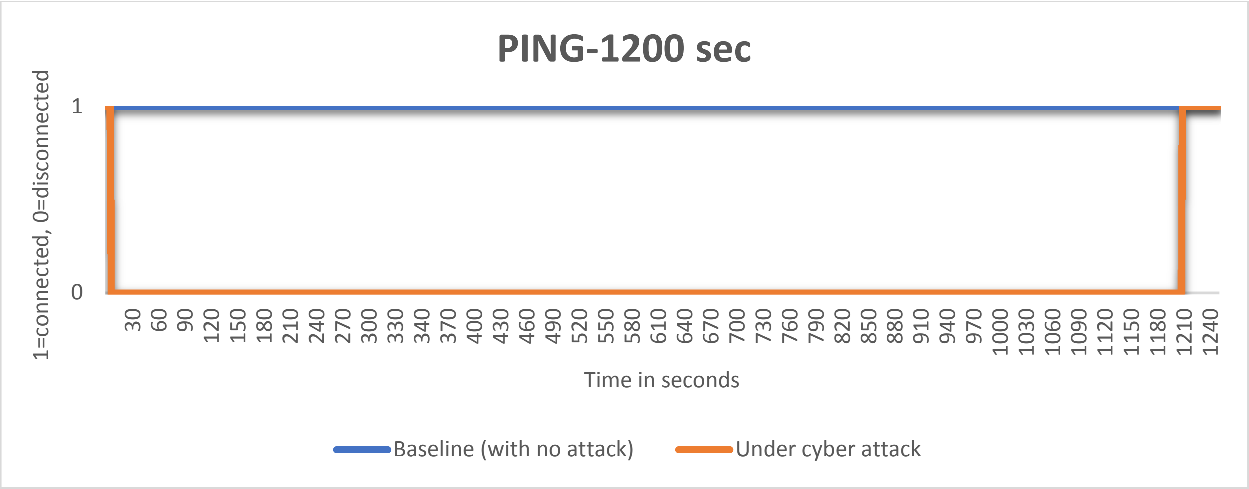


Figure 5.37: Observation under ping attack for 1200 seconds

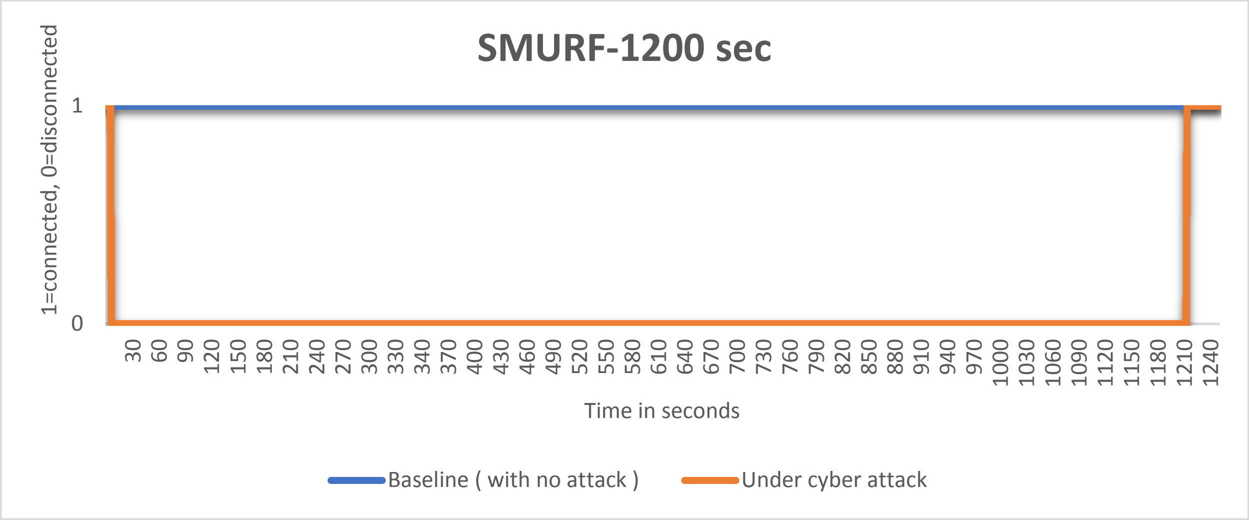


Figure 5.38: Observation under smurf attack for 1200 seconds

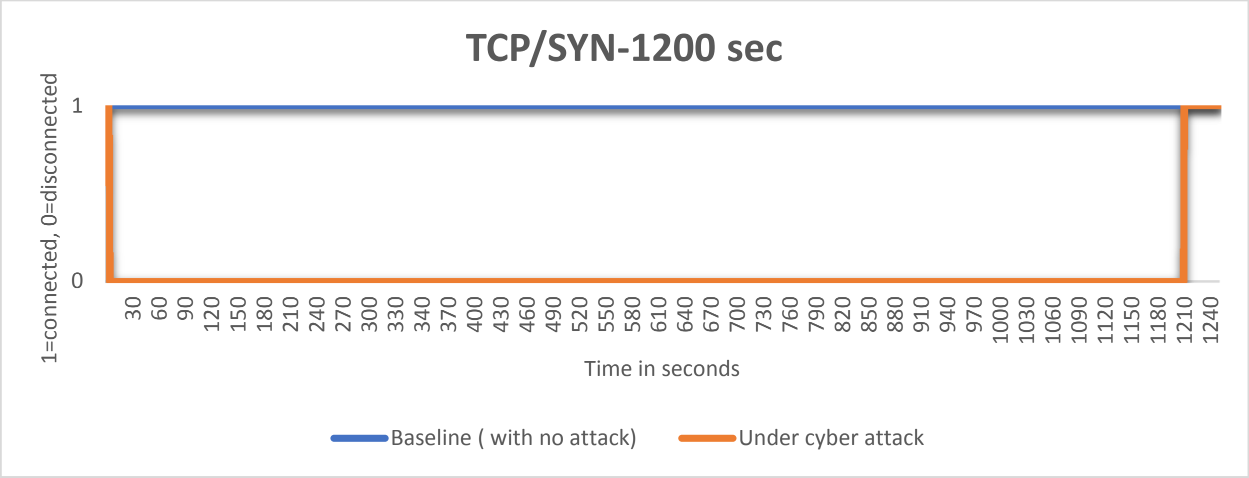


Figure 5.39: Observation under TCP/SYN attack for 1200 seconds

5.4 Chapter Summary

This chapter shows that the data communication performance of two smart meters from General Electric i.e. EPM 6100 and EPM 7000, when exposed to different cyber-attack. The disconnection time under different cyber-attack was identical whereas the recovery time was different under different attack and displays a positive trend with increase in attack duration but after certain increase in attack duration there was not much increase in recovery time after attack was removed and it seems stagnant with whatever attack duration is. Smurf attack has maximum effect out of all the attack used. EPM 7000 smart meters shows better performance and quick recovery as compared to EPM 6100 meter because EPM 7000 meter comes with 1.8 GHz process and 10 Mbytes of memory as compared to 1.2 Ghz and 100 Kbytes of memory for EPM 6100 meter.

CHAPTER VI

COMPARISION OF SECURITY INTEGRITY OF DATA COLLECTION UNDER AND EVALUATION OF SMART METERING DATA COMMUNICATION FROM EPM 6100 AND 7000 POWER QUALITY SMART ELECTRIC METER UNDER DIFFERENT CYBER ATTACKS

As observed cyber Security Attack influences security and integrity of data collection from smart electric meter. In this chapter, I compared security integrity of data collection from EPM 6100 and EPM 7000 power quality smart electric meter under cyber-attack and performance of smart metering communication of EPM 6100 and 7000 smart power quality meter.

6.1 Experimental Setup for evaluating security integrity of data collection from EPM 6100 and EPM 7000 power quality smart electric meter under direct and indirect cyber-attack

Initially, the EPM 6100 smart meter was evaluated for its security integrity of its data collection under indirect cyber-attack starting with evaluating it for 4 days followed by 7 days and 15 days reaching up to 30 days i.e. a typical customer billing cycle. Following that then meter was experimented separately under direct attack and for that meter was under no attack on day 1, under direct attack day 2 and under no attack on day 3. This was done to observe the possible trend and effect of cyber-attack on the smart electric meter.

Cyber-attack traffic is sent to the communication network through which smart meter was transmitting the usage data to the remote monitoring computer. Before that baseline for the data usage was created without attack which was acting as a reference for comparison of possible effect and deviation. The same evaluation process was conducted for the EPM 7000 meter and at the end all results were compared separately. The condition for each experiment along with parameters like attack intensity load, environment condition etc. used were kept same. Out of all well-known DDoS cyber-attacks, ping attack with lower intensity was used for the experiments. The experimental set ups for EPM 6100 and EPM 7000 smart meter were shown in (Figure 6.1 and Figure 6.2) respectively.

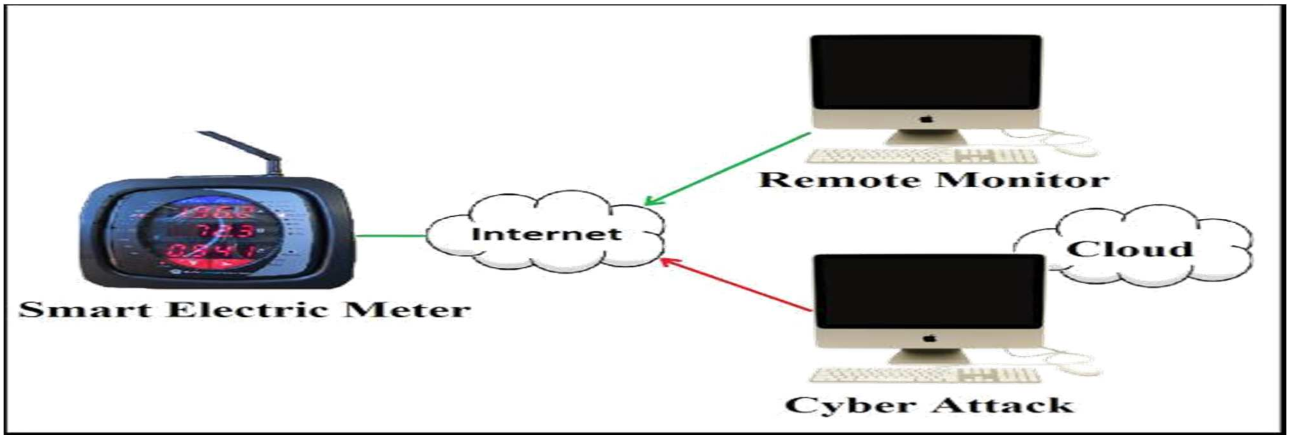


Figure 6.1: Experimental Setup for EPM 6100 power quality meter

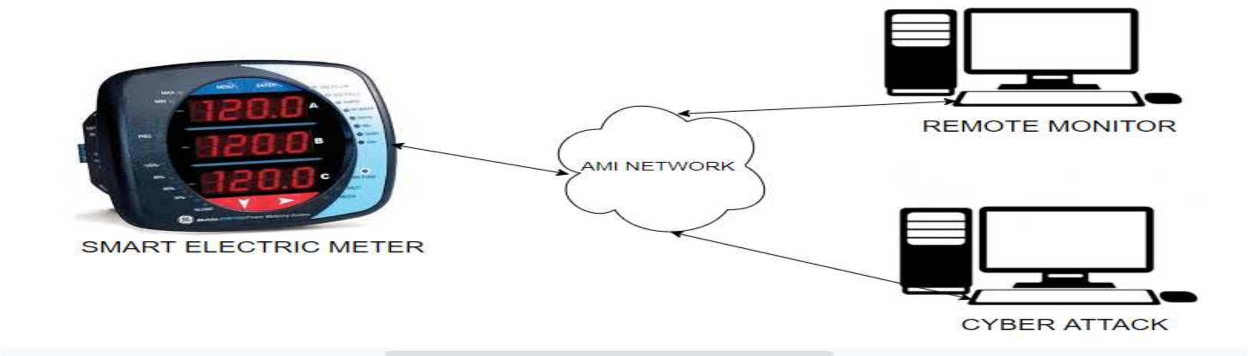


Figure 6.2: Experimental Setup for EPM 7000 power quality meter

6.2 Comparison of Results from Security Integrity of Data Collection from EPM 6100 and EPM 7000 Power Quality Smart Electric Meter Under Direct and Indirect Cyber-Attack

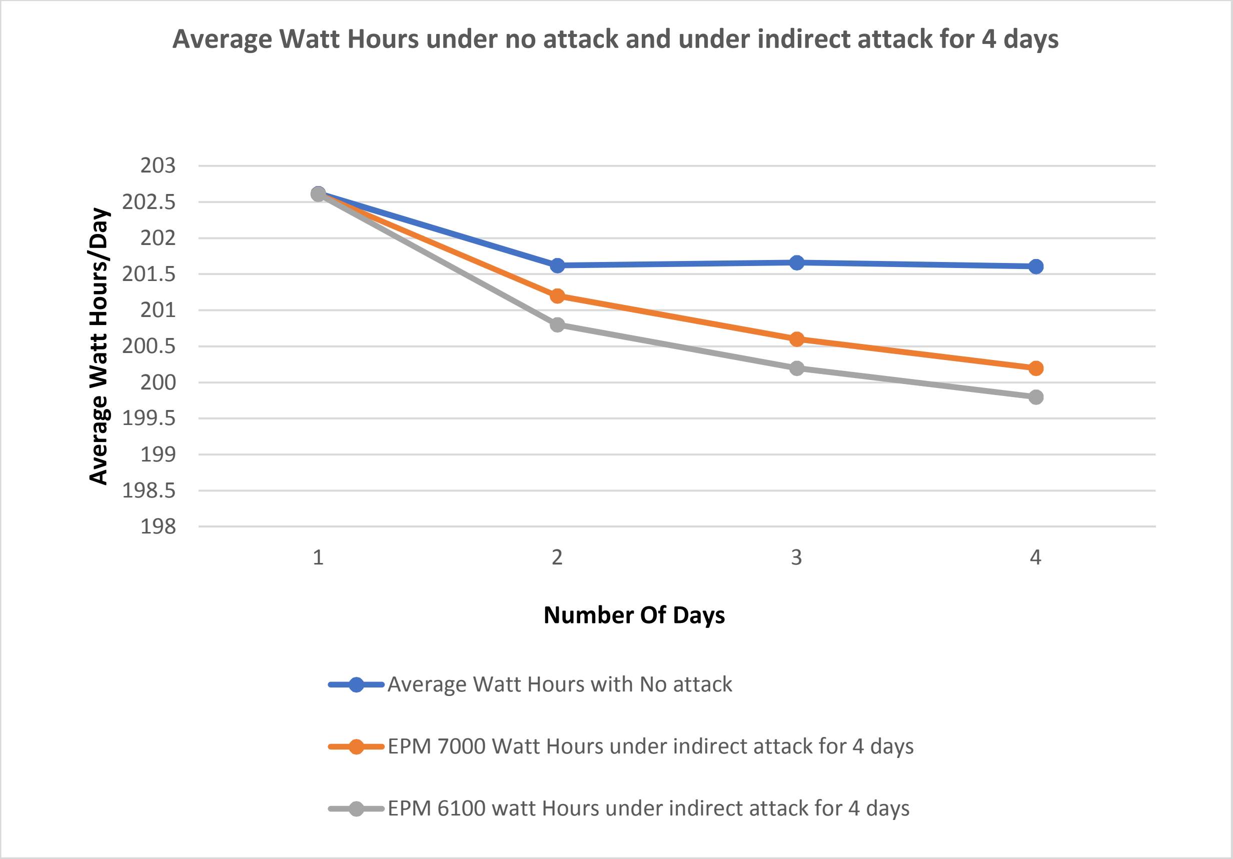


Figure 6.3: Average Power Consumption measured in Average Watt hour for Experiment I without cyber-attack (baseline shown in blue) and with indirect cyber-attack (shown in orange for EPM 7000 and shown in grey for EPM 6100)

As we can observe from (Figure 6.3) indirect cyber-attack or traffic has its effect on security integrity of data collection for both EPM 7000 and 6100 smart meter. The % deviation from the baseline can be observed to be increasing very day. At the end of day 4 EPM 7000 has the deviation of 0.29% whereas EPM 6100 has the deviation of 0.32% from the baseline watt hours. The % deviation in case of both the meters is not have significant difference.

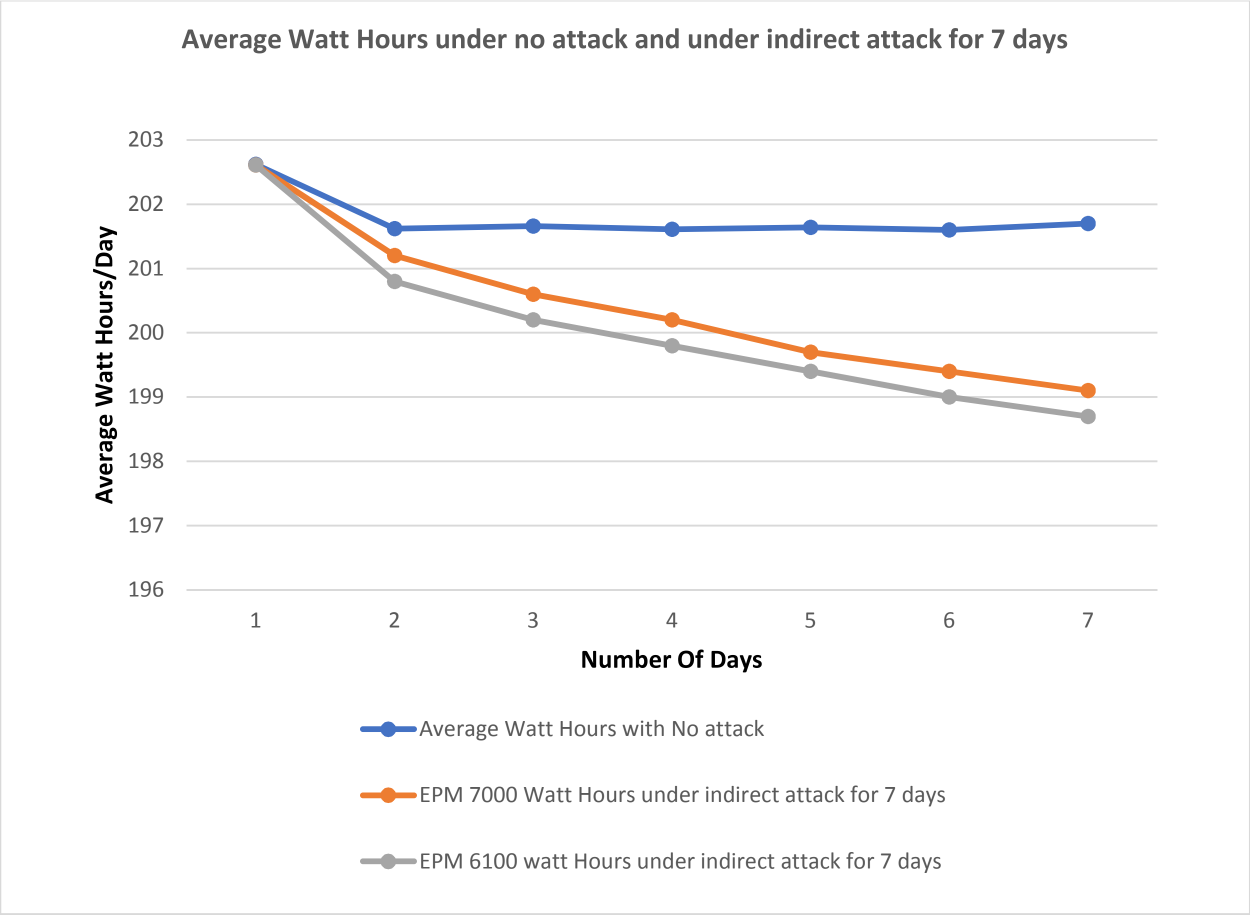


Figure 6.4: Average Power Consumption measured in Average Watt hour for Experiment II without cyber-attack (baseline shown in blue) and with indirect cyber-attack (shown in orange for EPM 7000 and shown in grey for EPM 6100)

As we can observe from (Figure 6.4) indirect cyber-attack or traffic has its effect on security integrity of data collection for both EPM 7000 and 6100 smart meter. The % deviation from the baseline can be observed to be increasing very day. At the end of day 7 EPM 7000 has the deviation of 0.79% whereas EPM 6100 has the deviation of 0.92% from the baseline watt hours. The % deviation in case of both the meters is not have significant difference.

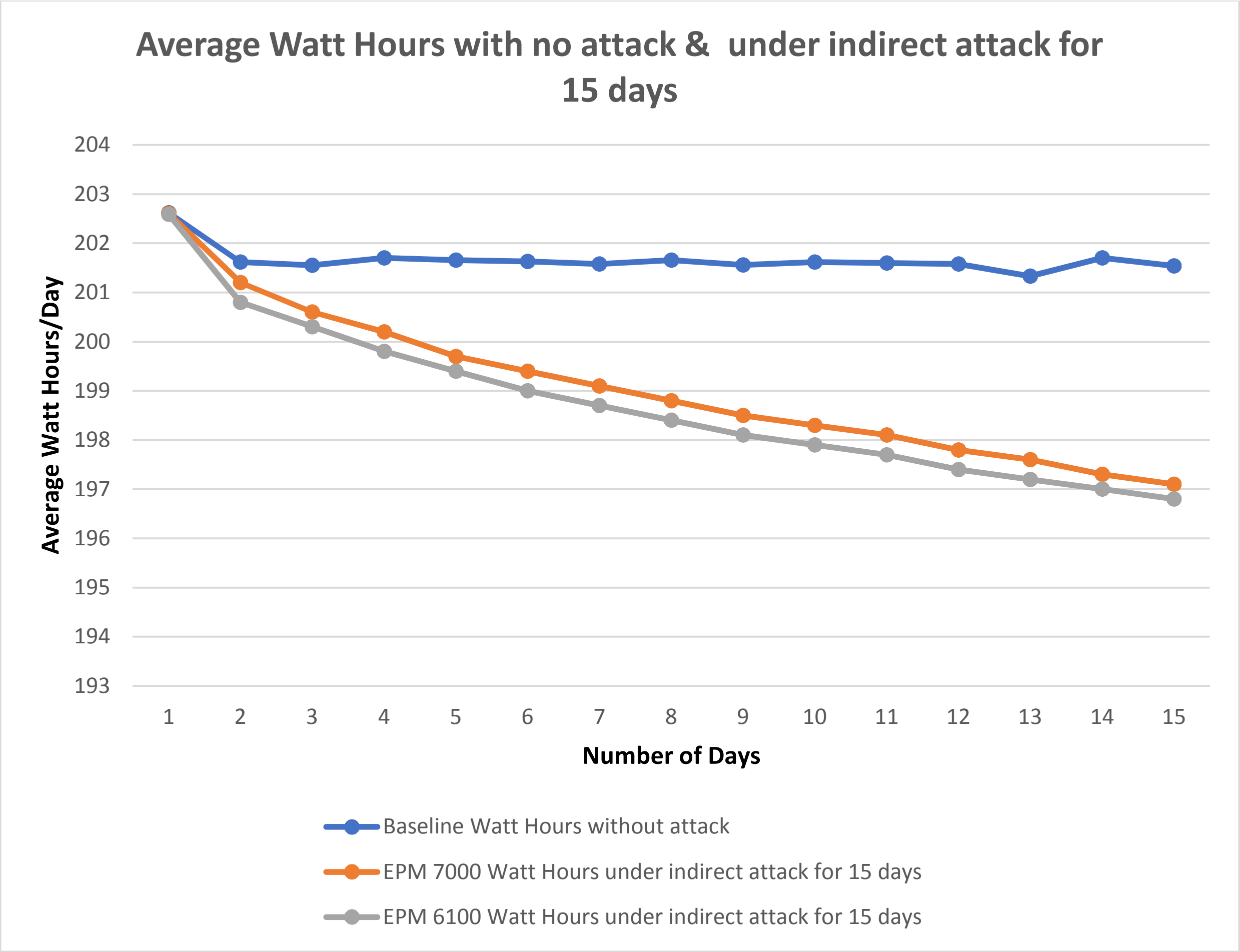


Figure 6.5: Average Power Consumption measured in Average Watt hour for Experiment III without cyber-attack (baseline shown in blue) and with indirect cyber-attack (shown in orange for EPM 7000 and shown in grey for EPM 6100)

As we can observe from (Figure 6.5) indirect cyber-attack or traffic has its effect on security integrity of data collection for both EPM 7000 and 6100 smart meter. The % deviation from the baseline can be observed to be increasing very day. At the end of day 15 EPM 7000 has the deviation of 2.16 % whereas EPM 6100 has the deviation of 2.28% from the baseline watt hours. The % deviation in case of both the meters is not have significant difference.

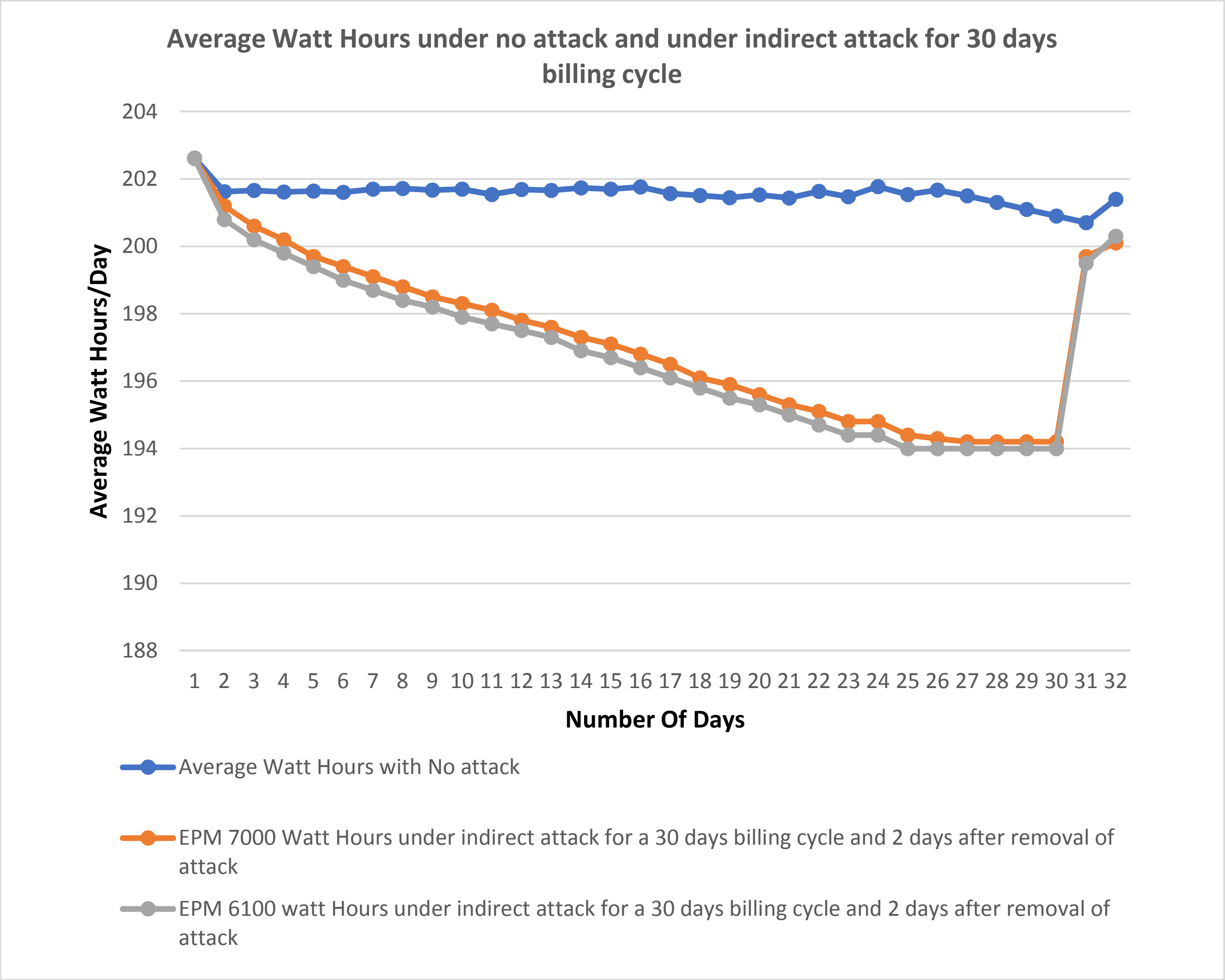


Figure 6.6: Average Power Consumption measured in Average Watt hour for Experiment-IV without cyber-attack (baseline shown in blue) and with indirect cyber-attack (shown in orange for EPM 7000 and shown in grey for EPM 6100)

As we can observe from (Figure 6.6) indirect cyber-attack or traffic has its effect on security integrity of data collection for both EPM 7000 and 6100 smart meter. The % deviation from the baseline can be observed to be increasing very day. At the end of day 30 EPM 7000 has the deviation of 3.72% which was almost identical as the EPM 6100 meter from the baseline watt hours. The was not significant % difference in watt hours recorded under cyber-attacks for both the meters.

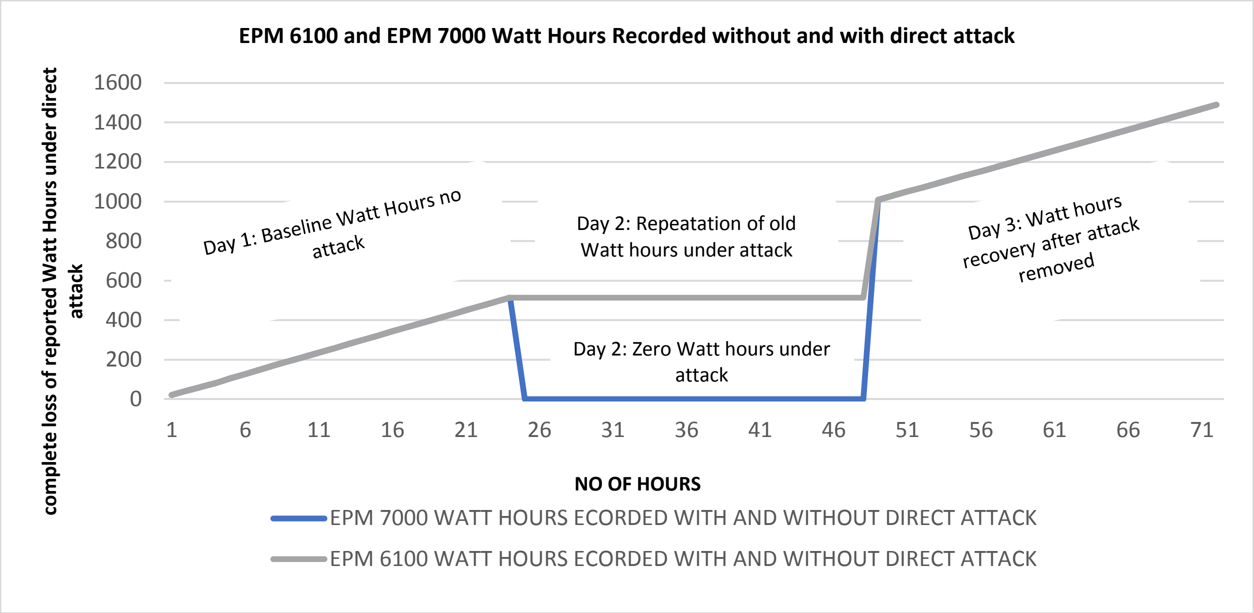


Figure 6.7: Data communication to remote monitoring computer from smart meter under direct attack

As we can observe from (Figure 6.7) direct cyber-attack or traffic has its effect on security integrity of data collection for both EPM 7000 and 6100 smart meter. Under direct cyber-attack EPM 6100 seems totally lost its connectivity and was not able to record the usage data and keeps repeating the same values which it recorded before the attack has started whereas in case of EPM 7000, it seems totally lost it communication and was unable to record the usage data but recorded zero watt hours during the attack period.

6.3 Experimental Set Up for Performance Evaluation of Smart Metering Data Communication of EPM 6100 and 7000 Power Quality Smart Electric Meter Under Different Cyber-Attacks

Initially, the EPM 6100 smart meter was evaluated for its communication under different cyber-attacks i.e. ping attack, smurf attack and TCP/SYN respectively separately for the time duration starting from 30 seconds up to 1200 seconds. This was done to observe the possible trend and effect cyber-attack has on the smart metering communication performance and how it behaves during different cyber-attack in terms of disconnection time during attack and recovery time when attack was removed. Cyber traffic or attack is sent to the communication network through which smart meter was transmitting the usage data to the remote monitoring computer. In this experiment, baseline acting as a reference for comparison of possible effect and deviation is always fixed and known as if meter is connected to the network and communication data usage without any interruption the software will record 1 and if it's not in action then it records 0. The same evaluation process was conducted for the EPM 7000 meter and at the end all results were compared separately. The condition for each experiment along with parameters like load, environment condition etc. used were kept same but the attack intensity was different because we already observed in last chapter that it requires 6% attack bandwidth i.e. 3.8Mbps for EPM 6100 power quality smart meter and 10% attack bandwidth i.e.7.6 Mbps for EPM 7000 power quality meter to break the communication. The experimental set ups for EPM 6100 and EPM 7000 smart meter were shown in (Figure 6.8 and Figure 6.9) respectively.

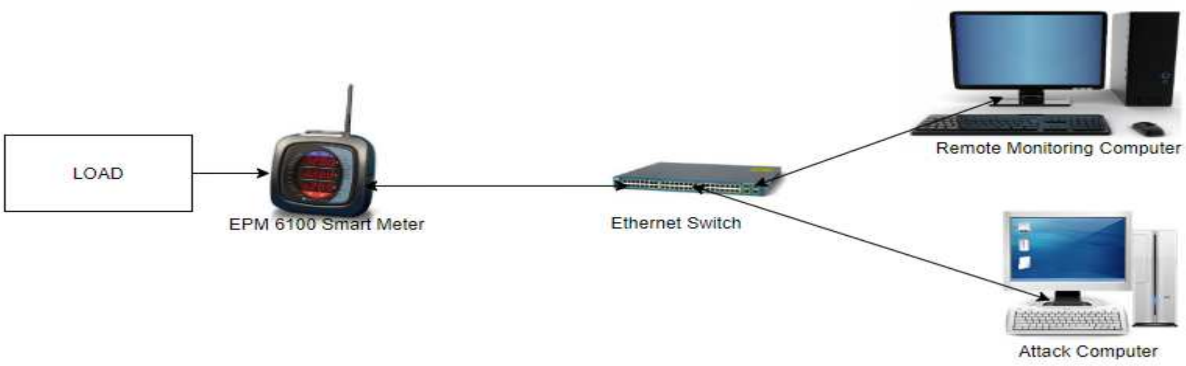


Figure 6.8: Experimental set up for evaluating EPM 6100 smart meter data communication performance under cyber-attack

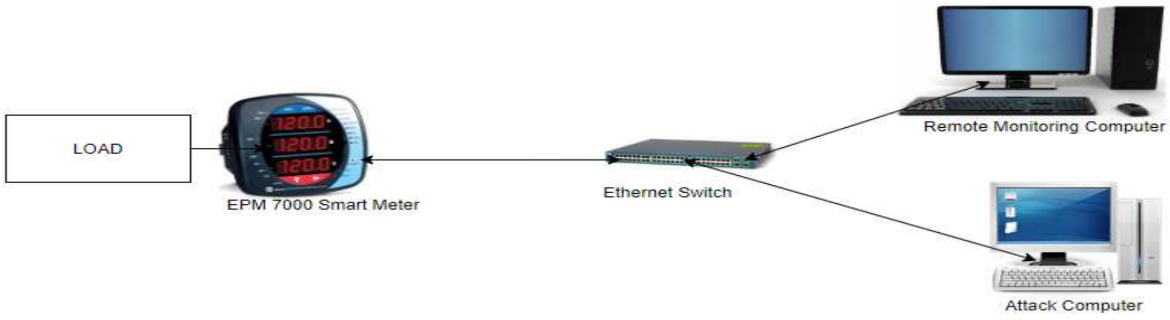


Figure 6.9: Experimental set up for evaluating EPM 7000 smart meter data communication performance under cyber-attack

6.4 Comparison of results for Performance Evaluation of Smart Metering Data Communication of EPM 6100 and 7000 Power Quality Smart Electric Meter Under Different Cyber-Attacks

As we can observe that different cyber-attacks have different effect on the performance of smart metering data communication and is different also for both the meters under different cyber-attacks in terms of time to break the communication and time to recovery after the attack was removed. Time to break the communication under all kinds of attack used was 3 seconds for EPM 6100 and was 5 seconds for EPM 7000 respectively which was almost immediate.

The duration of all attack used was 30 seconds in this case sent to both the meters through their data communication channel. Initially the meter could communicate the data without having any attack and then attack was introduced while it was communicating. Then attack was removed to allow meters to recover in order to evaluate their data communication performance. The recovery time under all attacks were different and was 4 seconds in case of ping attack for EPM 6100 whereas 2 seconds for EPM 7100, 7 seconds in case of smurf attack for EPM 6100 whereas 3 seconds for EPM 7100and 6 seconds in case of TCP/SYN attack for EPM 6100 whereas 2 seconds for EPM 7100 shown in (Figure 6.10, 6.11 and 6.12) respectively.

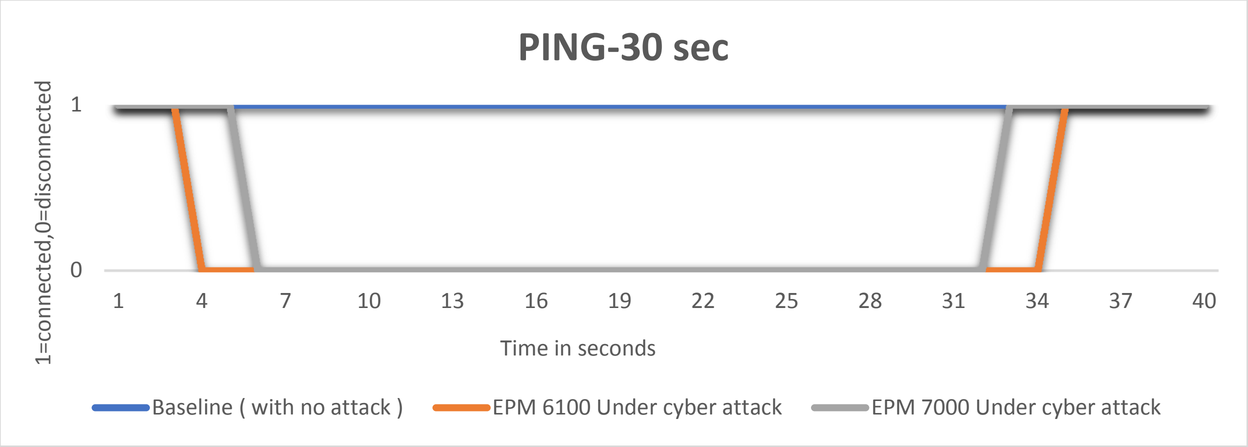


Figure 6.10: Observation under ping attack for 30 seconds

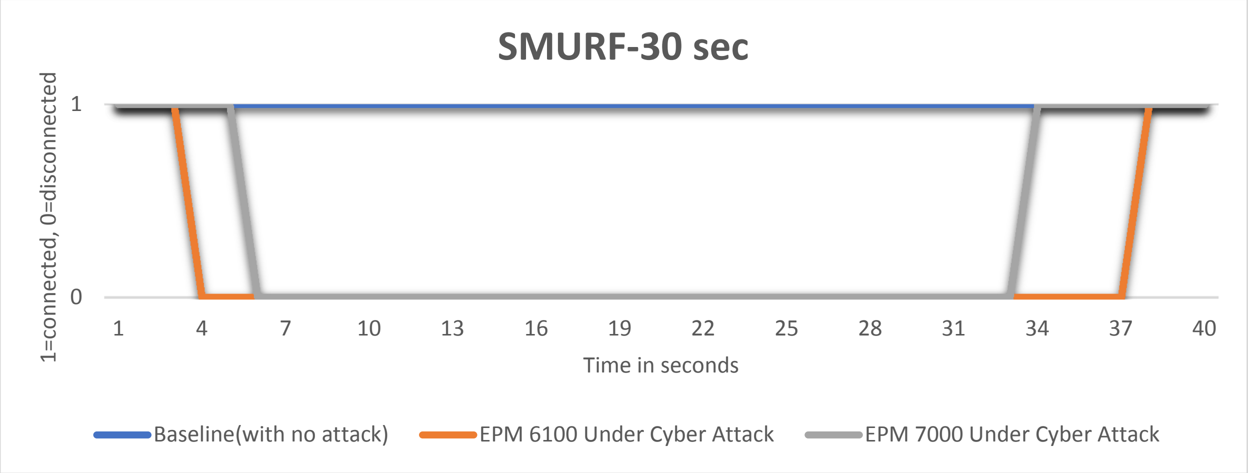


Figure 6.11: Observation under smurf attack for 30 seconds

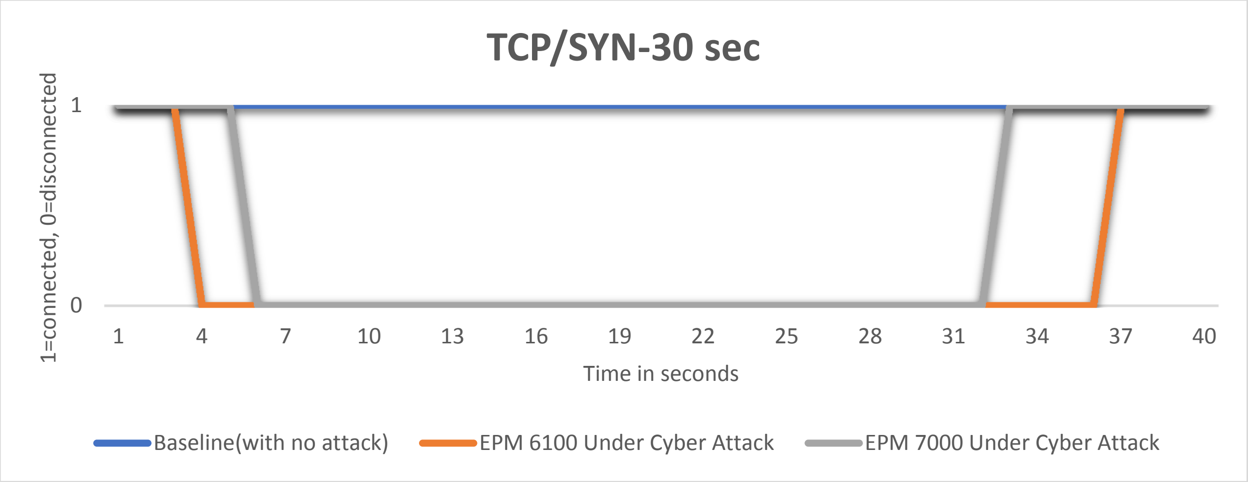


Figure 6.12: Observation under TCP/SYN attack for 30 seconds

To check on the trend, we experimented further with both meters by increasing the attack duration. In this case also disconnection time under all kinds of attack used was 3 seconds for EPM 6100 and was 5 seconds for EPM 7000 respectively which was almost immediate. The duration of all attack used was 60 seconds in this case sent to both the meters through their data communication channel. Initially the meter could communicate the data without having any attack and then attack was introduced while it was communicating. Then attack was removed to allow meters to recover in order to evaluate their data communication performance. The recovery time under all attacks were different and was 7 seconds in case of ping attack for EPM 6100 whereas 3 seconds for EPM 7100, 14 seconds in case of smurf attack for EPM 6100 whereas 5 seconds for EPM 7100 and 10 seconds in case of TCP/SYN attack for EPM 6100 whereas 3 seconds for EPM 7100 shown in (Figure 6.13, 6.14 and 6.15) respectively.

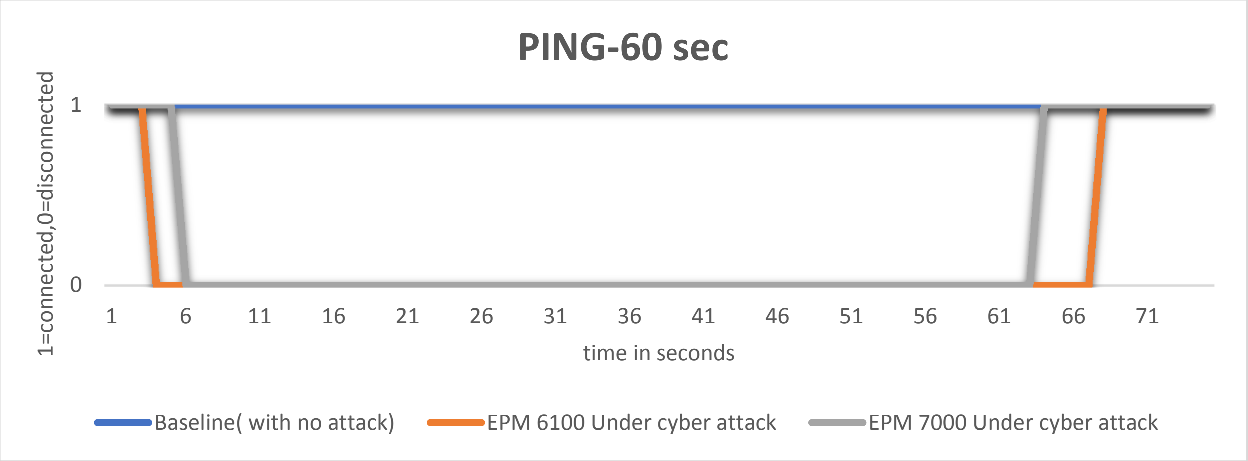


Figure 6.13: Observation under ping attack for 60 seconds

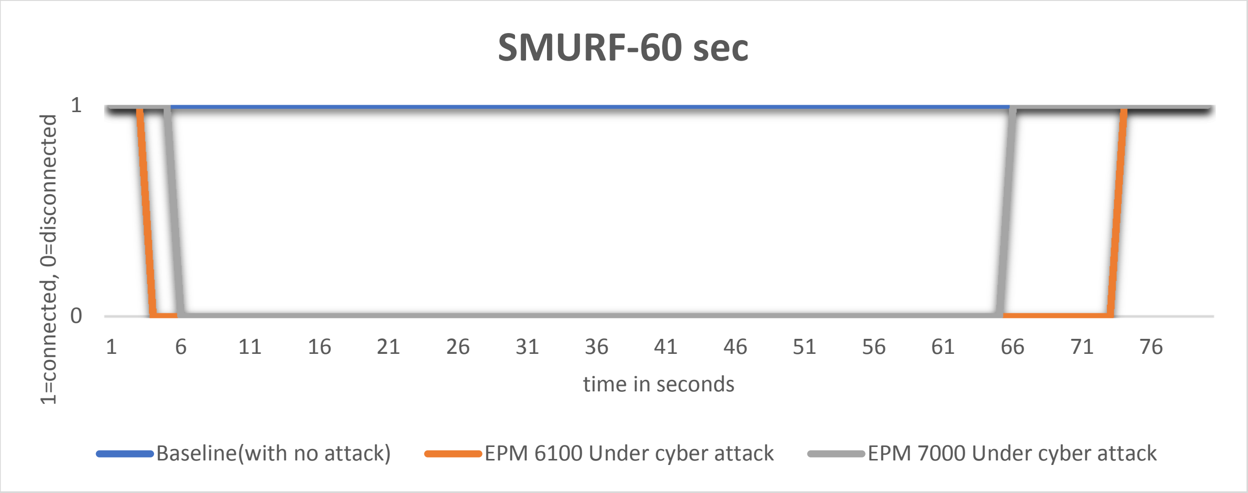


Figure 6.14: Observation under smurf attack for 60 seconds

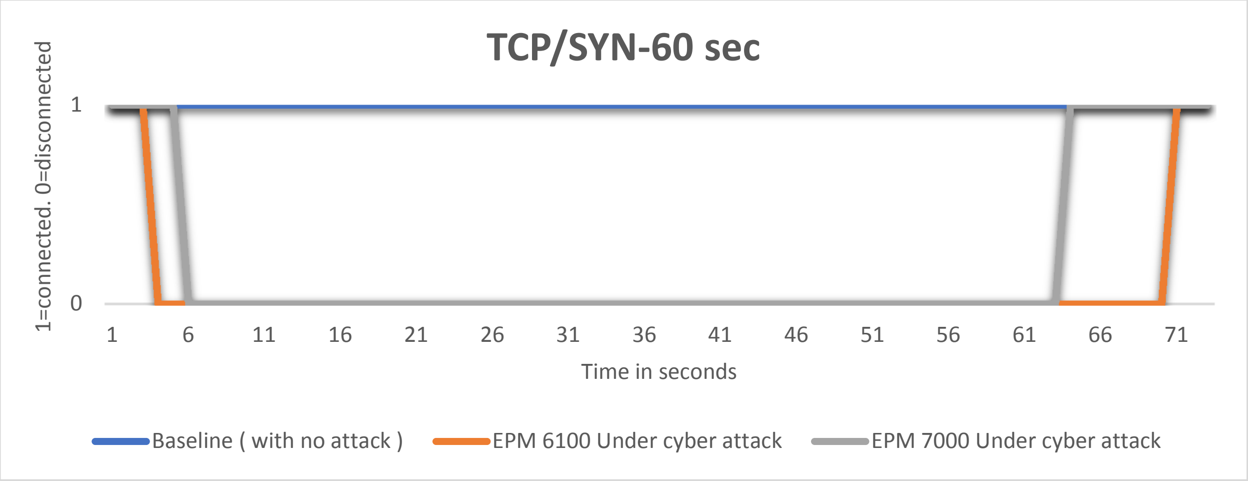


Figure 6.15: Observation under TCP/SYN attack for 60 seconds

To check on the trend, we experimented with both meters further with increasing the attack duration. In this case also time to break the communication under all kinds of attack used was 3 seconds for EPM 6100 and was 5 seconds for EPM 7000 respectively which was almost immediate. The duration of all attack used was 120 seconds in this case sent to both the meters through their data communication channel.

Initially the meter could communicate the data without having any attack and then attack was introduced while it was communicating. Then attack was removed to allow meters to recover in order to evaluate their data communication performance. The recovery time under all attacks were different and was 10 seconds in case of ping attack for EPM 6100 whereas 4 seconds for EPM 7100, 19 seconds in case of smurf attack for EPM 6100 whereas 8 seconds for EPM 7100and 14 seconds in case of TCP/SYN attack for EPM 6100 whereas 6 seconds for EPM 7100 shown in (Figure 6.16, 6.17 and 6.18) respectively.

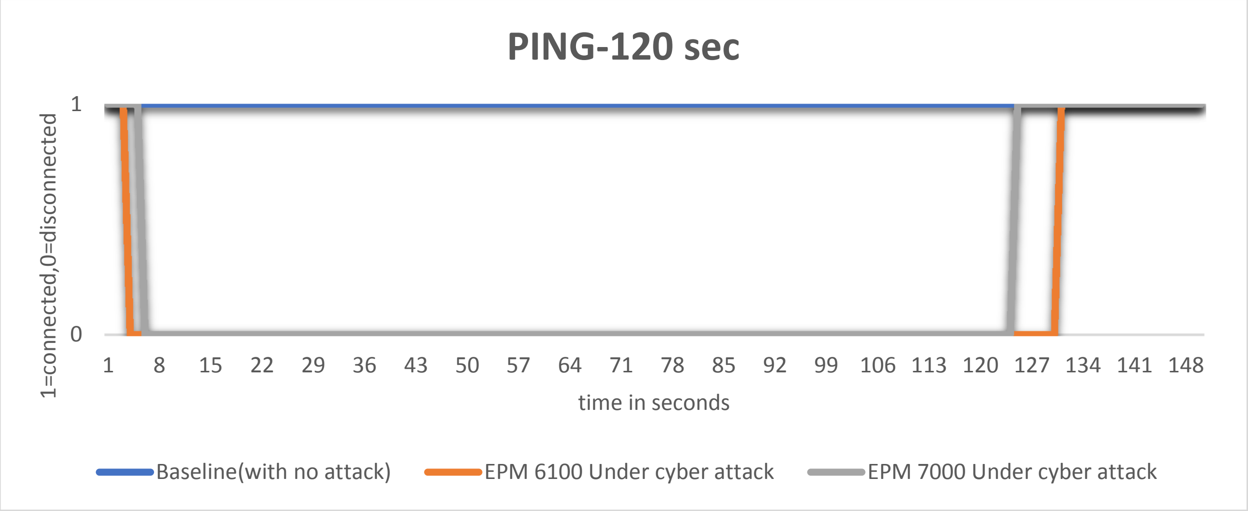


Figure 6.16: Observation under ping attack for 120 seconds

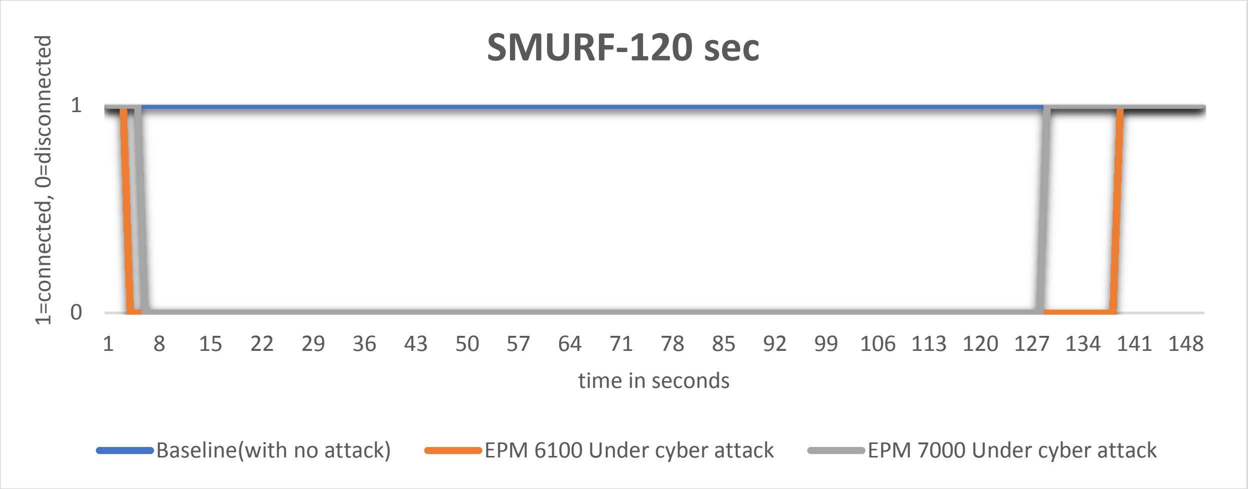


Figure 6.17: Observation under smurf attack for 120 seconds

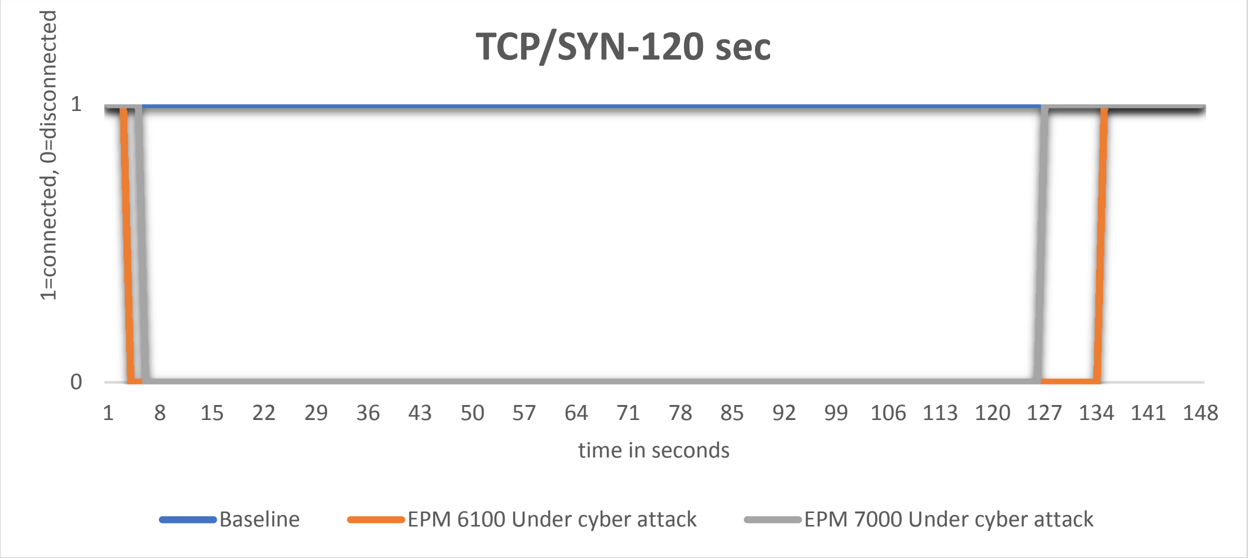


Figure 6.18: Observation under TCP/SYN attack for 120 seconds

To check on the trend, we experimented further with both meters by increasing the attack duration. In this case also disconnection time under all kinds of attack used was 3 seconds for EPM 6100 and was 5 seconds for EPM 7000 respectively which was almost immediate. The duration of all attack used was 300 seconds in this case sent to both the meters through their data communication channel. Initially the meter could communicate the data without having any attack and then attack was introduced while it was communicating.

Then attack was removed to allow meters to recover in order to evaluate their data communication performance. The recovery time under all attacks were different and was 14 seconds in case of ping attack for EPM 6100 whereas 7 seconds for EPM 7100, 23 seconds in case of smurf attack for EPM 6100 whereas 12 seconds for EPM 7100and 19 seconds in case of TCP/SYN attack for EPM 6100 whereas 9 seconds for EPM 7100 shown in (Figure 6.19, 6.20 and 6.21) respectively.

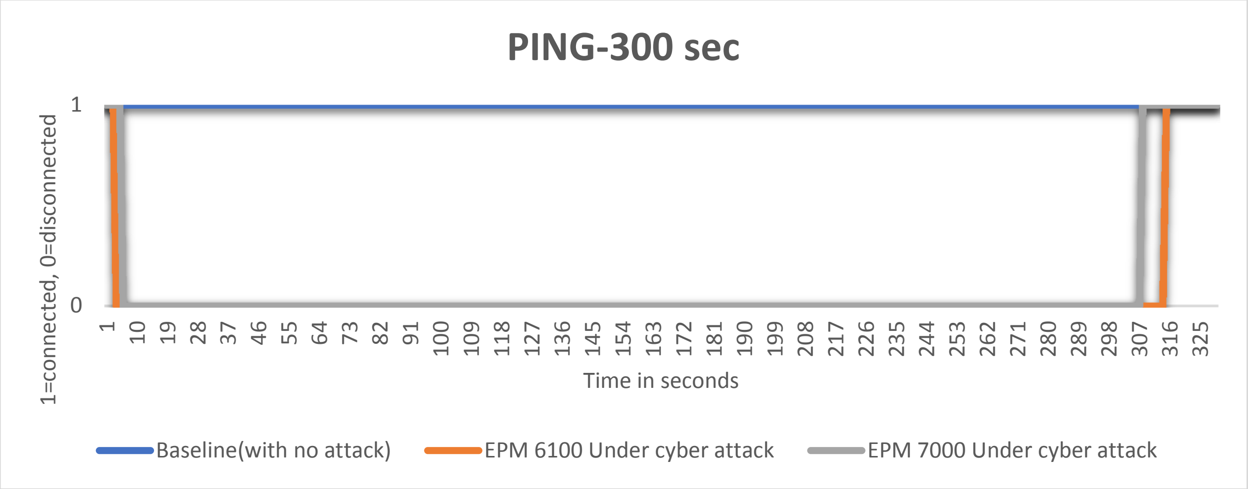


Figure 6.19: Observation under Ping attack for 300 seconds

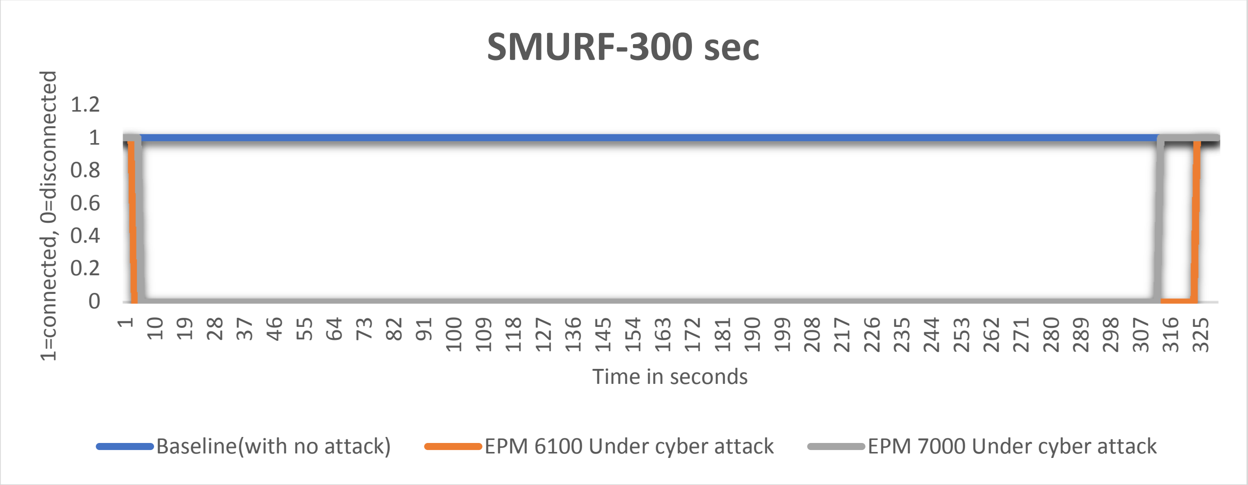


Figure 6.20: Observation under smurf attack for 300 seconds

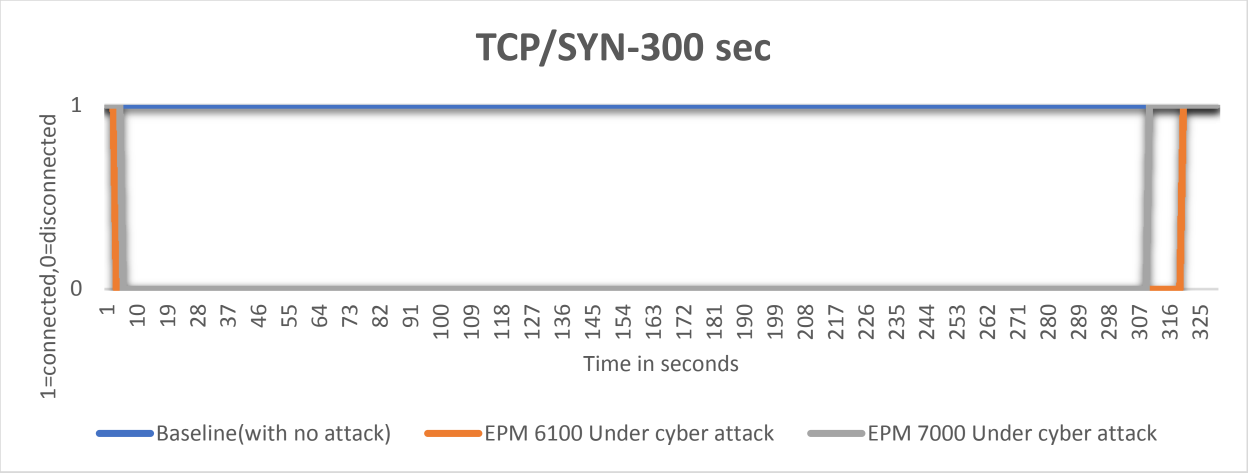


Figure 6.21: Observation under TCP/SYN attack for 300 seconds

To check on the trend, we experimented with both meters further with increasing the attack duration. In this case also disconnection time under all kinds of attack used was 3 seconds for EPM 6100 and was 5 seconds for EPM 7000 respectively which was almost immediate. The duration of all attack used was 600 seconds in this case sent to both the meters through their data communication channel. Initially the meter could communicate the data without having any attack and then attack was introduced while it was communicating. Then attack was removed to allow meters to recover in order to evaluate their data communication performance. The recovery time under all attacks for duration of 600 seconds was identical as compared to recovery time under all attacks for duration of 300 seconds for both the meters as shown in (Figure 6.22, 6.23 and 6.24) respectively.

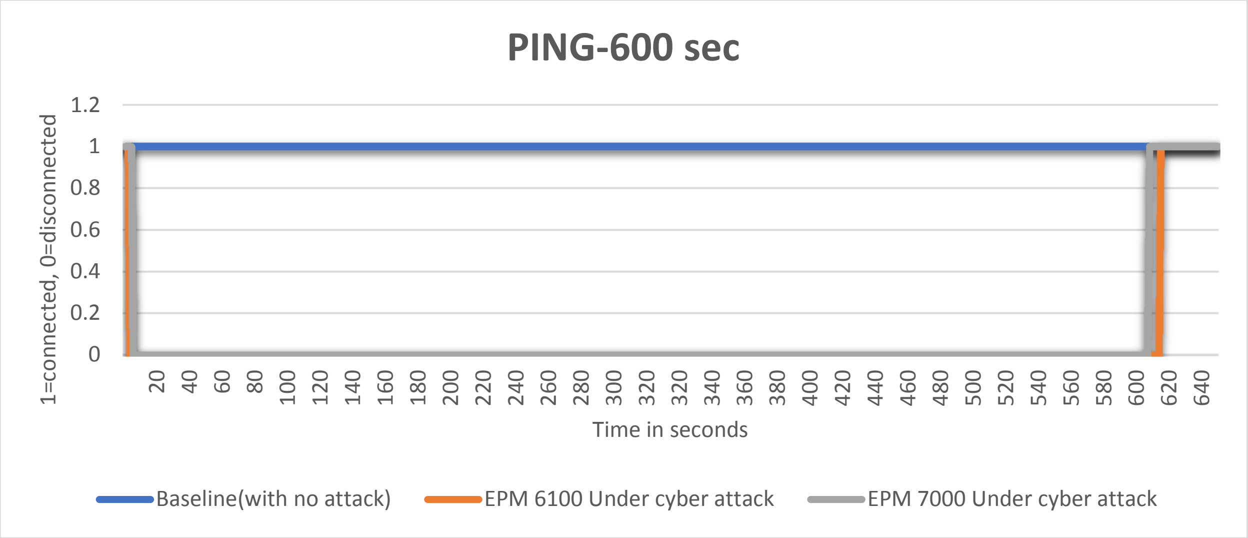


Figure 6.22: Observation under ping attack for 600 seconds

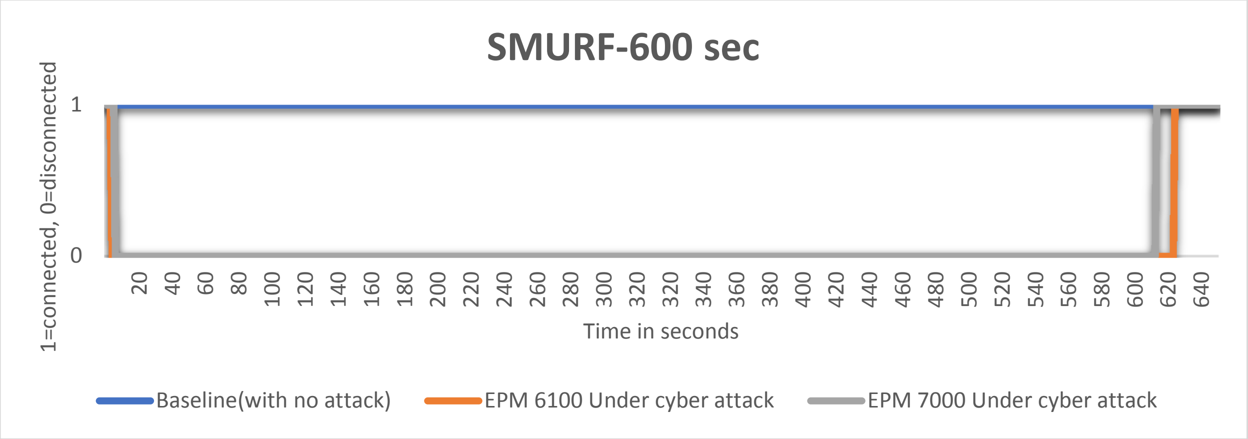


Figure 6.23: Observation under smurf attack for 600 seconds

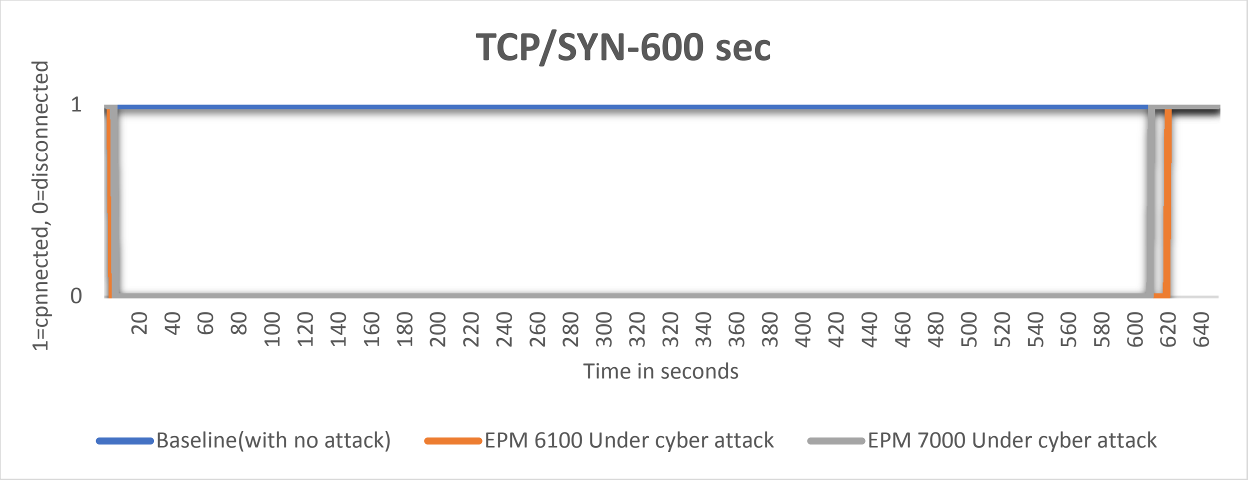


Figure 6.24: Observation under TCP/SYN attack for 600 seconds

To double check on the trend, we experimented with both meters further with increasing the attack duration. In this case also disconnection time under all kinds of attack used was 3 seconds for EPM 6100 and was 5 seconds for EPM 7000 respectively which was almost immediate. The duration of all attack used was 1200 seconds in this case sent to both the meters through their data communication channel.

Initially the meter could communicate the data without having any attack and then attack was introduced while it was communicating. Then attack was removed to allow meters to recover in order to evaluate their data communication performance. The recovery time under all attacks for duration of 1200 seconds was identical as compared to recovery time under all attacks for duration of 300 seconds and 600 seconds for both the meters as shown in (Figure 6.25, 6.26 and 6.27 respectively).

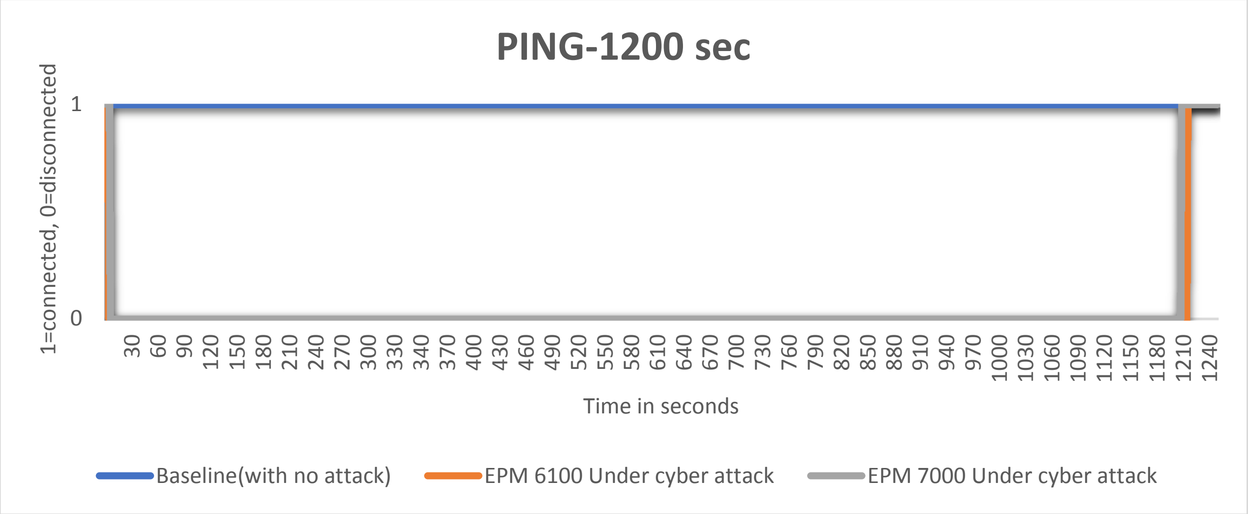


Figure 6.25: Observation under ping attack for 1200 seconds

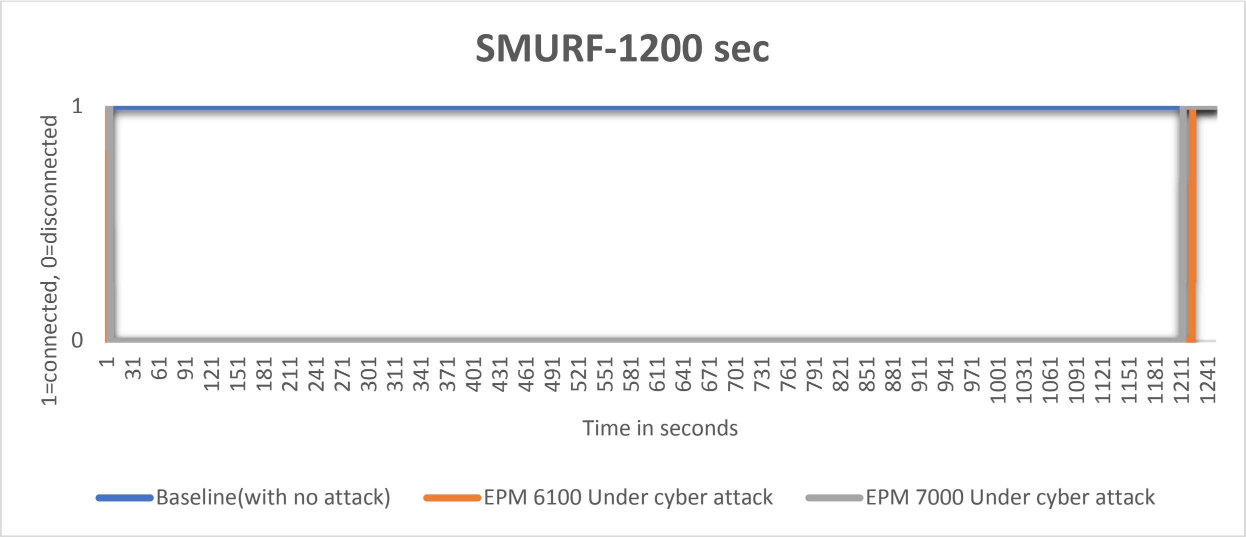


Figure 6.26: Observation under smurf attack for 1200 seconds

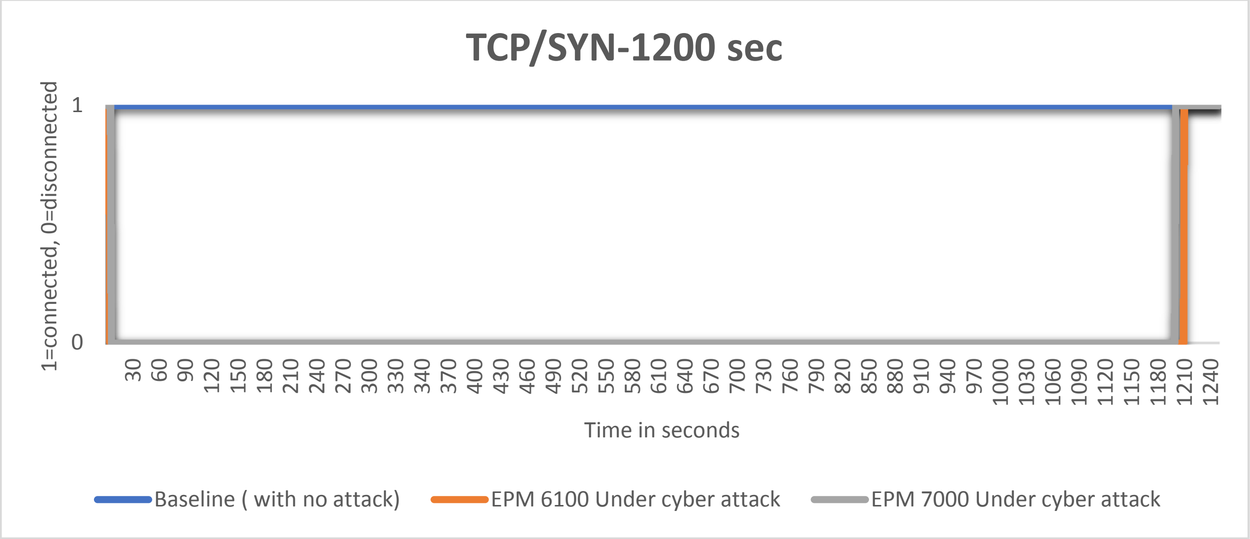


Figure 6.27: Observation under TCP/SYN attack for 1200 seconds

6.5 Chapter Summary

In this chapter It was observed, the comparison of security integrity of data collection to remote location from EPM 6100 and EPM 7000 power quality smart electric meter under direct and indirect cyber-attack and data communication performance of two smart meters when exposed to different cyber security attack. Indirect cyber was having its effect on both the smart meters in terms of security integrity of data collection at remote location. Watt hours recorded under attack has the positive deviation from the baseline recorded without attack. By the end of the billing cycles both the meters have almost identical deviation from the baseline. Direct cyber-attack has different effect as EPM 6100 was recording the same old value recorded before the attack started whereas EPM 7000 was not recording any value. Data communication performance for both the meters was different in case of ping, smurf and TCP/SYN attack used.

The break in data communication under different cyber-attack was identical whereas the recovery time was different under different attack and displays a positive trend with increase in attack duration but after 5min of attack duration any increase in attack duration there was not much increase in recovery time after attack was removed and it seems stagnant. Smurf attack has maximum effect out of all the attack used. EPM 7000 smart meters shows better performance and quick recovery as compared to EPM 6100 meter.

CHAPTER VII

CONCLUSION

This is the first time ever any smart electric meter has been tested and evaluated under a real direct and indirect Cyber security attack This was done to understand its effect on its operation and data communication to remote location. Smart meters are very helpful for customers as well as utilities in their electric power network implementation. Smart meters provide uninterrupted power monitoring and easy trouble shooting related to electric Smart meters in electric power system. But the actual problem is security and the effect of security attacks was not known until these experiments were done. In this thesis, this was found that even a very common Cyber security attack such as Ping based ICMP flood attack can have big impact on operation of a smart electric meter in electric power network. These cyber security attacks can result in significant financial loss in millions of dollars for the power company's deployment in a large-scale power network. This was discovered that the deployment of Ethernet based Advanced Metering Infrastructure (AMI) can contribute to the increase in power consumption for overall customer base served by the AMIs. Customers have no way of knowing that the AMI deployment would cause their electric bill to go higher because the power consumption is higher due to the intermediate systems used in AMI. And the additional power consumption charges may be unfairly passed on to the customers to pay for deploying the AMI network comprising of intermediate network systems, which may be wireline or wireless equipment.

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_Cyber security.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] Nikos Komninos, Eleni Philippou, and Andreas Pitsillides “Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures” IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 16, NO. 4, FOURTH QUARTER 2014 page 1-22https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6805165.

[12] Pardeep Kumar, Yun Lin, Guangdong Bai, Andrew Paverd , Jin Song Dong, and Andrew Martin “Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues” page IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 21, NO. 3, THIRD QUARTER 2019 1-42 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8642293

[13] Muhammad Rizwan Asghar, György Dán, Daniele Miorandi, and Imrich Chlamtac “Smart Meter Data Privacy: A Survey” IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 19, NO. 4, FOURTH QUARTER 2017 page 1-16 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7959167

[14] Zhong Fan, Parag Kulkarni, Sedat Gormus, Costas Efthymiou, Georgios Kalogridis, Mahesh Sooriyabandara, Ziming Zhu, Sangarapillai Lambotharan, and Woon Hau Chin (2013) “Smart Grid Communications: Overview of Research Challenges, Solutions, and StandardizationActivities” IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 1, FIRST QUARTER 2013 page 1-18.

[15] Yi Wang ,Qixin Chen , Tao Hong , and Chongqing Kang (2019) “Review of Smart Meter Data Analytics: Applications, Methodologies, and Challenges” IEEE TRANSACTIONS ON SMART GRID, VOL. 10, NO. 3, MAY 2019 page 1-24 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8322199

[16] Chun-Hao Lo, Nirwan Ansari (2012) “The Progressive Smart Grid System from Both Power and Communications Aspects” IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 14, NO. 3, THIRD QUARTER 2012 page 1-23 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5989902

[17] Electric Power Research Institute. 2007. “Advanced Metering Infrastructure (AMI)” page 1-2

[18] L. Wei, A. Sarwat, W. Saad, and S. Biswas, “Stochastic games for power grid protection against coordinated cyber-physical attacks,” IEEE Trans.on Smart Grid, vol. PP, no. 99, pp. 1–1, 2017.

[19] Advance metering infrastructure based on AMI in smart meter in Smart Grid http://dx.doi.org/10.5772/63631

[20] I. Parvez, A. Sundararajan, and A. Sarwat, “Frequency band for han and nan communication in smart grid,” in IEEE Symposium on Computational Intelligence Applications in Smart Grid (CIASG), Orlando, Dec. 2014.

[21] A. Anzalchi and A. Sarwat, “A survey on security assessment of metering infrastructure in smart grid systems,” in IEEE Southeast Conference, Fort Lauderdale, 2015.

[22] I. Parvez, A. I. Sarwat, L. Wei, and A. Sundararajan, “Securing metering infrastructure of smart grid: A machine learning and localization based key management approach,” Energies, vol. 9, no. 9, 2016.

[23] Sridhar, S.; Hahn, A.; Govindarasu, M., "Cyber-attack-resilient control for smart grid," Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES, vol., no., pp. 1-3, 16-20 Jan. 2012. DOI: 10.1109/ISGT.2012.6175567.

[24] Schukat, M., "Securing critical infrastructure," Digital Technologies (DT), 2014 10th International Conference on, vol., no., pp.298-304, 9-11 July 2014. DOI: 10.1109/DT.2014.6868731.

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

[26] 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.

[27] Department of Energy Office Electricity Delivery and Energy Reliability, “Roadmap to Achieve Energy Delivery Systems Cyber security,” Online: http://energy.gov/oe/downloads/roadmap-achieve-energy-deliverysystems- cybersecurity-2011, retrieved Oct 2014.

[28] 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.

[29] S. Baker, N. Filipiak, and K. Timlin, “In the dark: Crucial industries confront cyber attacks,” 2014.

[30] F. Milano, C. Canizares, and M. Invernizzi, “Multi-objective optimization for pricing system security in electricity markets,” IEEE Trans. on Power Syst., vol. 18, no. 2, pp. 596–604, 2003.

[31] K. Xie, Y.-H. Song, J. Stonham, E. Yu, and G. Liu, “Decomposition model and interior point methods for optimal spot pricing of electricity in deregulation environments,” IEEE Trans. Power Syst., vol. 15, no. 1, pp. 39–50, 2000.

[32] M. Esmalifalak, G. Shi, Z. Han, and L. Song, “Bad data injection attack and defense in electricity market using game theory study,” IEEE Trans. Smart Grid, vol. 4, no. 1, pp. 160–169, Mar. 2013.

[33] S. Amin, G. A. Schwartz, A. A. Cardenas, and S. S. Sastry, “Gametheoretic models of electricity theft detection in smart utility networks: Providing new capabilities with advanced metering infrastructure,” IEEE Control Systems, vol. 35, no. 1, pp. 66–81, Feb 2015.

[34] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. S. Shen, “Energytheft detection issues or advanced metering infrastructure in smart grid,”Tsinghua Science and Technology, vol. 19, no. 2, pp. 105–120, April 2014.

[35] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, “A multi-sensor energy theft detection framework for advanced metering infrastructures,” IEEE Journal on Selected Areas in Communications, vol. 31, no. 7, pp. 1319–1330, July 2013.

[36] E. de Buda, “System for accurately detecting electricity theft,” Patent US 20 100 007 336 A1, January, 2010.

[37] V. Badrinath Krishna, G. A. Weaver, and W. H. Sanders, PCA-Based Method for Detecting Integrity Attacks on Advanced Metering Infrastructure. Cham: Springer International Publishing, 2015, pp. 70–85.

[38] V. Badrinath Krishna, R. K. Iyer, and W. H. Sanders, ARIMA-Based Modeling and Validation of Consumption Readings in Power Grids. Cham: Springer International Publishing, 2016, pp. 199–210.

[39] P. Jokar, N. Arianpoo, and V. C. M. Leung, “Electricity theft detection in ami using customers’ consumption patterns,” IEEE Transactions on Smart Grid, vol. 7, no. 1, pp. 216–226, Jan 2016.

[40] A. A. Crdenas, S. Amin, G. Schwartz, R. Dong, and S. Sastry, “A game theory model for electricity theft detection and privacy-aware control in ami systems,” in 2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Oct 2012, pp. 1830–1837.

[41] 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

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

[43] Gade, R.S.R., Vellalacheruvu, H. and Kumar, S. (2010) Performance of Windows XP, Windows Vista and Apple’s Leopard Systems under a DDoS Attack. International Conference on Digital Society (ICDS’10).

[44] Kumar, S. (2007) Smurf-Based Distributed Denial of Service (DDoS) Attack Amplification in Internet. 2nd International Conference on Internet Monitoring and Protection (ICIMP), San Jose, 1-5 July 2007, 25.

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

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

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

[48] Vellalacheruvu, H.K. and Kumar, S. (2011) Effectiveness of Built-In Security Protection of 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

[49] 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

[50] 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

[51] Einar Petana and S. Kumar, “TCP SYN-based DDoS attack on EKG signals monitored via a wireless sensor network,” Wiley Journal of Security and Communication Networks, Jan 2011 (Online), Sept. 2011 (in print)

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

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

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

[55] EPM 7000 Power Quality Meter Energy Instruction Manual, GE Grid Solutions, Available online https://www.gegridsolutions.com/products/manuals/epm/GEK-113584D.pdf

[56] K. Sundar and Sanjeev Kumar, “BlueScreen of Death observed for the Microsoft’s Server 2012 R2 under Denial of Service Attacks,” *Journal of Information Security*, vol. 7, pp. 225-231, April 2016.

[57] Sanjeev Kumar, Raja Gade, “Windows 2008 Vs. Windows 2003: Evaluation of Microsoft’s Windows Servers under Cyber Attacks,” *Journal of Information Security*, April 2015.

[58] S. Kumar, Ricardo Valdez, Orifiel Gomez “Survivability Evaluation of Wireless Sensor Networks Under DDoS Attack,” *International Conference on Networking*, April 2006.

[59] 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

[60] 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.

[61] 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.

[62] 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).

[63] Sanjeev Kumar, Sirisha Surishetty, 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: A Global Perspective, Vol.20 No.3, Page(s):163-172, 2011.

[64] 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

[65] 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

[66] 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

[67] 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

[68] 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.

[69] 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.

[70] 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.

[71] 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.

[72] 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.

[73] 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.

[74] H. Kumar and S. Kumar, “Effect of Intermediate Network Systems on Remote Power Data Collection in Smart Grid,” accepted *IEEE ICDIS 2020*.

His Publications:

1) Sanjeev Kumar, Harsh Kumar, Ganesh Reddy Gunnam (2019), “Security Integrity of Data Collection from Smart Electric Meter under a Cyber Attack” 2nd IEEE International Conference on Data Intelligence and Security (ICDIS) page 5-9.
2) Harsh Kumar, Sanjeev Kumar (2020), “Effect of Intermediate Network Systems on Remote Power Data Collection in Smart Grid” 3rd IEEE International Conference on Data Intelligence and Security (ICDIS)-Accepted.
3) Harsh Kumar, Oscar A Alvarez, Sanjeev Kumar, “Impact of Indirect and Direct Cyber Security Attack on IoT Based Smart Electric Meter in Smart Grid Infrastructure” Under Review for a Journal.
4) Harsh Kumar, Sanjeev Kumar, “Cyber Attack on Smart Electric Meter”, Poster Presentation, ICDIS, South Padre Island, 2019.
5) Harsh Kumar, Oscar A.Alvarez, Sanjeev Kumar, “ Smart Metering Communication Protocols”, HESTEC, University of Texas Rio Grande Valley, 2018.

BIOGRAPHICAL SKETCH

Harsh Kumar was born on December 21, 1992. He has completed his Diploma in Electrical Engineering from Technical Examination Board, Gandhinagar, India in May 2010. He has completed his Bachelor of Engineering in Electrical Engineering from Gujarat Technological University, Ahmedabad, India in May 2013. He has completed his master's in technology in power system from Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India in May 2018. He has completed his Master of Science in Electrical Engineering from University of Texas Rio Grande Valley, Texas, USA in May 2020. He worked as a Shift Engineer in Prime Health Care Products, Daman, India from July 2013 to May 2014. He worked as a Manager Marketing and Operation in Eram Scientific Solutions Pvt Ltd, Kerala, India from June 2014 to May 2017. He worked as a Research Assistant in Network Research Lab at UTRGV from September 2018 to July 2019. He worked as a Teaching Assistant in Electrical Computer Engineering department at UTRGV from August 2019 to May 2020.

Local Address:

University Commons 1609 W Schunior ST Apartment 1807, Edinburg, Texas, USA-78541.

Email Address & Contact:

madhusasaram@gmail.com

956-780-2916