12-2021

Smart Metering Communication Protocols and Performance Under Cyber Security Vulnerabilities

Oscar A. Alvarez
The University of Texas Rio Grande Valley

SMART METERING COMMUNICATION PROTOCOLS AND PERFORMANCE UNDER CYBER SECURITY VULNERABILITIES

A Thesis

by

OSCAR A. ALVAREZ

Submitted in Partial Fulfillment of the

Requirements for the Degree of

MASTER OF SCIENCE IN ENGINEERING

Major Subject: Electrical Engineering

The University of Texas Rio Grande Valley

December 2021

SMART METERING COMMUNICATION PROTOCOLS AND PERFORMANCE

UNDER CYBER SECURITY VULNERABILITIES

A Thesis
by
OSCAR A. ALVAREZ

COMMITTEE MEMBERS

Dr. Sanjeev Kumar
Chair of Committee

Dr. Weidong Kuang
Committee Member

Dr. Wenjie Dong
Committee Member

December 2021

ABSTRACT

Alvarez, Oscar A., Smart Metering Communication Protocols and Performance Under Cyber Security Vulnerabilities. Master of Science in Engineering (MSE), December, 2021, 106 pp., 7 tables, 74 figures, references, 61 titles.

The communication process is the key that characterizes the modern concept of smart grid, a new technology that introduced a “two-way communication” in energy measurement systems and can be best represented through the smart meters. Hence, the goal of smart metering communication is to ensure a secure and reliable transmission of information that can only be accessed by end users and energy supplying companies. With the goal of improving the information security in smart energy grids, the research presented in this work focused on studying different advanced metering infrastructure communication protocols and, it showcases a series of experiments performed on smart meters to evaluate their defenses against a set of cybersecurity attacks. A small-scale simulation of a smart metering system was performed in the cybersecurity laboratory in the department of Electrical and Computer Engineering at the University of Texas - Rio Grande Valley; and specialized software applications were developed to retrieve data in real time. Our experimental results demonstrated that security attacks have a considerable impact on the communication aspect of smart meters. This could help making smart meter manufacturing companies aware of the dangers caused by cyber-attacks and develop robust defenses against security attacks and enhance overall efficiency and reliability of the smart grid power delivery.

DEDICATION

The completion of my master studies would not have been possible without the love and support of my family. My mother, Nancy Reyna, my father, Oscar Alvarez, my wife, Adelaeda Barrera, and my brothers, Abraham Alvarez, and Ricardo Alvarez. I thank you for believing in me and giving me all your support in the times of need, and happiness. I pray to God for your success in life, as for me this is a big step that will lead me closer to thus goal.

ACKNOWLEDGMENTS

First, and foremost, I would like to thank God who has given me the opportunity to work for a master's degree in electrical engineering, which I have been looking forward to achieving since I graduated from college. He has helped me stand up in the most difficult times and has granted me with wisdom to make life-important decisions throughout these years. Second, I would like to acknowledge Dr. Sanjeev Kumar -a truly knowledgeable, approachable, and patient mentor. You have demonstrated exceptional mentorship that has helped me grow professionally and personally. In addition, I would like to acknowledge my Network Research Lab colleagues, specially, Harsh Kumar, who generously helped with these studies. Third, I am whole heartily thankful for the love and support of my family: my mother, Nancy M Reyna, my father, Oscar A Alvarez, my brothers, Abraham A Alvarez, and Ricardo A Alvarez, and my wife, Adelaeda Barrera. If there is anything I would never replace, it is the guidance of my mother, the wisdom of my father, and the unconditional help of my brothers. To my wife, holding your hand while walking through this path was the most exciting part of this journey. You were always there for me, and you have proven to be my better half. I want to give special thanks to Gilberto Mendez, who has also been a great mentor and friend, and taught me everything I know about smart metering. Finally, to my friends, Miguel Ramirez, Misael Morales, and Jose Luis Rodriguez whose support was essential during the early days of my career in engineering, thanks. The support of this research is provided in part by the US National Science Foundation under Grant No. 0421585, Benston Jr. Endowment Chair in Engineering Fellowship, and Houston Endowment Chair in Science, Math and Technology Fellowship.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

CHAPTER I

INTRODUCTION

Today, electrical energy is a necessity to execute most of daily regular tasks. Washing machines, televisions, air conditioners and every single light bulb used at home requires electrical energy to work. Nevertheless, electrical energy is not cheap. Special machinery, dedicated personnel, and various resources are necessary to obtain electrical energy. Some industries have made their business to create this energy for us and, through arrangements with other companies (utilities), the administration of electrical energy deliverance to each single household and business has been possible. This administration has led to the creation of a system of energy deliverance denominated as the "grid."

An electric power grid is a network of power generators, transmission lines, transformers, and distribution systems to provide consumers with the power they need [1,2]. Thanks to this system, every home has the privilege of electrical energy usage. Yet, administration of energy is not an easy task. Utility companies must study how much energy they must deliver, where, and when. Otherwise, a bad administration can lead to disastrous results, like blackouts that could last weeks. This led to the conclusion that an electrical grid had to be improved in a way that a proper communication system between the energy administrators and every single end in the grid were achieved. Hence, the grid stopped being simple, and became smart.

Smart grids became the next generation of power grids due to the use of bidirectional stream of energy [3]. Communication is the key component for the proper administration of energy in any smart grid infrastructure [3-6]. Modern technology offers the tools to achieve successful communication through different mediums and methods. But also, modern technology has also tools that can compromise a communication between ends. This unfortunate truth has made communication systems a field of study in cybersecurity.

The work presented here demonstrates how is a smart metering system severely affected when modern technology is used to perform cyber-attacks. This thesis begins by introducing common concepts in smart grid science, then it provides three major contributions: a deep study about current smart metering communication technologies and protocols, a series of experiments involving the use of common cyber-attacks in metering systems, and finally, results that demonstrate the negative effects of cyber-attacks in the communication aspects of smart meters. As smart grids are becoming part of humanity's necessary technology, cybersecurity must keep studying to help improve the existing communication methods and ensure a reliable system where consumers can always count with their needed energy and utility companies can control its delivery.

1.1 Advantages of Smart Grid Implementation

By "grid" it refers to the electrical grid, a network of transmission lines, substations, transformers, and power generators that deliver electric energy from the power plant to homes and businesses [1,2]. The term "smart" comes from the digital technology that allows a two-way communication between the utility and its customers, and the ability to sense along the transmission lines. The key to use the enormous potential that this idea offers is the

communication. Having the knowledge of the energy a user consumes creates awareness of all energy consumption. Yet, there are more benefits associated with smart grid as:

- More efficient transmission of electricity.

  Analyzing the places where less energy is required, energy waste can be considerably reduced. The energy that was not wasted can be used to always ensure delivery where it is needed.

- Quicker restoration of electricity after power disturbances.

  Smart grid allows communication between ends and nodes within the grid. This meaning that devices can communicate to each other and alert when some are behaving abnormally.

- Reduced operations and management costs for utilities, lowering costs for consumers.
- Reduced peak demand, which will also help lower electricity rates.

  There are programs where users are asked if they can have a reduced energy delivered to their homes during peak times, this to ensure energy used on all the demanding sectors. In exchange, the user obtains reduced electricity rates [4].

- Increased integration of large-scale renewable energy systems.
- Better integration of customer-owner power generation systems.
- Improved security.

1.2 Smart Meters

Before being called smart, electricity meters, patented by Samuel Gardiner in 1872, were only capable of providing information about the current flow; and had to be physically read by a person standing in front of the meter [7,8]. Smart meters are a common form of smart grid technology; their digital design replaced the old analog meters used in homes to record

electrical usage. Smart meters are defined as devices capable of performing two-way communications, allowing to make deep analysis of energy consumption in a certain location, and making possible the access of data from any part of the grid [9]. Smart grids allow users to monitor the consumption more precisely, so the user can make more informed energy choices. Work done in [10] explains that in the European Smart Metering Alliance (ESMA), the definition for smart metering is set as follows:

•An automatic process, transfer, management, and utilization of metering data.

•A 2-way data communication with meters.

•A Supporter of services that improve the energy efficiency of the energy consumption and the energy system (generation, transmission, distribution and especially end-use)

The use of smart meters has been well accepted worldwide. By 2019, the United States already had installed 94.8 million smart meters out of which 88% were for residential use [11]. In summary, smart meters implement two major functions, which are communication and measurement. This means that each meter electronic system consists of two subsystems. The metrology subsystem records the data obtained from the power line, whose interpretation depends on the program that calibrated the meter. The communication subsystem takes care of the security and transmission of information [2,12]. Depending on the type of technology used, field purposes, and manufacturing company's interests, the communication designed can be either using wireless technologies (radio, ZigBee, cellular, Wi-Fi), or wired (ethernet, power line communications). Wireless communications have the advantage of having a low-cost infrastructure and ease of connection to difficult areas [3]. A very accurate statement described by the authors in [7] about a successful implementation of a smart metering system is that the

choice of communication technology is the most important aspect to take care of. The final application, the features of the location, and the topology of the electricity grid, among others, must influence when choosing the most appropriate technology. Some technology solutions offered by companies such as Landis+Gyr, establish a well-designed communication net. For example, Landis+Gyr offers a solution called Gridstream. This solution, also known as mesh network, has the advantage of having meters sending their recorded information to all the nearby meters until reaching the operations center. In the case of an anomaly, the information travels using the shortest path to their destination [3,13]. In the United States, radio frequency (RF) technologies for smart metering deployments are the most widely spread. The best-known topology is called RF mesh, where each smart meter talk to each other and form a Local Access Network (LAN) cloud to a collector [7,14]. Smart meters also come with a variety of features such as the remote disconnection, which allows utility companies to disconnect power from a specific home without the necessity of physically sending a technician.

1.3 Advanced Metering Infrastructure (AMI)

Before the introduction of AMI, for many years the smart metering system used was called Automated Meter Reading (AMR). AMR advantage consisted of the remote readings of meters which allowed the availability of metering data to the utility companies. However, AMR communication was one-way type, and therefore, meter management was not possible [15-17].

The AMI is an integrated system of smart meters, communications networks, advanced sensors, monitoring systems, and data management systems that enables two-way communication between utilities and customers [3,4]. The system provides several important functions that were not previously possible or had to be performed manually such as the ability

to, automatically and remotely, measure electricity use, connect and disconnect service, detect tampering, identify, and isolate outages, and monitor voltage. Hence, AMI makes possible the intelligent management of various power-related applications and services-based power-related data [2]. Data presented in [18] prove through statistics that thanks to AMI implementations, utilities can identify outages quicker than before which ends in producing lower costs and fewer inconveniences for both customers and producers. While smart grid extends its definition to all devices arranged in a network, AMI refers specifically to meter communication infrastructure (an integration of technologies that provide an intelligent connection between consumers and suppliers) [19].

1.4 Importance of Cybersecurity in Smart Grid

If the communication in a smart grid is compromised, it can be turned against users. In article [20], the authors defined three types of scenarios depending on the threats to the smart grid: manipulation, sabotage, and espionage. Each of these scenarios are directly involved with the three elements of the security triad (confidentiality, integrity, availability). The possible scenarios could be as the following:

- Confidentiality. An AMI secure system must be the one where all stored information regarding consumption and billing must be protected to ensure the customer's privacy and business. Knowing the energy consumption from a home could let cyber criminals detect when the peak demand occurs as well as when is the consumption at is minimum. This would allow anyone to predict when a certain home is empty, and to study the behavior of customers [2]. Authors in [21] demonstrated how they can identify major devices by analyzing the energy consumption data from the smart meter. Such information is useful for espionage from a single individual to a whole community [20].

- Integrity. An AMI operation is dependent of the integrity of information [2]. To have a better administration, system owners must know how energy is consumed. Even worse, reporting less energy consumption in a certain area will lead to disastrous shortages since energy delivering companies would not be prepared for such consumption.
- Availability. This element is the response to the question why smart grid. AMI must always ensure that any network resources, such as data, bandwidth, and equipment, will always be available to any authorized entity [22, 2]. Not only having incorrect information can cause the consequences described before, but also the lack of access to this information. Interrupting communication leads also to wrong reports. According to many studies like in [2] and [20], DoS attacks are of the most dangerous attacks against an AMI. They overload the communication risking the failure of the functionality and not many improvements have been done that could prevent these types of attacks.

There are different cyber-attacks that theoretically, could be used to achieve one of the bullets before. Thankfully, meter manufacturing companies have paid attention to this matter, and developed meters with strong security. Hence, this work attempts to simulate a system already implemented in the field and determine through a different type of known cyber-attacks whether if the meter or the whole system has weak spots.

CHAPTER II

SMART METERING COMMUNICATION TECHNOLOGIES AND PROTOCOLS

2.1 Communication Technologies

Technologies in smart metering communication can be divided in two types: wired and wireless. Ethernet, powerline, and optical wiring are the most common wired technologies used. Radio-frequency communication, Wi-Fi, Bluetooth, ZigBee, and cellular technology are currently the most common wireless used technologies. Each technology has their own hardware specification and communication protocols. Although wireless communications have some advantages over wired communications like low-cost infrastructure and ease of connection to unreachable areas, the choice of communication technology is carefully considered as it may fit to one environment, but not to another one (mostly depends on the infrastructure already in place before a transition to smart metering) [3]. The table below provides some advantages and disadvantages of most of the technologies mentioned above.

Table 1. Advantages and Disadvantages of Common Smart Metering Communication Technologies [3,23,24,25].

Communication Technology	**Advantages**	**Disadvantages**
Ethernet	i. Very high speed ii. Secure against attacks iii. High reliability iv. Latest cables like Cat-6 consume less power.	i. Lack of mobility ii. High expansion cost iii. Connections are limited to number of ports
Wi-Fi	i. Users can connect at any location ii. Minimal infrastructure setup iii. Easily expandible iv. Range can be extended with repeaters.	i. Not very secure ii. Susceptible to interference iii. Low speed compared to wired network iv. May be hazardous to health

Table 1, continued.

Bluetooth	i. Low power consumption ii. Short setup time Support limited node star topology.	i. Low coverage area ii. Very low bandwidth Interference from RF on same Hz
IrDA	i. Very cheap ii. Compact and light weight iii. Consumes less power. iv. No interference from RF waves Secured compared to RF technologies.	i. Requires line of sight for both sender and receiver. ii. Device cannot move around while transmission is in progress Used for a very short distance
Zigbee	i. Operates on multiple frequency band. ii. Supports up to 65,000 devices in a network. iii. Operates on a very low power. iv. Zigbee nodes have a very low cost.	i. High interference ratio from applications using the same bandwidth. ii. Licensing fees are high, with a single license at approximately $3,500. iii. Limited support available
LTE	i. Low latency ii. Low power consumption iii. Fully integrated with 3GGP iv. Fast handover across networks Spectral Efficiency	i. Uses the Licensed spectrum. ii. Not always available Not compatible with older technologies
RF Mesh	i. Easily scalable due to redundancy ii. Resistance to problems Range can be easily defined	i. Initial high setup cost ii. Increased workload for each node Latency issues in low powered networks

2.2 AMI Protocols

Most of machines in this era communicate through signals and information displayed through strings of letters and numbers. The units used to represent data depend on the OSI layer. For this work, the units used were frames. For a machine to interpret the information received, specific rules and standards have been designed so that any computer can receive data packets, understand them, and execute the proper action according to the information received. These rules and standards are known as protocols. Generally, communication protocols consist of defined sequences that begin by having a requesting device identifying itself to the requested device. After the identification, there must be an exchange of parameters to stablish the

communication desired. Not all protocols are used to perform communication rules, but also to define structures to store and retrieve data. ANSI C12.19 for example, is a set of defined tables where every bit corresponds to a cell with a name that is associated to a specific state of the smart device; and table cells can be associated with other cells. Protocols are also used to define standards for the physical medium used. For example, standards like RS232, RS422, and RS485, define the electrical characteristics of drivers and receivers for use in serial communications systems. The study presented in [26] explains the differences between these three and [27] explains design standards of RS485 (network topology, cable specifications, data rate). However, these standards define the hardware technology (physical medium) of the communication system, not the data transmission protocol. Other standards define the protocols for communication over a RS-485 link. Table 1 displays some of the protocols used to stablish communication.

Table 2. Common meter communication protocols in the market and a brief description.

PROTOCOL	DESCRIPTION
Open Smart Grid Protocol (OSGP)	Created by the European Telecommunications Standards Institute (ETSI). OSGP provides reliable and efficient delivery of command-and-control information for smart meters, direct load control modules, solar panels, and other smart grid devices. It is one of the most widely used smart meter and smart grid device networking standards. The full protocol is in [28].
ANSI C12.18	Used for two-way communications with a meter. Written specifically for meter communications via an ANSI Type 2 Optical Port and specifies lower-level protocol details [29].
ANSI C12.19	Specifies data table structures to store and manage data within the meter's memory. C12.19 does not define communication hardware design criteria nor specify the language or protocol used to transport data [30].
ANSI C12.21	Used for two-way communications with a meter. Written specifically for meter communications via telephone modem [31].
ANSI C12.22	Describes the communication session over a network for interoperability purposes among communications modules and meters [32].
IEC 61107	Published by the International Electrotechnical Commission (IEC). It sends ASCII data using a serial port. The physical media are either a modulated light, sent with an LED and received with a photodiode, or a pair of wires [33].
DLMS/COSEM	It has an object-oriented structure, allowing reading application data of different manufacturer's meters in the same way. DLMS is a universal abstract language for meter communication being standardized in IEC" [33].
Modbus TCP/IP	Created for industrial automation systems and controllers. It is an application protocol designed as a messaging structure defining rules for the organization and interpretation of data. Modbus devices use a master-slave (client-server) relation [34-36].
G3 PLC.	Adapted to the power lines that are already installed in homes running electrical energy. This protocol was designed to overcome all these adversities in the power line hostile environment with the use of an orthogonal frequency division multiplexing (OFDM) modulation technique [37].

2.3 ANSI Protocols

Most of the information about these protocols was obtained from the referenced documents [30], [29], [31], and [32]. The American National Standards Institute (ANSI) has served as an administrator and coordinator of the United States private sector of voluntary standardization system for more than 100 years. ANSI protocols were designed to help smart meter companies establishing rules and specifications for the communication between a user and the meters. Landis+Gyr, one of the leading smart meter manufacturing companies, uses ANSI protocols to stablish communication with their meters [38]. Generally, ANSI C12.18, C12.21, and C12.22 protocols provide three common functions:

1) Adjustment of communication channel
2) Transport of information
3) Closure of channels once communication procedure is completed.

To provide their communication capabilities, the rules of all three protocols apply to the following layers from the OSI seven-layer model:

- Physical layer
- Data link layer
- Application layer

Nevertheless, most of the work detailed in all three protocols focuses on the application layer. ANSI protocols include an application language called PSEM (Protocol Specification for Electric Metering) that allow applications to read and write over meter memory tables.

START OF PACKET	IDENTITY	CONTROL	SEQUENCE NUMBER	DATA LENGHT	DATA	CRC

Figure 1. ANSI data frame structure.

Figure 1 shows the data frame structure followed by ANSI protocols. Where the start of packet byte is always represented by hexadecimal value EE. The identity byte represents the C12.19 devices used. The control byte indicates whether if the packet is unique, or if it was fragmentated. If the packet was fragmentated, the sequence number byte indicates the number of fragments remaining. The data length word indicates how many bytes of data are being sent in the frame. Data frames regulated by all three protocols contain a word-long field for cyclic redundancy check (CRC). The CRC defined by the protocol is the standard polynomial $X^{16} + X^{12} + X^5 + 1$. However, to reduce bit-errors in transmitted messages, a checksum is also included at the end of the data field. The author in [39] presented an experiment to determine the efficiency resulted from the interaction between both the checksum and the CRC.

2.3.1 ANSI C12.18: Protocol for Optical Ports

This protocol defines the standards used for optical communication using an ANSI Type 2 optical port. The original protocol ANSI C12.18 is defined in [29]. This protocol defines the requirements for the physical layer of (optical port and optical cable), and it also describes the data link layer specification, which consists of stablishing communication settings.

As stated before, the focus of these protocols is the application layer. ANSI defines nine PSEM (Protocol Specification for Electric Metering) services for data exchange during a communication session:

- *Identification*. Is the first service used. This service returns the version and revision of protocol.
- *Read*. This service is used to request data stored in the target device. The requesting device must specify the memory location of the data of interest.
- *Write.* This service is used to write data in the memory of the target device. The requesting device must specify the memory location where the new data will be written.
- *Logon*. Establishes a session without access permissions.
- *Security*. This service provides setting access permissions.
- *Logoff*. This service is used to shut down the session.
- *Negotiate*. This service is used to reconfigure certain parameters in the communication channel when the manufacturer does not wish to use the default values established. Examples of this parameters are baud rates, packet size, and maximum number of packets.
- *Wait.* This service is used to maintain an established communication channel during idle periods preventing termination.
- *Terminate*. Sets an immediate stop of communications.

Figure 2 displays a C12.18 typical ordered messaging exchange sequence in a common communication session.

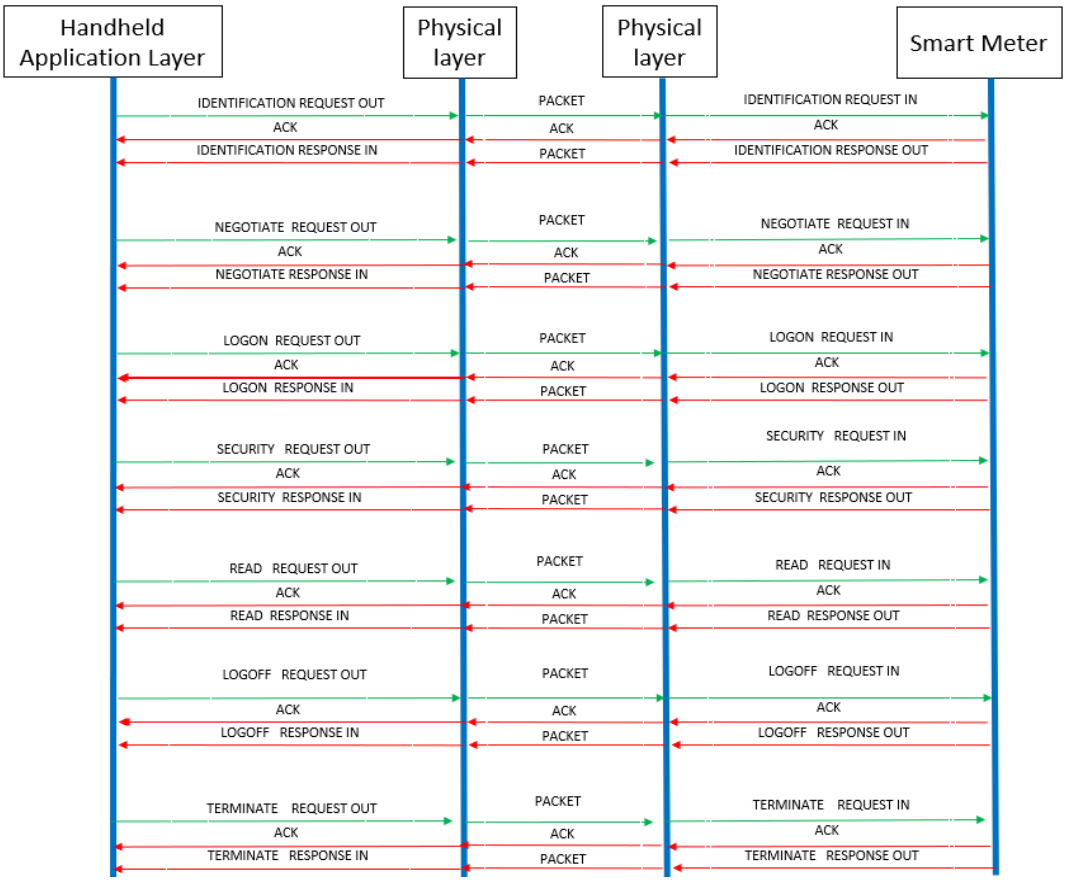

Figure 2. Typical communication session using ANSI C12.18.

2.3.2 ANSI C12.21: Protocol for Telephone Modem Communication

ANSI C12.21 was designed for communications between smart devices using modems connected to the switched telephone network. The original protocol ANSI C12.21 is defined in [31]. The structure of C12.21 was designed as an extension of C12.18, but applied for a different communication medium, which required a bigger number of PSEM services and an extended use of tables from C12.19. Another two major differences are that C12.21 does not define the physical layer standard and both protocols listed differences for their data-link layers. C12.21 provides important information about the communication channel settings, the CRC

selection, acknowledgement, retry attempts, timeouts, and collision. The communication channel settings can be subdivided into the two types: fixed settings, and variable settings.

Listed below are the differences between the services defined by C12.21 compared with C12.18 along with those services only defined by C12.21.

- *Identification Service*. More response options than C12.18 (more features)
- *Authenticate Service*. Used when a higher level of security is desired. It provides a two-way authentication with playback rejection at the session level.
- *Negotiate Service*. Same as in 12.18, but baud rate is ignored because the data rate for 12.21 is stablished by the modem.
- *Terminate Service*. Provides for immediate transfer to the base state. All parameters return to default values.
- *Timing setup service*. Helps reconfiguring time-outs, delays, and retry-attempts. It is an optional service.
- *Disconnect service*. Used for immediate disconnection of the communication channel.

A communication session using ANSI C12.21 protocol is represented in Figure 3.

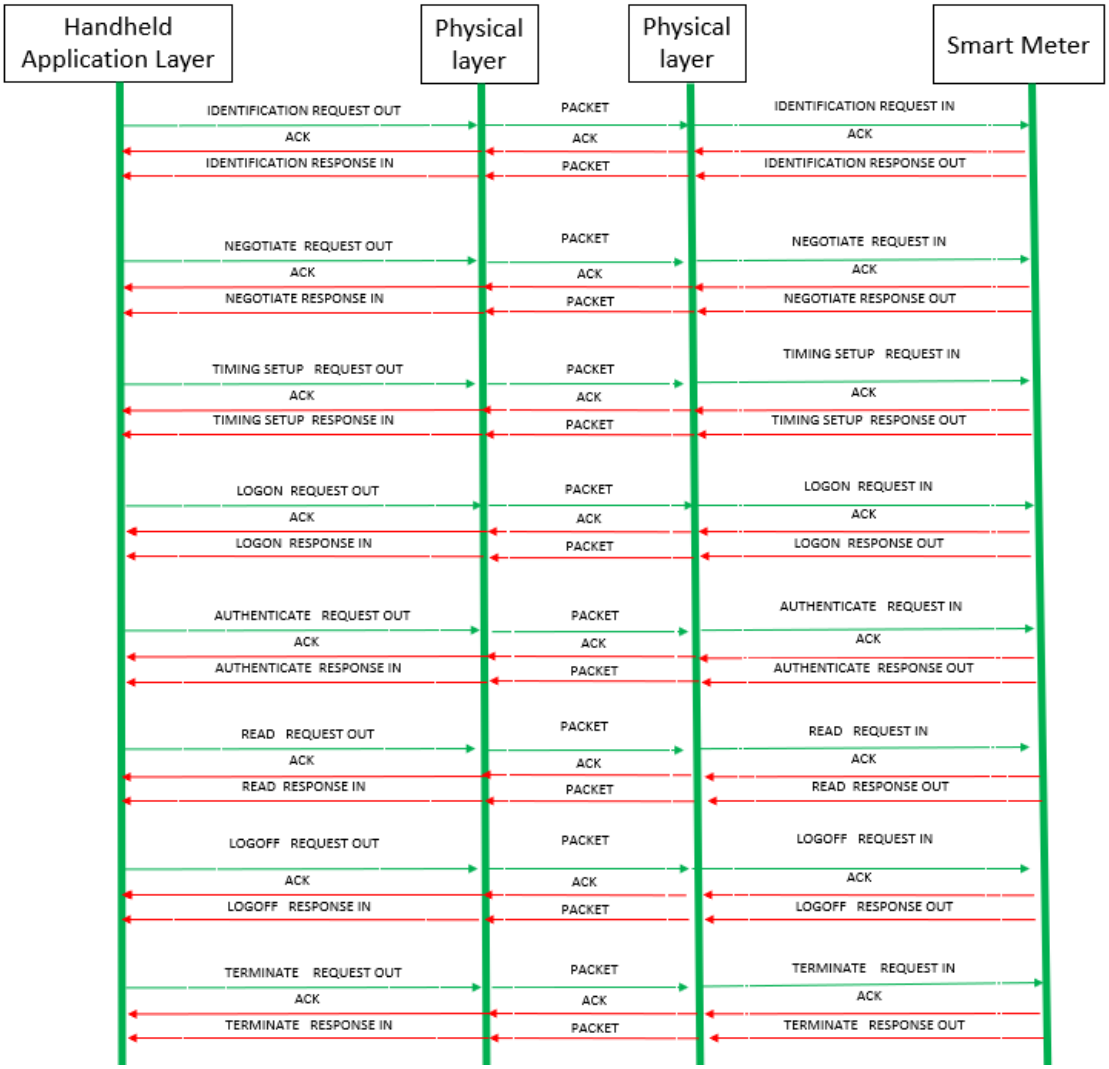

Figure 3. ANSI C12.21 typical communication session.

2.3.3 ANSI C12.19: Protocol for Utility End Device Tables

The original protocol ANSI C12.19 is defined in [30]. Unlike C12.18 or C12.21, C12.19 does not specify any type of rule or parameter used for the transportation of data. C12.19 stablished a multi-table structure used to allocate data in the memory of the smart meter. ANSI C12.19 defines several tables, yet the three major ones are:

- Standard tables

- Manufacturer tables
- Extender user-defined tables

Due to all the development done on C12.19, this protocol has been well accepted to define the data model even for non-ANSI protocols. In article [40], the author explains the improvements and extensions done to the protocol since its first published version in 1997. The author in [41] explored the use of ANSI C12.19 to implement a DDS middleware with the intention to prove it as the best solution to address the heterogeneity and complexity of advanced metering infrastructure systems.

When a data frame requesting to read/write information is received by the device, the frame must have the table intended as well as the fields required identified. Each field in the table represents a bit or bits of memory. The table below represents an example of a C12.19 implementation.

Table 3. C12.19 sample table

STANDARD TABLE	**20**
FIELD	**DATA TYPE**
ED_MODEL	CHAR [5]
FIRMWARE VERSION	UINT8
FIRMWARE REVISION	UINT8
SERIAL NUMBER	CHAR [3]

Using ANSI C12.18, if the user wishes to obtain the information from the standard table 20 in Table 3, the read request data frame would be EE0000000003300014382C. Down below, the frame is explained by sections.

EE	Start of packet
00	C12.19 identity
00	Control
00	Sequence number
0003	Length of DATA – 3 bytes
30	DATA – Requesting to read full table

0014	DATA – Table Id: 20 (decimal value)
382C	CRC

Hence, the device would respond with the data frame EE000000000E00000A55545247420A4B4A853F19432C. Down below, the frame is explained by sections.

EE	Start of packet
00	C12.19 identity
00	Control
00	Sequence number
000E	Length of DATA – 14 bytes
00	DATA – OK (ACK)
000A	DATA – length of TABLE DATA: 10 bytes
5554524742	DATA – TABLE DATA: ED_MODEL (CHAR [5]) – UTRGV (ASCII)
0A	DATA – TABLE DATA: FIRMWARE VERSION (UINT8) – 10 (decimal value)
4B	DATA – TABLE DATA: FIRMWARE REVISION (UINT8) – 75 (decimal value)
4A853F	DATA – TABLE DATA: SERIAL NUMBER (CHAR [3]) – 4,883,775 (decimal value)
19	DATA – Checksum
432C	CRC

The user will interpret that the device model name is “UTRGV”, the firmware version is “10”, the firmware revision is “75”, and the meter serial number is “4,883,775”.

2.3.4 ANSI C12.22 Protocol Specification for Interfacing to Data Communication Networks

Using all the definitions from ANSI C12.18 and ANSI C12.21, plus the table structure defined by ANSI C12.19, ANSI C12.22 was created to make ANSI applications possible to transport data to any type of network communication system. The author in [42] provides a survey about the advantages of implementing C12.22.

The original protocol ANSI C12.22 is defined in [32]. The standard focuses on defining the services used to stablish a communication session between two ANSI devices and how can an ANSI device can communicate with a device from another protocol. To achieve the extend of the protocol, C12.22 introduces the Extended Protocol Specification for Electric Metering (EPSEM) which differentiates from PSEM because of the inclusion of more services than the ones used in previous ANSI protocols. Besides the introduction of EPSEM, the standard defines data management procedures on more OSI model layers than in previous protocols and it adds more table information to C12.19 to assist the allocation of values used for network communication of any kind. The table below displays the extra services used in the application layer.

Table 4. Extra-Services used to stablish a communication session using C12.22 [32].

SERVICE	DESCRIPTION
Registration	Adds and keeps routing table entries of C12.22 relays active. To be part of a C12.22 network, a C12.22 node shall send a registration service request to one of the C12.22 master relays.
Deregistration	Removes routing table entries of C12.22 relays, master relays, and provide service discontinuation of all the C12.22 master relay authentication and notification hosts.
Resolve	Retrieves the native network address of a C12.22 node. This native address is used to communicate directly with other C12.22 nodes on the local area network.
Trace	Retrieves the list of C12.22 relays which has forwarded a C12.22 message to a target C12.22 node.

The network topology used for ANSI C12.22 communication requires C12.22 gateways for the translation of the C12.22 protocol to other protocols. The purpose of this architecture is to allow the creation of C12.22 devices that can reside on any type of network. This architecture also allows the development of C12.22 communication modules that can interface any C12.22 devices to specific networks. Transport layer services are defined to facilitate setup, management and communication with one or more C12.22 communication modules.

The Data Link Layer is used only for communication between the C12.22 device and the C12.22 communication module. Figure 4 below represents the general idea of the data flow between a C12.22 device to the C12.22 communication module to the network.

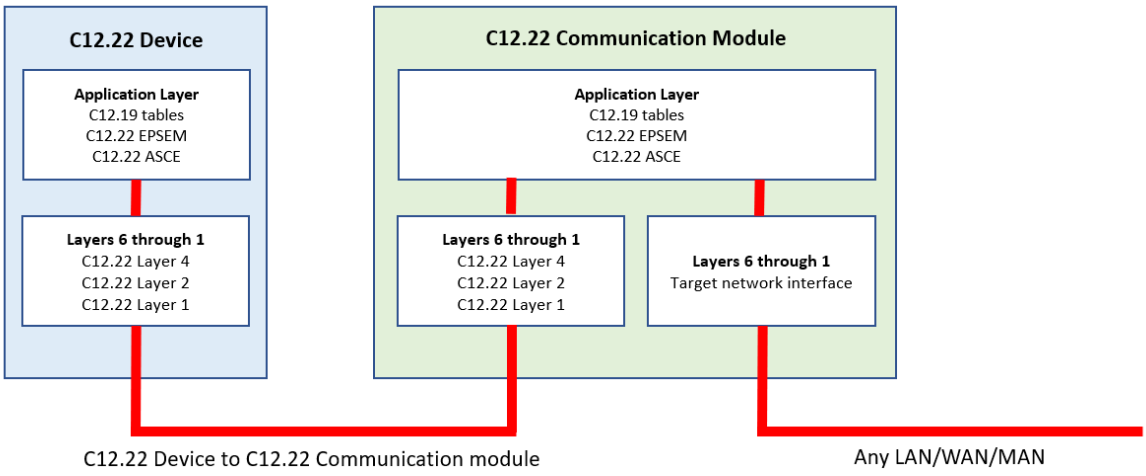

Figure 4. Flow of communication using ANSI C12.22 [32].

ANSI C12.22 security mechanism relies on a mode of encryption called EAX' in conjunction with the Advanced Encryption Standard (AES) block Cipher with 128-bit keys. The protocol provides the ability to both protect the privacy of portions of a message, as well as authenticate the entire message. To successfully exchange authenticated and private messages, each side of the communication link must share the same cipher-algorithm and key [32]. Although the security aspect may seem well developed, authors in [43] claim vulnerabilities that could lead to a denial of service attack.

2.4 Modbus TCP/IP

Most information about this protocol was obtained from the referenced documents [34], [35], and [36]. Modbus TCP/IP was created for industrial automation systems and controllers. It

is an application protocol designed as a messaging structure for the organization and interpretation of data. This protocol is independent of the transmission medium (physical layer) since it uses Ethernet technology which is standardized by IEEE 802.3. MODBUS TCP/IP devices use a master-slave (client-server) relation in which one device (master/client) initiates a transaction (query), while the slaves (servers) respond by returning the requested data to the master. A client's transaction is a data packet consisting of a server address, a function code defining the requested action, data required for the transaction, and an error checking field. A server's response consists of fields confirming the action taken, data returned, and an error checking field. The error check field of the server's message frame allows the client to confirm if the contents of the message are valid. Hence, the client/server model; is based on four types of messages:

- *Modbus Request* – message sent by the client to initiate a query.
- *Modbus Confirmation* – used by the client to confirm the response sent by the server.
- *Modbus Indication* – used when the request message is received by the server.
- *Modbus Response* – sent by the server to answer client's request.

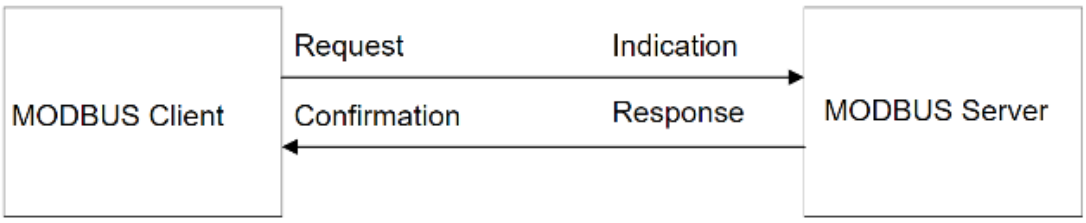

Figure 5. Modbus TCP/IP message exchange [34]

Figure 6 displays a representation of the network architecture for a system using Modbus TCP/IP communication standards. In general, MODBUS communication systems consist of

three different types of devices: MODBUS clients, MODBUS servers, and Interconnection devices (bridges, routers, gateways)

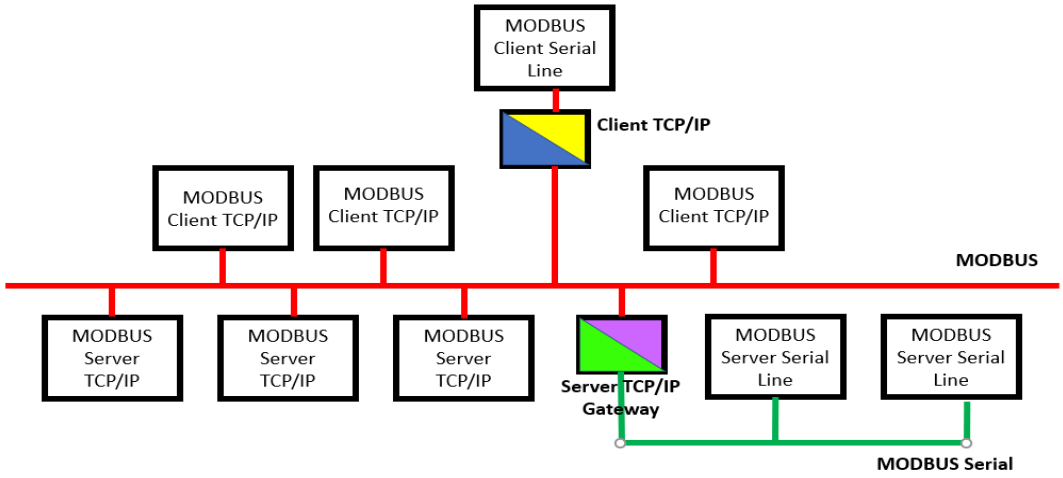

Figure 6. Modbus TCP/IP communication architecture.

Modbus TCP/IP defines a Protocol Data Unit (PDU) as the basic data frame, which consists of a function code and the data of interest. For traditional serial Modbus, the PDU gets extra fields added (additional address and error check) making the packet to become an Application Data Unit (ADU). The data field in the PDU includes register addresses, count values, and written data. When the slave device responds to the master, it uses the function code field to indicate either a normal response, or that an error has occurred.

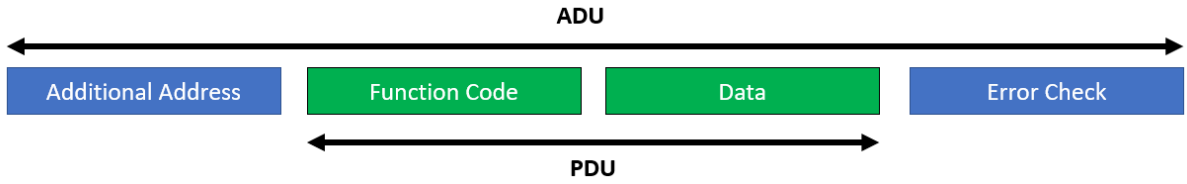

Figure 7. ADU & PDU [34]

TCP/IP refers to the Transmission Control Protocol and Internet Protocol. These

protocols allow data to be exchanged between computers. TCP ensures that all packets of data are received correctly, while IP makes sure that messages are correctly addressed and routed. Modbus TCP/IP combines a physical network (Ethernet), with a networking standard (TCP/IP), and a standard method of representing data (Modbus as the application protocol).

In Modbus TCP/IP, the client that initiates the transaction builds what is called a MODBUS Application Data Unit. This unit uses a header called the MBAP (MODBUS Application Protocol) to identify itself when is used on TCP/IP layers. Modbus TCP/IP Application Data Unit consists of a 7-byte header, and the protocol data unit (function code + data). The PDU is embedded into the data field of a standard TCP frame and sent via TCP to system port 502, which is specifically reserved for Modbus applications. Modbus TCP/IP clients and servers listen and receive Modbus data via port 502.

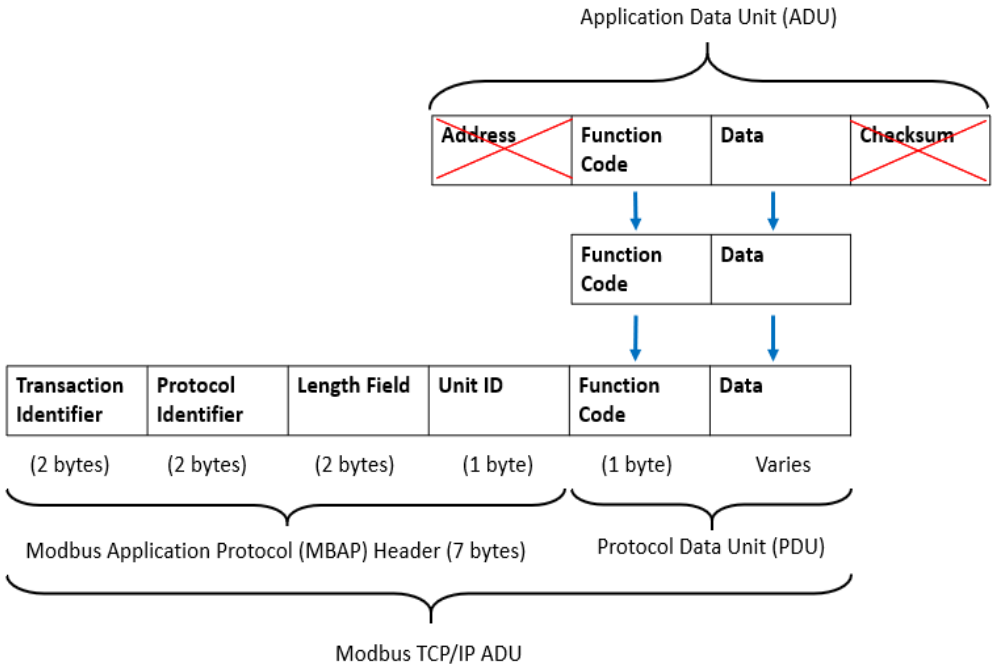

Figure 8. Difference between a MBAP and a ADU [34]

As shown in Figure 8, the MBAP header consists of a transaction identifier, protocol identifier, length field, and unit identifier:

- *Transaction Identifier* (2 bytes). This field has the purpose of identifying the response or request. Used for transaction pairing.
- *Protocol Identifier* (2 bytes). Used to identify the protocol used. Always 0 for Modbus.
- *Length* (2 bytes). Declares the number of followed bytes.
- *Unit Identifier* (1 byte). Identifies a remote slave connected on a serial line or other buses.

With Modbus TCP/IP, a Modbus server is addressed using its IP address. When a Modbus client wants to send a message to a remote Modbus server, it opens a connection with remote port 502. As soon as a connection is established, the same connection can be used to transfer user data in either direction between clients or servers.

The Data Link Layer specification for Modbus TCP/IP uses the CSMA/CD protocol (Carrier Sense Multiple Access w/ Collision Detection) to arbitrate access to the shared Ethernet medium. With CSMA/CD, any network device can try to send a data frame at any time, but each device will first try to sense whether the line is idle and available for use.

The following figure represents a MODBUS TCP/IP communication session between a client and the server, which uses Berkeley Software Distribution (BSD) socket interface to manage TCP connections. As a note, the document [34] remarks that BSD is not the only type of interface for performance issues.

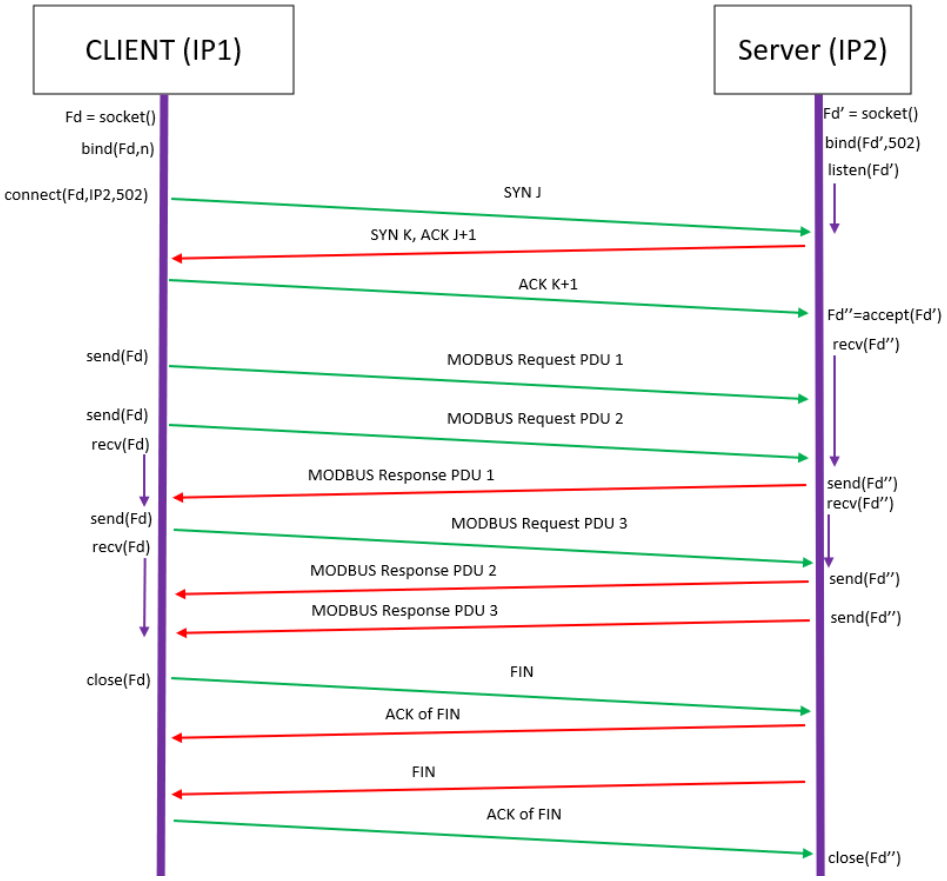

Figure 9. Typical Modbus TCP/IP communication session

The communication session as displayed in Figure 9, begins with the application on both sides using the socket() function. The socket() function creates a virtual socket (endpoint of communication). The bind() function binds a port number to a socket. The server always uses port 502. Once the sockets have a port number associated, the client uses the function connect() using as parameters the socket, the server IP address, and the port number. The connect() function is used to begin the connection sending an SYN packet to the server. At this moment, the server uses the function listen() to receive the SYN and immediately responds. Once the client has acknowledge the response from the server, the server uses the accept() function to complete the connection. After this procedure, both server and client can begin the transfer of

data through the functions recv() and send(). An advantage of this protocol is that the client can send as multiple requests as desired without having to wait for a response to each request. Once all the requests have been responded, to end the session, the client must use the close() function and wait for the acknowledge from the server. Once the server has sent its ACK packet, the server will also use the close() function and wait for the client's ACK packet to finally end the communication session.

2.5 G3 Power Line Communications (PLC)

Powerline communication is a technique that uses the existing powerlines to transmit high speed data and establishes a direct connection with the meter [44]. This protocol was designed to overcome high interferences and collisions for frequencies below 500 kHz in the hostile environment of the power lines and has been successfully implemented in urban areas where other solutions struggle to meet the utility needs [3]. To overcome the hostility, the standard uses an orthogonal frequency division multiplexing (OFDM) technique to increase the efficiency when using all the available bandwidth. Because of the noise, interference and other factors, a robust communication is only possible through the application of advanced channel coding techniques [37]. Authors in article [45] perform a study of G3 PLC implementation to demonstrate that the use of the encoder/decoder, Interleaver, and the modulator, can be effectively used to overcome narrowband interferences. Yet, to use this communication protocol, smart devices must incorporate PLC technology in their hardware. Another concern about the powerline was the effect over the meters in regards of accuracy in their metrology and communication ability. Fortunately, the author in [46] demonstrated that PLC signals do not provide a negative influence over the meter capabilities.

Article on [37] explains all the details related to the protocol specification. Since the power line communication medium is not as suitable as the medium used for the previous protocols, the use of more processes is required before sending data into the communication line which include the use of OFDM. The following figure represents the diagram followed by G3 PLC for the manipulation of data.

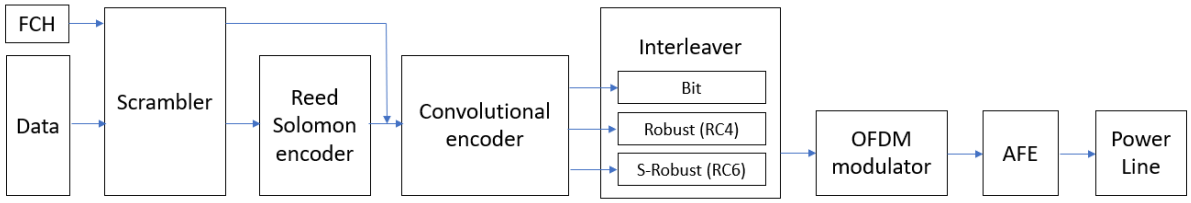

Figure 10. G3 PLC protocol. Data is manipulated through different processes before being sent through the power line [37].

Except for the FCH (Frame Control Header), Data, and Power Line diagram blocks from Figure 10, all other blocks perform a manipulation of data essential for the standard. The first two blocks in the G3 PLC diagram are the data with its FCH. Before the data is sent to the scrambler, it gets structured in frames. This structure can be of two types:

1. Typical. Each frame begins with a preamble used for synchronization and detection in addition to automatic gain control adaptation. The preamble is followed by the frame control header (FCH) which contains control information to demodulate the data frame.

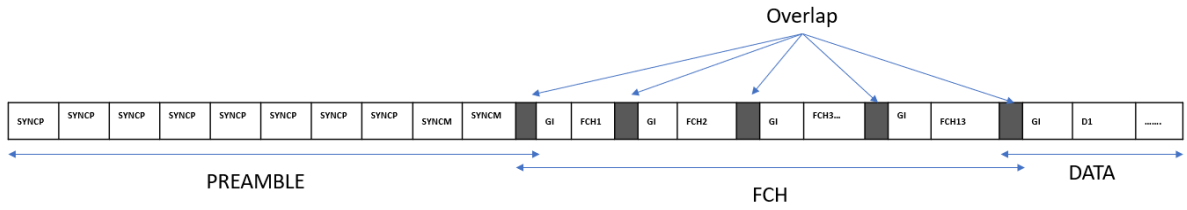

Figure 11. G3 PLC Typical data frame [37].

2. ACK/NACK. It only consists of the preamble and the frame control header. Since the frame is used only for acknowledgment purposes, it does not need to contain data fields.

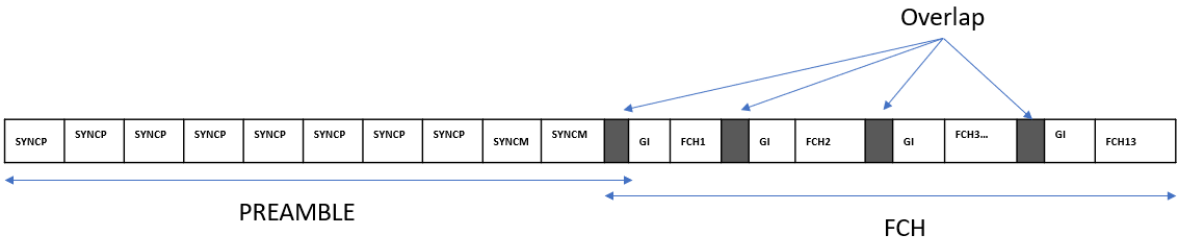

Figure 12. G3 PLC ACK/NACK data frame structure [37].

For both cases, the frame control header is protected with CRC5 and CRC8 depending on band plan:

CRC5: $G(x) = x^5 + x^2 + 1$ for CENELEC Band plan

CRC8: $G(x) = x^8 + x^2 + x + 1$ for FCC Band plan

The data to transport in the physical frames is provided by the upper layers as a byte stream and it is read with the most significant bit first into the scrambler as seen in Figure 11. The data scrambler gives the data a random distribution using the generator polynomial

$S(x) = x^7 \oplus x^4 \oplus 1$

As shown in Figure 10, once the frame passes through the scrambler, it continues through the Reed Solomon encoder, which is used to correct errors by adding redundancy to the original data. The convolutional encoder is another type of correction code that can correct errors by adding redundancy to the data stream. Hence the convolutional and the Reed Solomon encoder provide redundancy bits allowing the receiver to recover lost bits caused by background and impulsive noise. The Interleaver helps the data to protect against two types of errors:

1. Burst: corrupts a few consecutive OFDM symbols.

2. Frequency deep fade: corrupts a few adjacent frequencies for many OFDM symbols.

Once the data has passed the Interleaver block, it enters the OFDM modulator. The Orthogonal Frequency Division Multiplexing is a modulation technique that uses many orthogonal subchannels to transmit data. It splits the information into several subchannels allowing an optimal use of the available spectrum. The OFDM addresses the following objectives:

1. Creates a robust communication for extremely harsh power line channels.

2. Provides a minimum of 20kbps effective data rate in the normal mode of operation.

3.Ability to notch selected frequencies, allowing the cohabitation with S-FSK narrow band communication.

4. Dynamic tone adoption capability to select frequencies on the channel that do not have major interference.

The following figure provides a general representation of the physical frame (PHY frame), which is the data packet after being manipulated through the required processes before being sent to the power line.

Figure 13. G3 PLC general representation.

G3 PLC defines standards only for layers one and two of the OSI model. Messaging exchange between the physical layer and the data link layer begin with the receipt of a data or acknowledge request package (PD-DATA.request or PD-ACK.request). Once the packet is received, the end that received must reply with a confirmation packet (PD-DATA.confirm or PD-ACK.confirm) that contains a status (success, busy, failed).

For the case of the data link layer, the specification is subdivided in two sublayers: MAC sublayer, and the adaptation sublayer. The channel access in the MAC sublayer uses the carrier sense multiple access with collision avoidance (CSMA/CA). MAC sublayer deals with the necessary fields to make the transmission successful between the data link layer and the physical layer, while the adaptation sublayer helps with the interface between upper layers in the OSI model with the data link layer. In article [37], the author provides a chart that resembles a complete messaging sequence between two ends in the system. Figure 14 displays the messaging sequence.

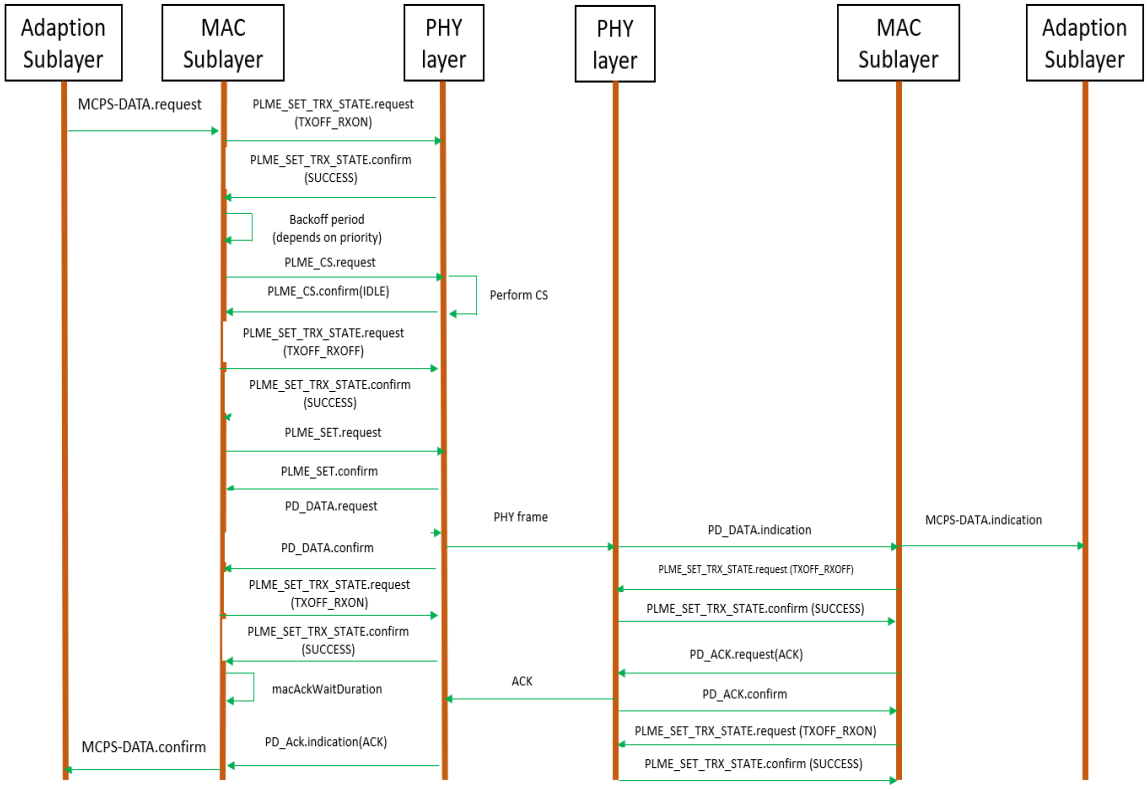

Figure 14. G3 PLC communication session between two end devices involving both first and second OSI layers [37].

Table 5 describes the commands used in Figure 14.

Table 5. G3 PLC commands used for a communication session. There are more defined in [37].

COMMAND	**DESCRIPTION**
MCPS-DATA.request	Request transmission of data to the MAC sublayer
MCPS-DATA.confirm	Confirms transmission of data to the Adaptation sublayer.
PLME_SET_TRX_STATE.request (TXOFF_RXON)	Requests the PHY to change the state of the receiver (ON) and turns off the transmitter.
PLME_SET_TRX_STATE.confirm (SUCCESS)	Confirms the PHY changing state, SUCCESS meaning that both the Receiver and the Transmitter are set.
PLME_CS.request	Requests the PHY to get media status using carrier sense.
PLME_CS.confirm	Reports media status

Table 5, continued.

PLME_SET_TRX_STATE.request(TXON_RXOFF)	Requests the PHY to change the state of the transmitter (ON) and turns off the receiver.
PLME_CS.request	Request changes in the configuration from the PHY.
PLME_SET.confirm	Confirms the configuration on the PHY
PD_DATA.request	Requests the transmission of a MAC protocol data unit (MPDU) to the PHY
PD_DATA.confirm	Confirms the end of the transmission of an MPDU.
macAckWaitDuration	Duration of acknowledgement in microseconds
PD_Ack.indication(ACK)	Indicates the reception of the ACK frame from the PHY to the local MAC sublayer entity.
PD_DATA.indication	Indicates the transfer of a MPDU from the PHY to the local MAC sublayer.
PD_ACK.request(ACK)	Requests to send an ACK frame to the PHY from the MAC sublayer.
PD_ACK.confirm	Confirms the end of the transmission of an ACK packet.
MCPS-DATA.indication	Indicates the reception of data from the MAC sublayer to the adaptation.

Beside the specifications for the physical and data link layers, G3 PLC protocol also defines its security procedures. First, an end device must be identified and pass through an authentication procedure to access the network. This is achieved based on two parameters:

-An address defined in IEEE 802.2001.

-A 128-bit shared key between the end user and an authentication server, which is used as a credential during the authentication process.

The authentication and identification processes are activated when an end device restarts and at any time depending on the security policy in place.

Confidentiality and integrity are insured at two different levels: MAC level and EAP-PSK level. At the MAC level, ciphering is used when delivering any frame between nodes in

the network. MAC frames are encrypted and decrypted at every hop using a group master key. At the EAP-PSK level, confidentiality and integrity are protected according to IETF RFC 4764, where the service is known as protected channel (PCHANNEL) between the EAP server and any peer.

Taking into consideration that DoS attacks are usually difficult to prevent, for the case of G3 PLC, the impact of a DoS would only affect a small area. This is achieved by preventing unauthenticated devices accessing the network and not having malicious actions on routing.

G3 PLC prefers the use of pre-shared key EAP to achieve the security that it offers. It consists of a 128-bit group master key generated by the EAP server and delivered to all peers via the EAP-PSK protected channel (PCHANNEL). EAP-PSK key hierarchy overview is detailed in the protocol.

CHAPTER III

SIMULATING A SMART METERING COMMUNICATION SYSTEM

For an accurate smart metering system assimilation, the setup consisted of three smart devices (smart meters), a computer to monitor the system, a small-scale electrical setup, and energy loads. For reference, all meters were setup in a fashion to always measure the same load. Each meter represents either a business or a home and report their consumption in real time. The monitoring computer has access to all information stored in meters as long as all devices are connected to the grid. The types of communication involved in our experiments were ethernet and optical communication. Authors in [47] discussed ethernet-based infrastructures in smart grids and how they are not widely implemented due to the high costs in equipment and challenging redeployments during emergencies. However, their high security has kept ethernet smart grids an option in today's implementations [2]. According to most sources, the most famous smart meter manufacturing companies are:

- Landis+Gyr
- Itron
- Aclara
- Elster Group
- Sensus

Because of their capability to communicate using ethernet technology, this study was focused on three meters:

- Landis+Gyr S4x Ethernet
- General Electric EPM 6100
- General Electric EPM 7000

3.1 Landis+Gyr S4x Ethernet

Figure 15. Landis+Gyr E650 S4x ethernet meter [48].

Document [48] describes E650 S4x meters as designed to be the foundation for a complete metering infrastructure. They can yield a complete package for accessing real-time voltage, current, and load data monitoring, extensive user-defined event and tamper alerts, data and graphical load analysis capability, and vector diagrams. Communications boards, such as RS485, RS232, and Ethernet boards can be supplied with the meter from the factory or added to a meter in the field. An optical port (ANSI Type II) is provided for programming and recording meter data. Some characteristics of E650 S4x Ethernet meter are:

- It offers a Secure web portal access to individual meters

- Allows access to up-to-the minute information including status, meter information, meter reads, instantaneous readings, and billing data
- Supports either Dynamic or Static IP addressing modes through an under the glass RJ-45 Ethernet communication module.
- Supports Secure Shell (SSH) cryptographic network protocol using RSA encryption for secure connectivity without the bandwidth limitations of wireless networks

GENERAL SPECIFICATIONS	
ANSI C12.19 Standard Protocol	
Wired RJ-45 Ethernet Connection	
Interface with PrimeStone PrimeRead Head-End Software	
INTERNET INTERFACE STANDARDS	
Support	Dynamic (DHCP) or Static Addressing
	Secure Shell (SSH) (using RSA Encryption)
	Synchronous Time (via NTP Server)
	IPv6 Protocol
TEMPERATURE	
Operating Temperature	-25°C to +85°C
VOLTAGE	
Nominal Voltage (Standard Power Supply)	120-480V 2 and 3 Wire - 120, 208, 240, 277, 347, 480 4 Wire - 120/208, 240/416, 277/480, 347/600
Operating Voltage (Standard Power Supply)	98 to 552 VAC (line to neutral) Auto Ranging Power Supply
Frequency	50 or 60Hz ± 5%
Humidity	Less than or equal to 95% relative humidity, non-condensing
AVAILABLE FORMS	
Self-Contained S-Base	2S, 12S, 14/15/16/17S, 25S, 1S, 2SE, 12SE, 14/15/16/17SE, 25SE
Transformer Rated S-Base	3S, 3SC, 4S, 8/9S, 45S, 36S, 29S
APPLICABLE STANDARDS	
ANSI C12.1 for Electric Meters	
ANSI C12.19 Standard Protocol	
LAPEM GWH00-05 & 48 Certified, 9S and 16S only	

Figure 16. S4x Ethernet specifications [48].

Landis+Gyr offers a web portal that can be access by only entering the meter assigned IP address into the web browser of preference. The web page requires a username and password that will have to be provided by the utility company. Once the user logs in, the website will display a menu of options that contain the desired information from the meter, such as the energy consumed, the voltage and current being read, the frequency detected, MAC address, etc.

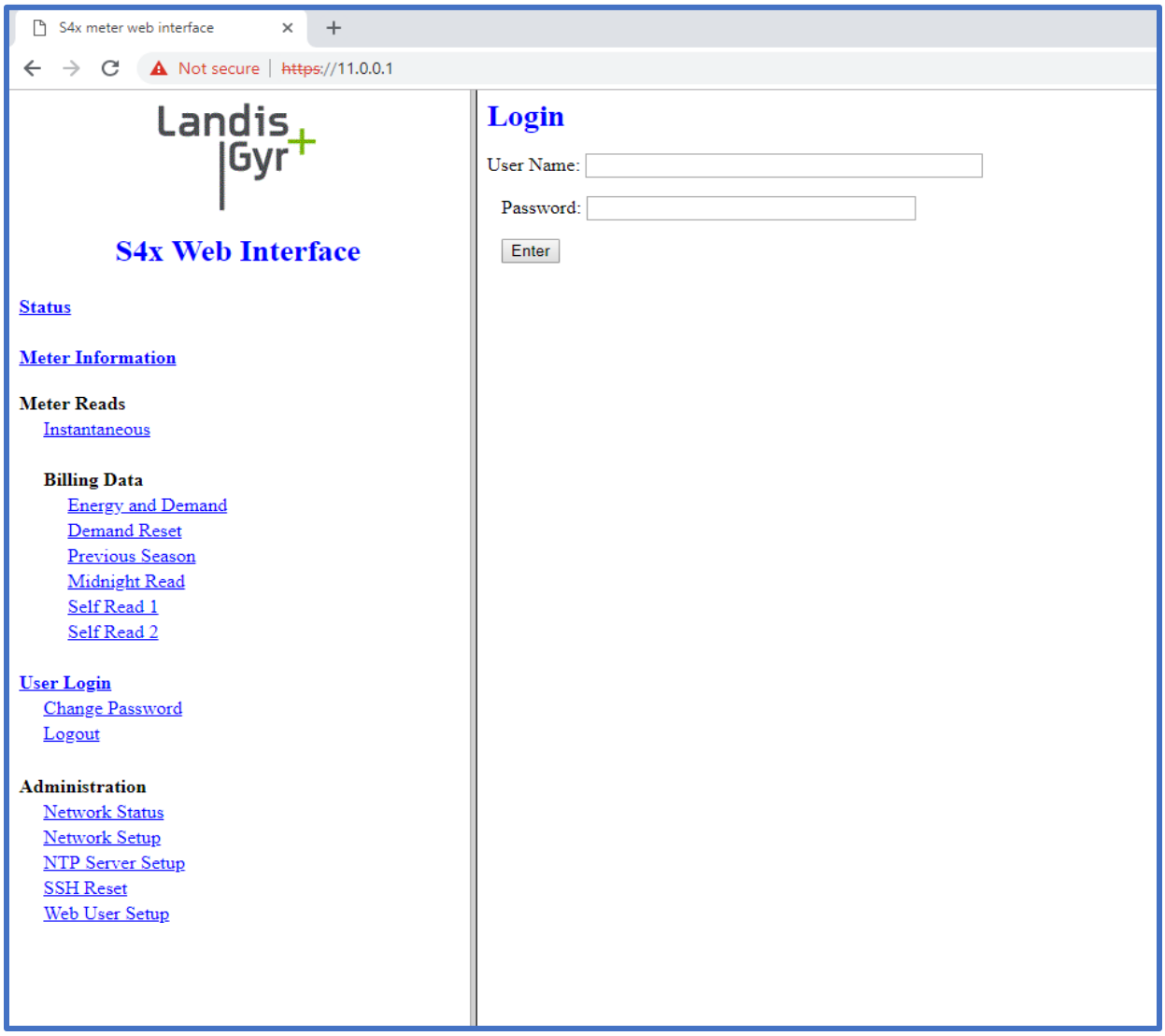

Figure 17. S4x Ethernet web portal start page.

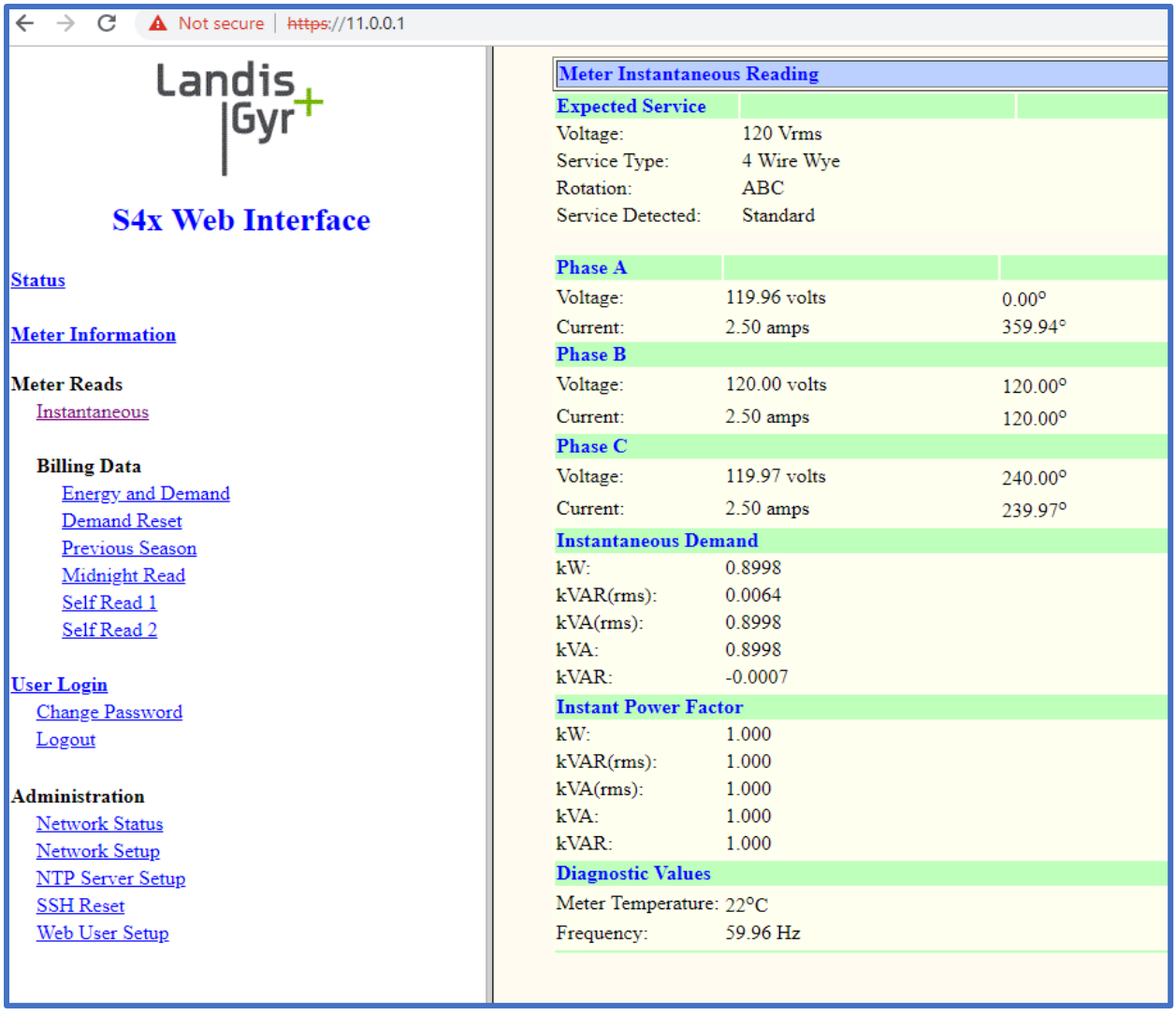

Figure 18. Web portal after selecting instantaneous readings option.

3.2 Landis+Gyr Deployment.

Unlike the rest of the meters produced by L+G, E650 S4x Ethernet meters are relatively new in the market. Most of metering solutions offered by Landis+Gyr communicate using radio technology when they are deployed in the field. The most common solution in L+G is called Gridstream. This works in the form of a mesh network where each device can access the transmitter and receiver. Gridstream consists mainly of the following elements: energy loads,

smart meters, network routers, data collectors, and the command center software. Energy loads are any device connected to the electrical grid of the home, business, or industry that consumes electrical power. All meters are interconnected and share their information until reaching the nearest data collector. If a data packet must be sent, the meter, knowing the location of the nearest data collector, will send the data though the minimum number of meters required and network routers (this is finding the shortest path). Network routers provide a powerful hub for moving information through the network and to another network router. The data collector is the link between the smart devices and the head-end software used by the utility company to process all the data from all meters. The command center software is the interface between the network and the multiple data management tools and applications used by the utility company. The following diagram represents in simple manner how the Gridstream solution works today:

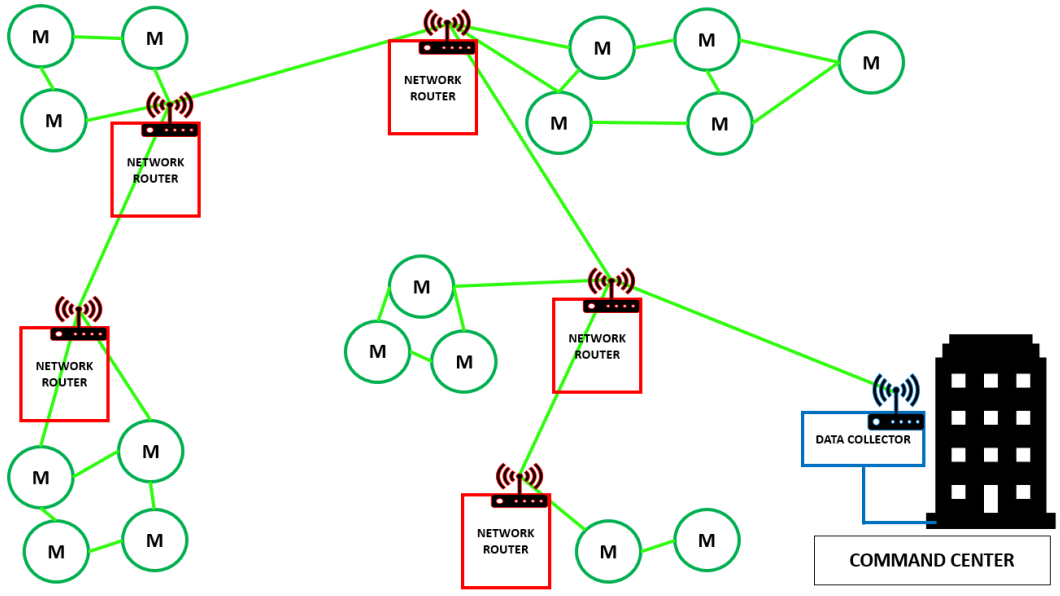

Figure 19. Landis+Gyr Gridstream solution. It is the most common form of communication deployed on Landis+Gyr meters.

However, for the case of E650 S4x Ethernet meters, the Gridstream solution does not apply. There reason is the communication medium. Gridstream is based on radio transmission

technologies, while Ethernet, like the name implies, communicates using ethernet technology. Therefore, its deployment and communication structure are completely different. The way the Ethernet solution works consists of the following elements: energy loads, smart meters, networking devices, modems, and the cloud. All energy loads must report the consumption to the smart meter. A networking device permits the availability of the meter information into a local area network. The modem allows the meter to send its collected information into the cloud, where it can be accessed remotely from a far distance by other intended users.

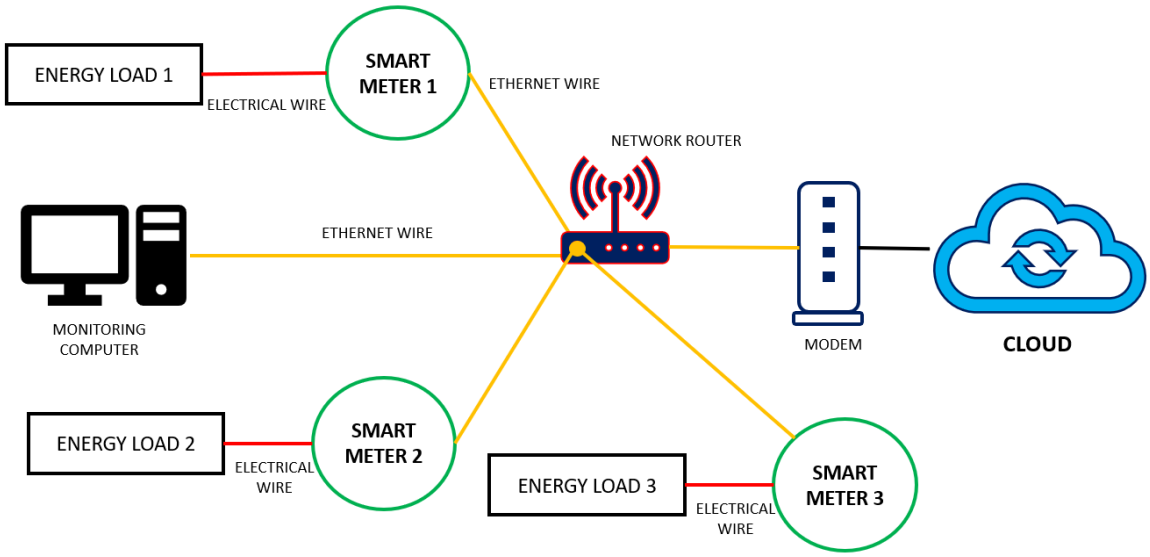

Figure 20. S4x Ethernet field deployment example. This particular example involves three meters in a single location. Usually only one meter is used per location.

The grid begins by having all energy consumption read by the smart meter, who afterwards, sends the data through an ethernet cable in the form of a digital signal to a networking device (for example, routers). Routers are devices capable of taking the digital signal delivered from the modem and retransmit it to multiple devices using ethernet cables or wi-fi technology. Thanks to routers or similar networking devices, a local area network can be

built, and users connected to the local area network may access the meter information. For users out of the LAN, the router will take the data from the meter and retransmit it to the modem using the same communication medium. The modem is a networking device capable of receiving a digital signal and converts it into an analog signal. Once the modem has finished converting the digital signal into an analog signal (demodulation), it sends the analog signal to the internet service provider (cloud). Having the information in the cloud, users outside the LAN could access it by retrieving the analog signal with this information and modulate it with a second modem. As already mentioned, the service that Landis+Gyr S4x Ethernet meters offers consists of letting the user access all the concerning information from the meter with the use of a web portal. The user can be able to access information such as the total watthour recorded, the actual voltage, current and frequency that the meter reads, and other billing data.

3.3 General Electric EPM 6100

Figure 21. General Electric's EPM 6100 [49]

General Electric's document [49] describes EPM 6100 as a multifunction meter that allow users to monitor and manage energy usage within factories, businesses, and across

campuses. It features ANSI C12.20 (0.2% class) accuracy, RS485, RJ45 Ethernet or IEEE 802.11 Wi-Fi communications. EPM 6100's installation is practical, easy to use, and General Electric provides a software application that allows detailed studies on energy management. For this thesis, the communication aspect studied in EPM 6100 is the ethernet communication system.

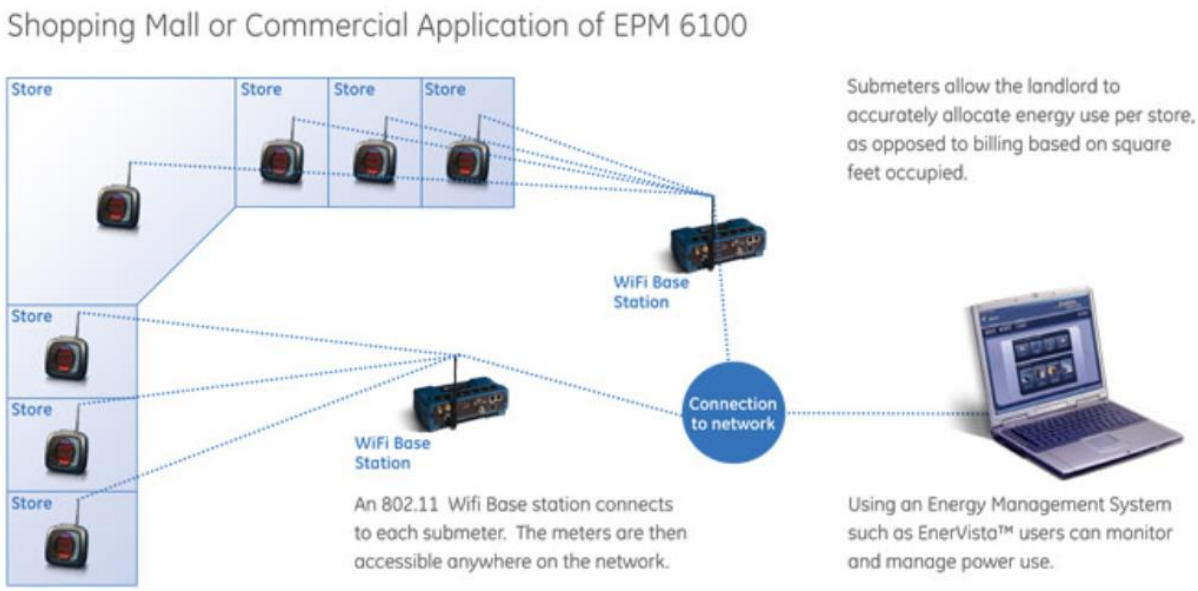

Figure 22. General Electric's sample application of EPM 6100 smart meters [49].

3.4 General Electric EPM 7000

General Electric's document [50] describes EPM 7000 as a meter capable of measuring three-phase systems with waveform capture (512 samples/cycle) and data logging. The meter supports Ethernet communication (100 BaseT), and it can perform energy measurements with 0.2% accuracy. EPM 7000 is a useful tool capable of supporting disturbance recording and power quality studies. Like with EPM 6100, General Electric provides a software application that allows users to manage and study the energy recorded by the meter, plus, like with the S4x

Ethernet meter, EPM 7000 also provides a web portal where the users can find the meter information.

Figure 23. General Electric's EPM 7000 [50]

3.5 Laboratory Setup

We built a smart metering system that complies with the basic idea of communication that ethernet grids used. For all our experiments, we used fans, light bulbs, and motors as loads. Given that we only required a local area network for our experiments, there was no need to get a modem. Hence, the most appropriate device to control the traffic of data was a network switch. Here is where the meters were connected on different ports, and on another port a computer was connected to monitor all the data gathered by the meter (this is the command center, or utility company). Therefore, our laboratory can be represented with the following diagram:

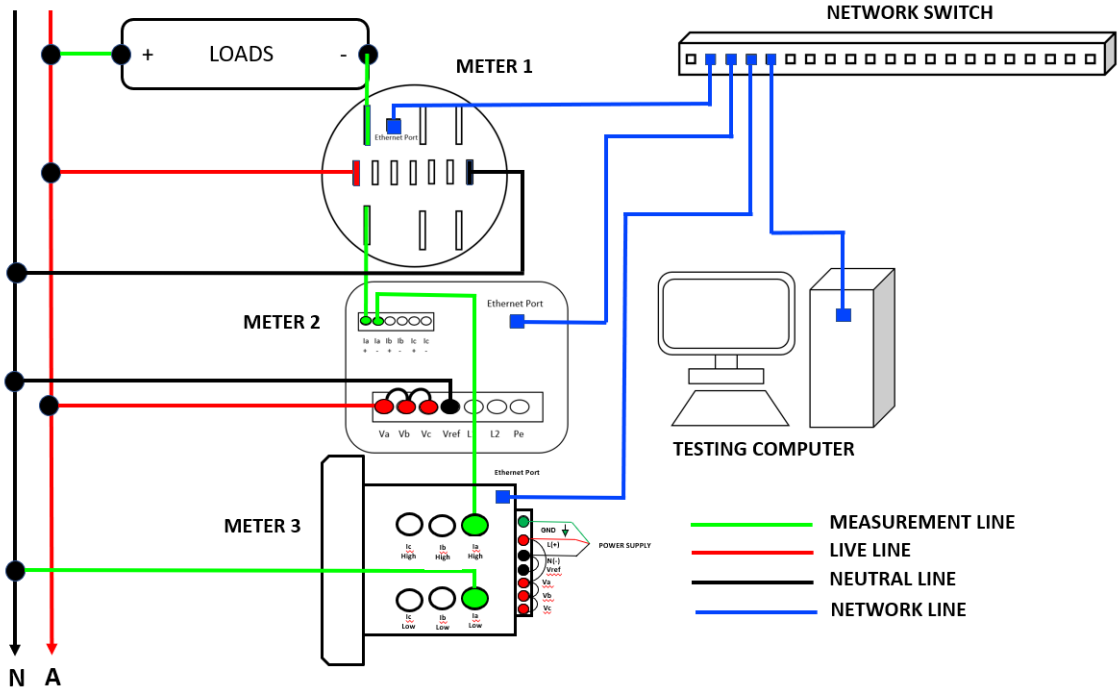

Figure 24. Ethernet-based smart grid system designed in the electrical engineering laboratory at the University of Texas Rio Grande Valley.

Even though network switches keep a table with all the devices' MAC addresses, the transportation of data is done using layers 2 and 3 of the OSI model. This, meaning that for every device connected to the grid, a different IP address was assigned.

Table 6. Smart meters used in the laboratory to create the smart grid.

Device	Manufacturing Company	Communication Technology	IP Address
Meter 1: S4x Ethernet	Landis+Gyr	Ethernet, Optical	192.168.1.12
Meter 2: EPM 6100	General Electric	Ethernet, Wi-Fi	192.168.1.11
Meter 3: EPM 7000	General Electric	Ethernet	192.168.1.15

Meters 1 and 3 have the capability of letting the user access a web portal to get the information recorded by the meter. Meter 2 comes with a specialized software provided by the manufacturing company to display all concerning information to the user.

3.6 AMT Monitor

Once having the communication networks and the electrical circuit setup ready. We had to make sure that we were recording the data properly. As already stated, for the case of the L+G meter, the manufacturing company offers a web portal to the utility company to check on the values recorded by the meter, this same portal was used by us, since we are simulating to be the operations center.

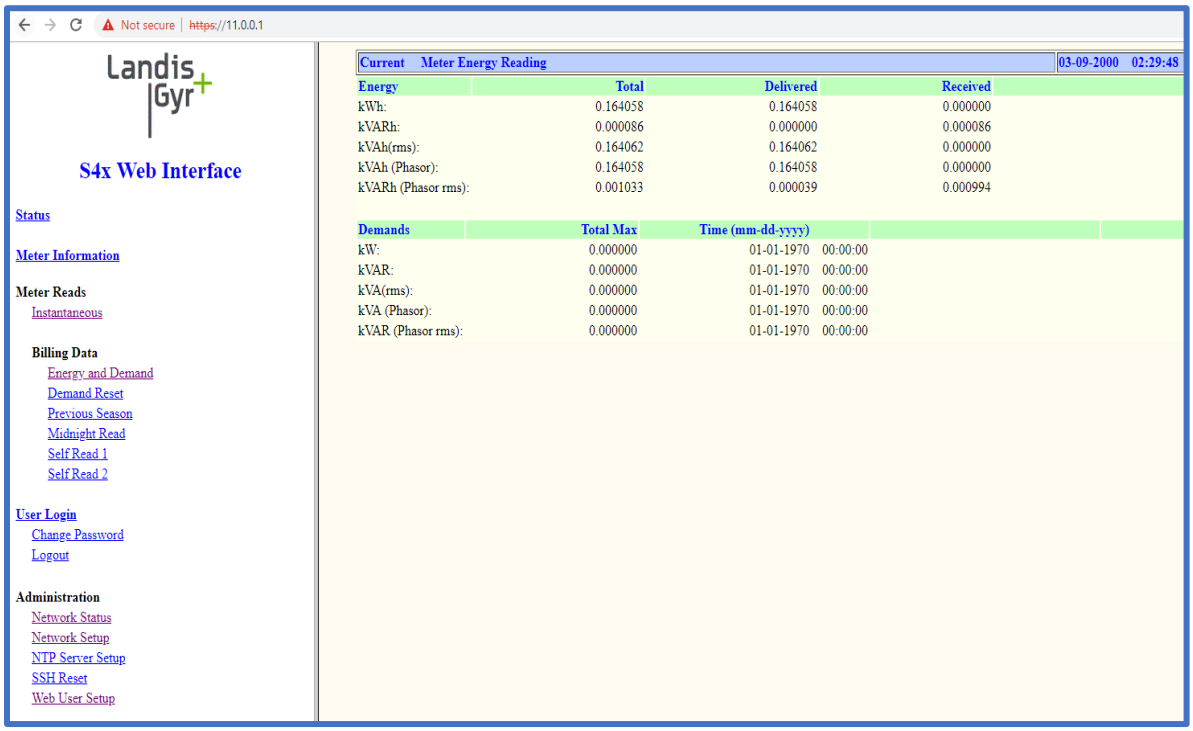

Figure 25. S4x Ethernet meter's web portal after selecting energy and demand from the billing data option.

However, our experiments would require long lasting times of even weeks, and our values had to be recorded per hour, minute, or even seconds. Therefore, a specialized software application was developed to make this job easier and human-error-free. This application was baptized with the name of Automatic Meter Transmission Monitor or AMT Monitor.

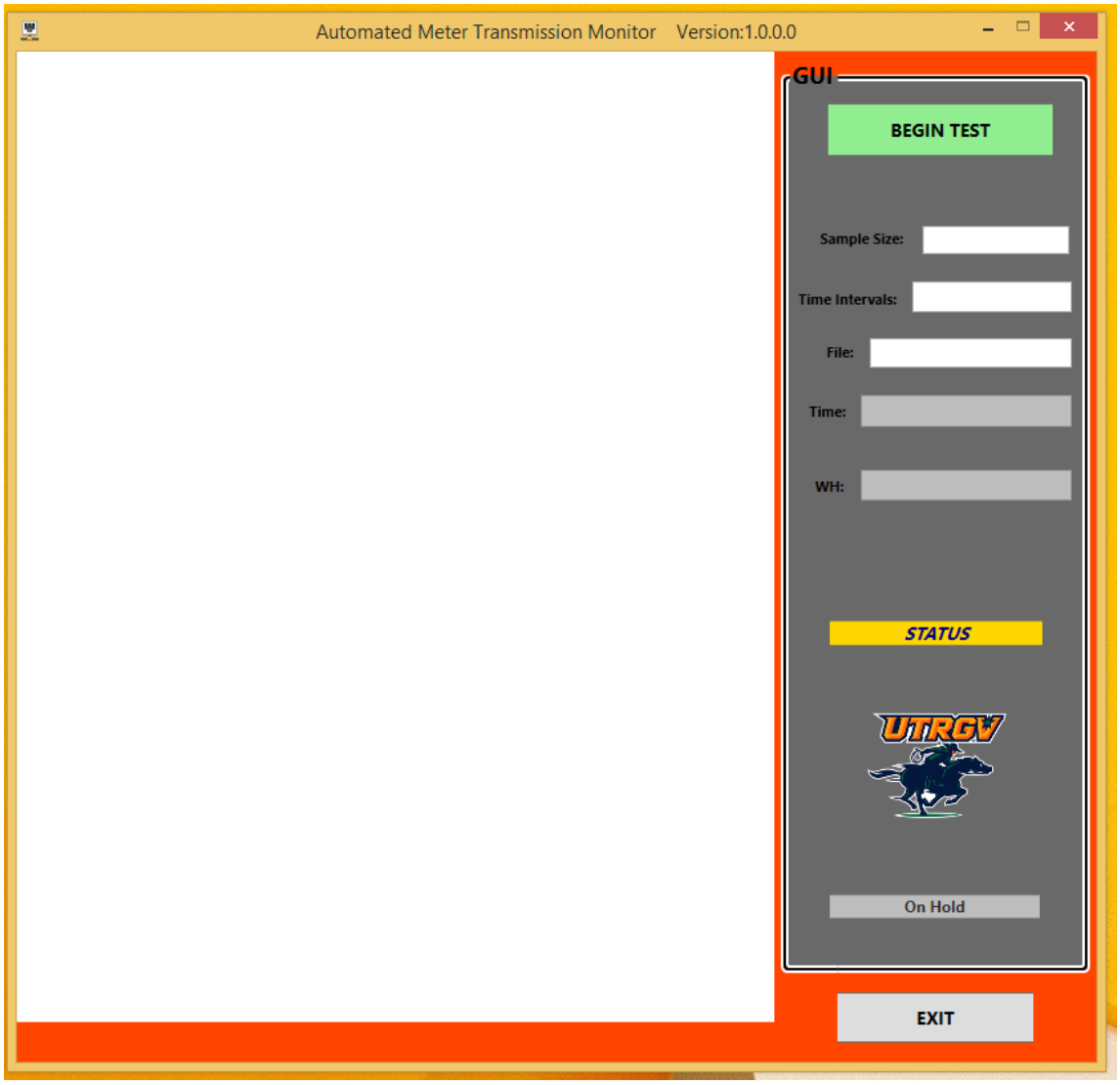

Figure 26. Automated Meter Transmission Monitor (AMT Monitor).

The development of AMT monitor became essential to this thesis as it provided critical information that revealed how the meter behaves regarding consumption and communication to the user. This software application was designed using Visual Studio in the .NET platform. The programming languages involved were C#, XAML, and HTML.

AMT monitor was designed to follow the following functioning diagram:

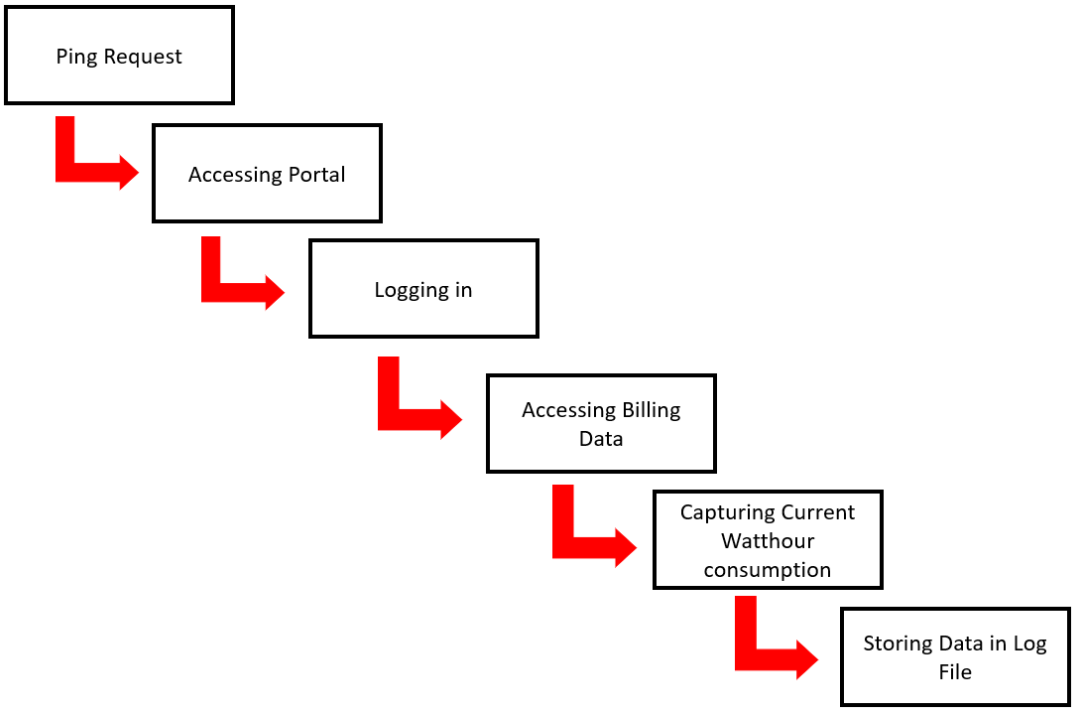

Figure 27. AMT Monitor process flow.

Before beginning the process, the user must enter three parameters:

- Sample size. Determines the number of readings that will be taken by the software.
- Time Interval. Determines the time that the software will take to read the information from the meter between samples. This time is set on seconds. Meaning that one reading per hour would require a parameter of 3600.
- File. This field will contain the name of the log file that the software will create after finishing the test. Log files are always stored in C:\temp. Once the software is installed, the user must manually create this folder, or the application will crash.

After setting the parameters correctly and starting the test, the software begins by sending a ping request to the meter. If successful, then the test proceeds. The next step is

accessing the web portal, followed by an automatic login, and it ends displaying the billing information. Once the billing information is displayed, AMT Monitor will fill the two remaining boxes in the window:

Time. Displays the time when the reading was taken.

WH. Displays the watthour recorded at the time. Units are in Kilo watthours.

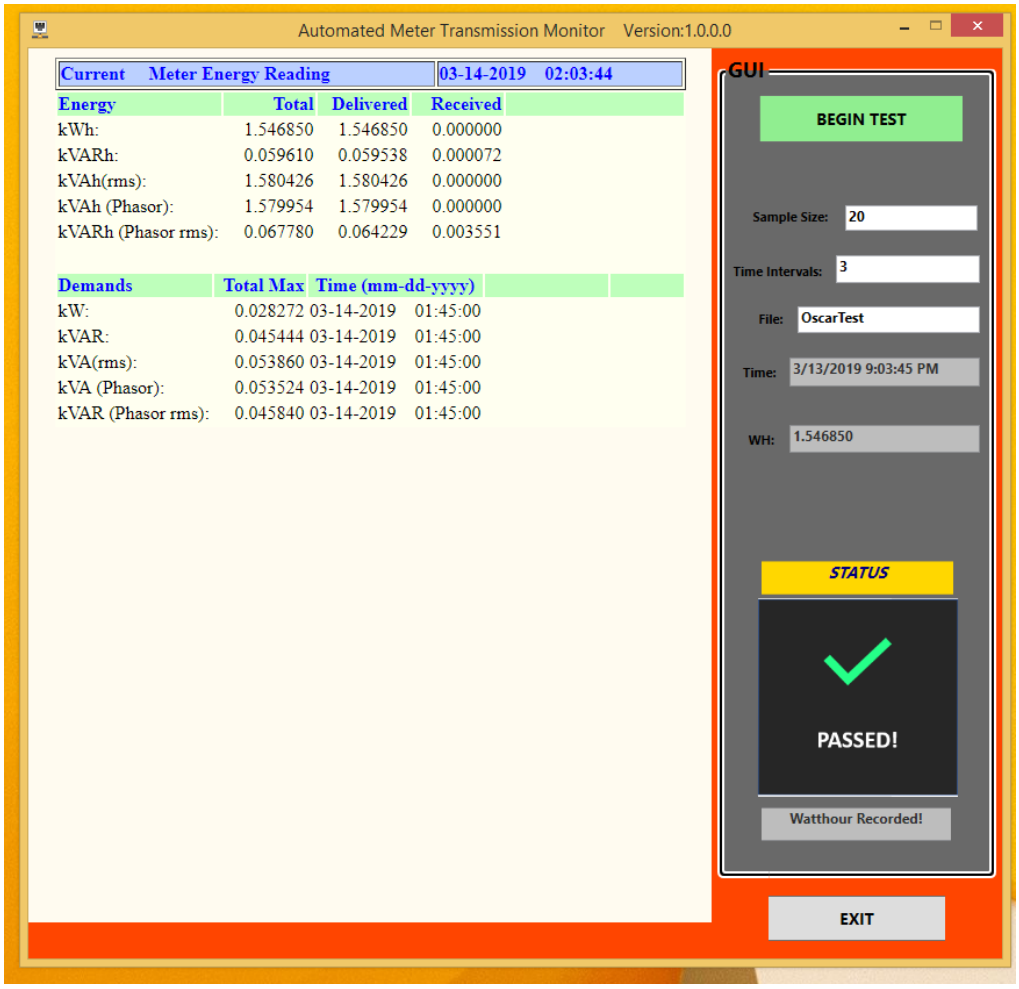

Figure 28. Successful execution of AMT Monitor.

After displaying the readings in the boxes, the test will repeat the same process as many times as indicated in the sample size field. Once the last test is done, the user can check all the readings in the log file created. The log file is a text file that contains the time and KWH of

every single sample taken during the test. As a note, the user does not have to wait until the whole test is done to access the log file, after the first reading, the user can access the log file at any time. This is done in case the user detects an irregularity during the test.

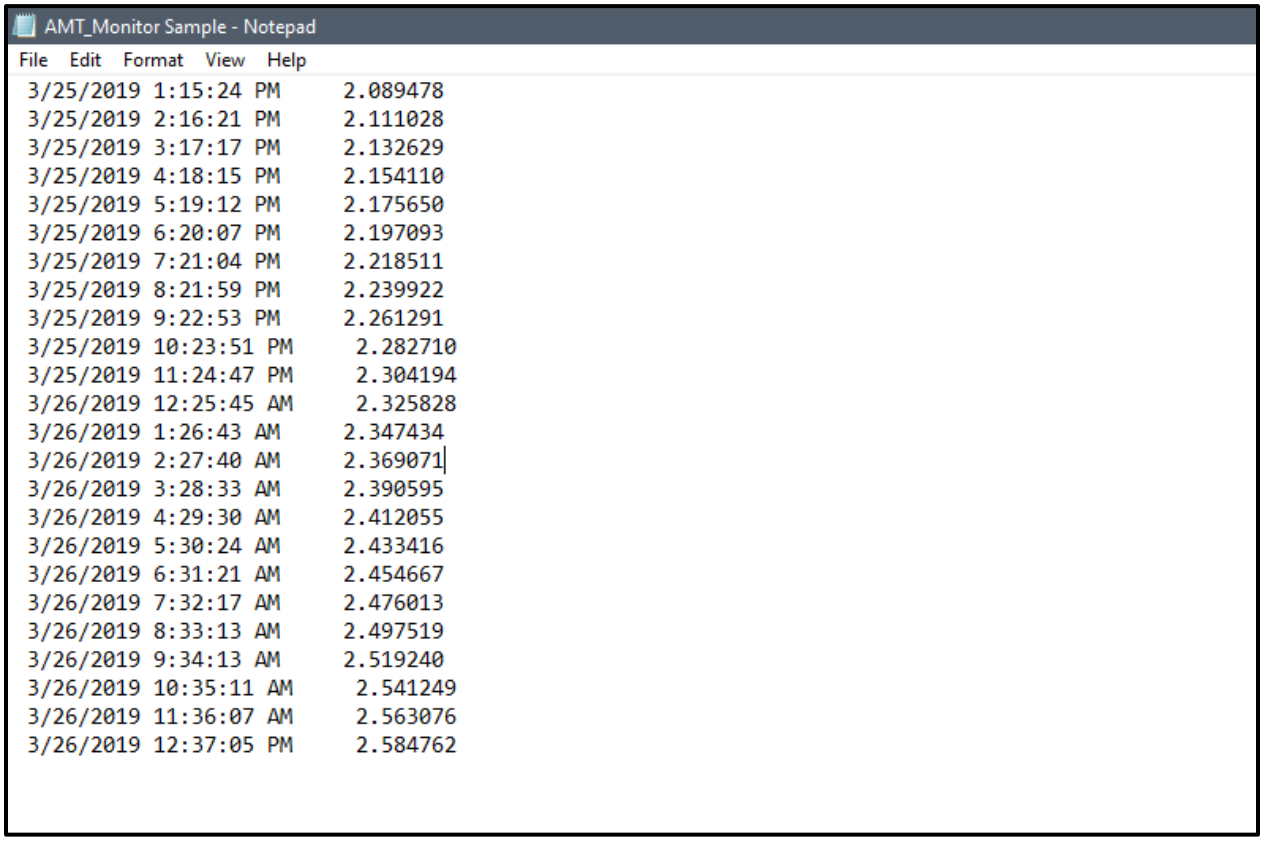

Figure 29. AMT Monitor log file sample.

Once the software was developed and the smart grid system was terminated, several tests were done until all the minor details were fixed. At the end, the system could have the meter recording data for as many days as desired and the software could take readings with a small probability of interruption of 1/73. This meaning that every reading had a failure probability of 1.34% Still, the results were satisfactory enough to proceed with the real experiments.

3.7 Performance Measurement

The final element to complete the laboratory is the attacking computer. To study the performance of an ethernet-based smart grid, a performance simulator was introduced to the systems as if it were one more element in the grid. The idea of this experiment was to attack the communication lines and record all the observable the effects.

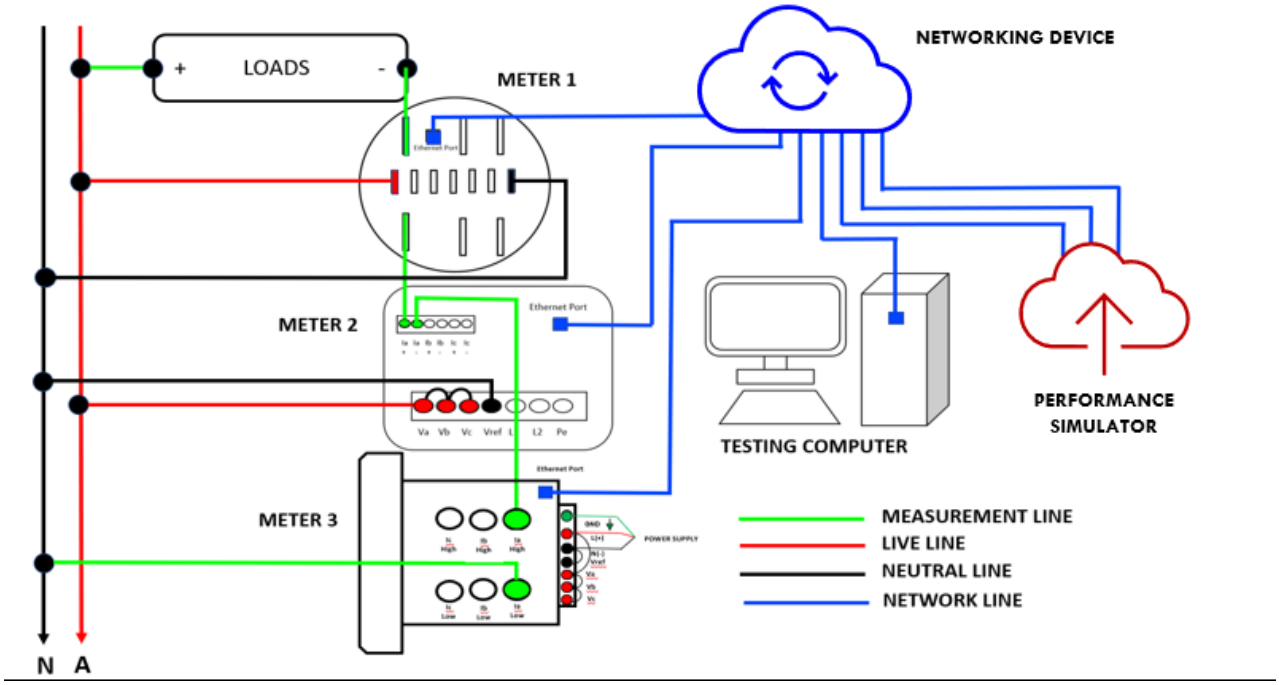

Figure 30. Complete (final) diagram of the performance laboratory.

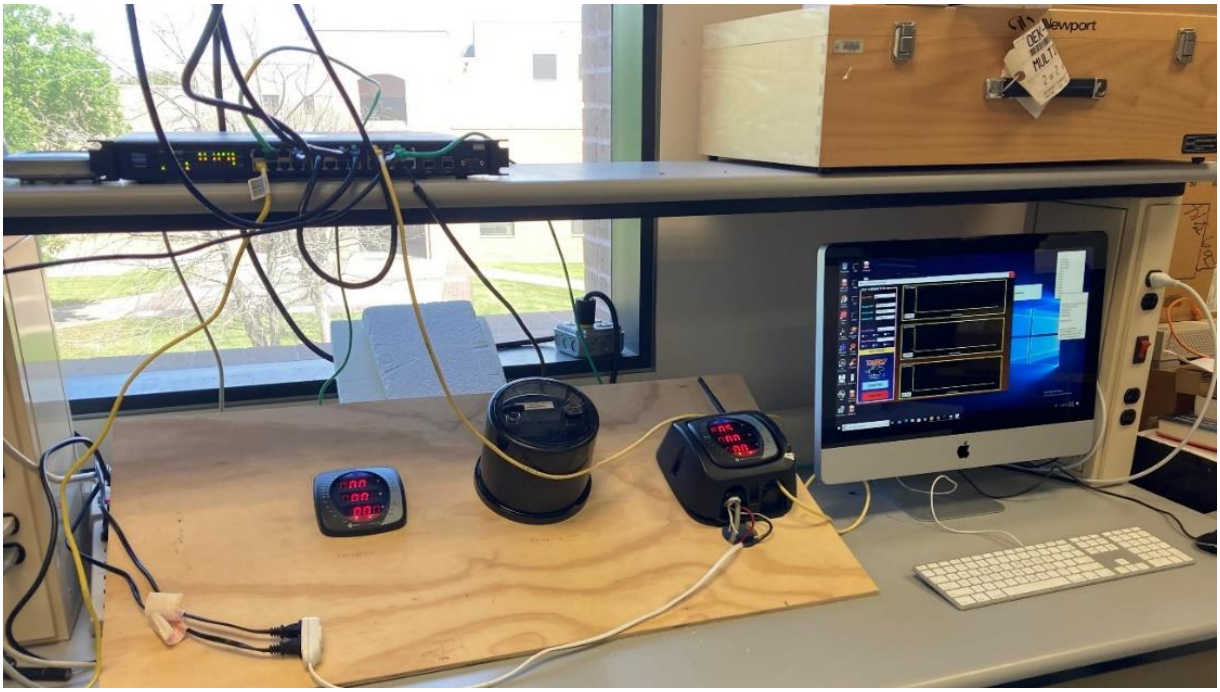

Figure 31. Photo of the performance laboratory setup at the University of Texas Rio Grande Valley.

CHAPTER IV

PERFORMANCE UNDER CYBERATTACKS

Smart meters can provide detailed information about how the user spends energy, billing data, and customized configurations. Furthermore, today's communication technology allows utility companies to remotely cut the power out of a facility or a home. All these new features can bring great advantages with the goal of optimizing energy, yet it can also bring risks in security of information. If an action performed by a third party ends up affecting any of the information security triad elements (Confidentiality, Integrity, Availability), it is considered a cyber-attack. Cyber-attacks are threads to any computer system, including smart grid systems. In November 2011, an attacker was able to gain access to the control system of an Illinois municipal water supplier and remotely disable operating equipment [51]. High reliability and availability are essential for energy management in smart grids [52]. For this work, a series of different attacks were analyzed to determine which ones could apply to the intended system. Taking into consideration that an attacker must force access to a wired system, like the one presented in this research, because of how easier is to secure it compared to wireless systems [52], this work's approach was not done to attempt violating specifically the meter security layers; but to evaluate the security of the smart grid system, which refers to the meters along with the communication medium and the monitoring software. Our experiments are similar to the ones performed in [53]. However, our performance simulator is a specialized tool that provides an ultra-high density testing platform supporting high bandwidth requirements of

large-scale application tests. Our tool would also let us control the stream of data used for testing. Hence, our results are different from [53] and are discussed in the following chapters.

4.1 Potential Cyber-Attacks on Smart Grids

The most common cyber-attacks that were considered for this research, which are described below, are DOS, ping floods, smurf attack, TCP/SYN attacks, and HTTP attacks.

4.1.1 DOS

Standing for Denial of Service, the goal of this type of attack is to make a machine or its resources unavailable to its user. There are different DOS attacks (some are below). Typically, DOS are accomplished by flooding the intended machine with dummy data packets that prevent the flow of traffic in the communication channel. Many sources like authors in [2] agree that DOS is one of the most dangerous attacks against AMI. These types of attacks risk the failure of the functionality when not detected and quarantined early enough. Although some security-enhancing works like key management schemes offered by the authors from [54] and [55] propose in AMI have been investigated and implemented, there has not been an ideal solution that can protect a smart metering system from a DOS attack.

4.1.2 Ping Flood

A ping is a simple data packet sent to a machine that requests a response. The purpose of this request is to ensure that the machine responding is available to communicate and displays the time taken for the response to arrive. In simple terms, a ping verifies availability and speed of communication between two devices. Ping floods are common denial of service attacks in which the attacking device saturates the target machine by sending an overwhelming number of

pings. The saturation occurs because for each ping send by the attacking device, the internet control messaging protocol (ICMP) indicates that the end machine will have to send a response. Since the number of requests and responses are significantly enormous, the network medium gets saturated consuming critical bandwidth and thus, communication becomes impossible until all the pings have been responded by the targeted device. Nevertheless, the attack will only become successful when the attacking device can use more bandwidth than the targeted device, only this way, the attacker will ensure to send more packets than the ones the victim can respond at the same time.

Figure 32. Ping flood progression.

4.1.3 Smurf Attack

Like the ping flood, a smurf attack is another type of DOS attack. In this case, a large number of Internet Control Message Protocol (ICMP) packets with the intended target's false IP are broadcast to a whole network using an IP broadcast address. By protocol, all the devices in the network receiving the ICMP packets will respond using response packets directed to the source address. In this attack, the source address is the victim's address. Therefore, depending on the number of devices in the network is how the attack will increase its severity.

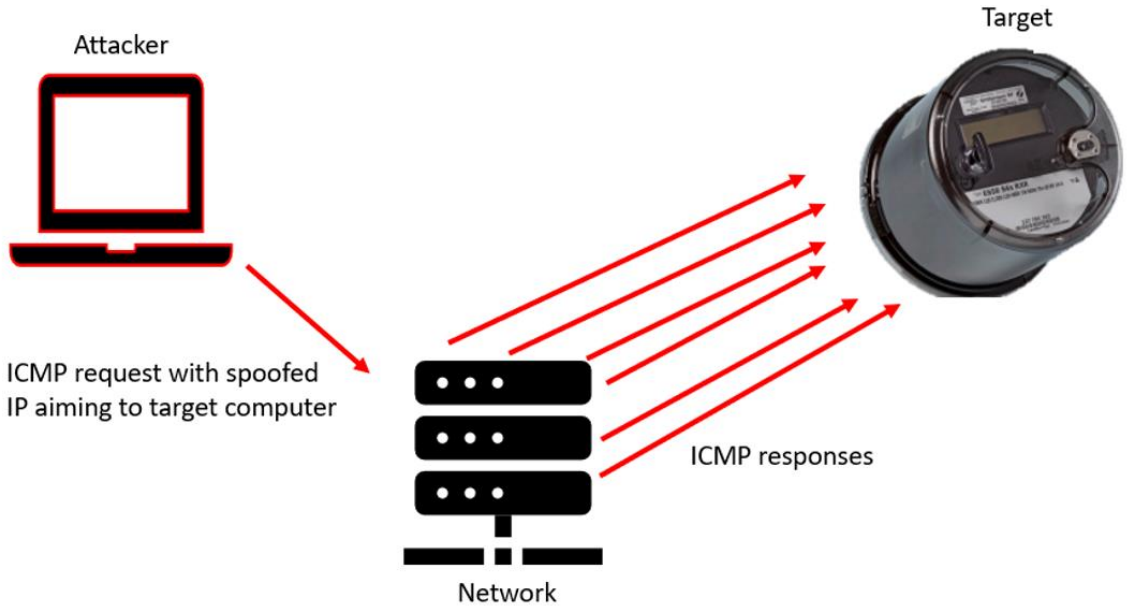

Figure 33. Smurf attack representation.

4.1.4 TCP/SYN Attack

This is another DOS type of attack. In this case, the attack focuses on the TCP three-way handshake feature to consume resources and saturate the communication network. In a regular communication session, a device sends a SYN (synchronized) message to another device to stablish communication. Once the intended device receives the SYN message, it acknowledges

it by replying with a SYN-ACK (synchronized-acknowledge) message. Finally, the third step of the establishment ends by having the initial device receiving the SYN-ACK message and responding with a final acknowledge message (ACK).

SYN flood attacks use this concept by having the attacker send multiple SYN packets to a targeted machine. The machine will receive all the different SYN packets as legitimate and will acknowledge every single one of them. Nevertheless, the attacker would not accept any of these packets, and therefore, will not send the final ACK packet to establish communication. The targeted machine will remain on wait because the connection will stay open until receiving the ACK message. Since the connection cannot be closed by the targeted machine, it will have to wait until the connection times out. However, just before the connection times out, the attacker will send another group of SYN packets causing the targeted machine to end up with connections half open. As the number of half open connections increase, the targeted machine will begin to lose its ability to establish connections with legitimate devices until it cannot establish a single connection.

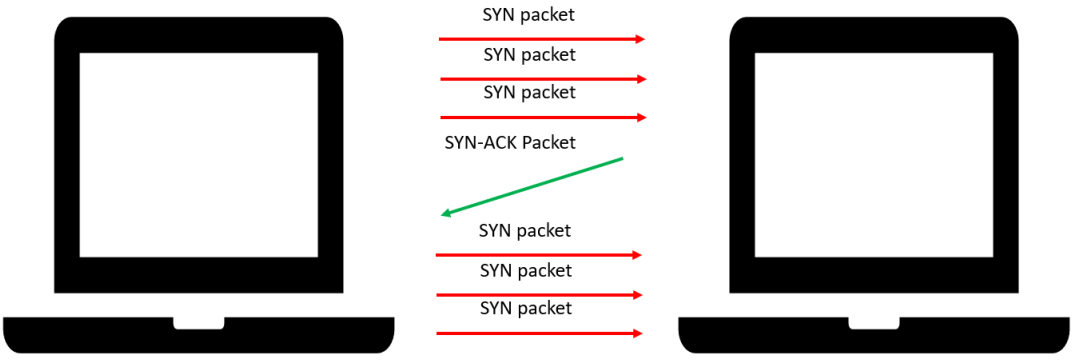

Figure 34. TCP/SYN Attack representation.

4.1.5 HTTP Attack

HTTP stands for Hypertext Transfer Protocol, and it is used to load web pages using hypertext links. Different from almost all the protocols already discussed in this work, HTTP works at the application layer. For this protocol, a device makes request to a server and waits for the server to response. To begin, the HTTP request consists of specifying HTTP version type, the URL, the HTTP method, request headers, and it ends with an optional body. The HTTP response is sent from the server to the requester device, the information varies depending on the request previously done. The HTTP response consists of a status code, headers, and the optional body. Like on previous attacks, HTTP flood attack is another type of DOS attack. The difference with this type of attack and ping flood is that it operates at the layer 7 of the OSI model. The attacker or attackers overwhelm a server with HTTP requests until it cannot respond anymore.

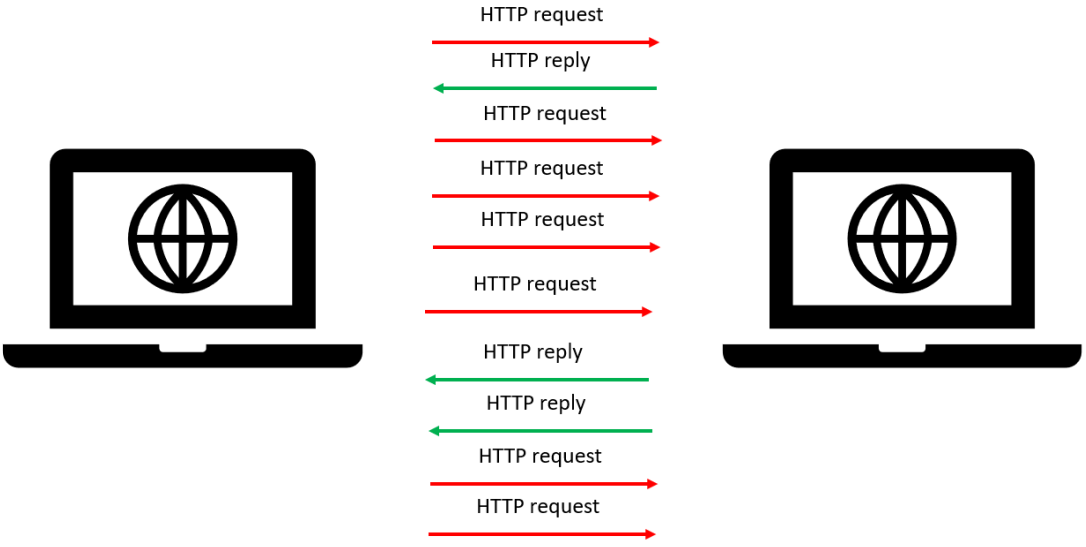

Figure 35. HTTP attack representation.

4.2 Experiment Setup

The experiments consisted of setting traffic loads directed at the three meters at the same time. Three different types of attacks were experimented: Ping flood, smurf attacks, and TCP/SYN attacks. All attacks are infamous due to the processor resources exhaustion effects caused on the victim's computer. Articles [56] and [57] provide complete studies that show the effects of ping floods and smurf attacks. Work done in [56] displays experiments done using ping floods and work in [57] shows how smurf attacks can even be amplified with the number of elements associated to a network. In order to create an environment where an attacker floods the system, the use of a performance tester becomes the key. The tester played the role of the attacker in this system.

There are three elements of the information security triad that must be complied to ensure a high security in information technology: Confidentiality, Integrity, and Availability. The elements of focus of this research are integrity and availability.

Having the integrity aspect compromised in a smart grid system 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. A simple example could be that the meter physically reports x watthour consumed, yet the information that the monitoring computer receives is y. Another interesting experiment was comparing the energy consumption made between a smart meter in normal conditions versus another one under cyber-attacks.

The other aspect to investigate was the information availability. During the attack, it was observed if every single element in the smart grid remained available, meaning that the monitoring computer must be able to access the information from all connected devices. Having the information always at hand help users and providers to determine how the energy is being consumed, how to define billing data, and also help utility companies to execute special commands like the mentioned remote disconnection of service. However, if an element gets cut out of the grid, either the user or the company will start to use extra resources that always end up in wasting money.

4.3 Smart Grid System Simulation

The first test consisted of setting a three-days baseline (the meter was not under any type of attack) after three experiments performed on the S4x Ethernet meter. The electrical loads were active (200 watts) while the metrology board (boards inside the meter in charge of taking the electrical signal and return the value within the internal memory that represents it) took care of the metering job. Inside the meter, the metrology board maintained a continuous communication with the communication module. As the metrology boards determined the readings being taken, they sent the information to the communication modules. In the case of the S4x Ethernet meter, the communication module works at the same time as a network interface card (NIC). The signal then traveled through an ethernet medium until it reached the network switch. On the other side of the system, the monitoring computer was connected on a different port of the network switch. To begin a communication session with the meter from the monitoring computer, the computer accessed the web portal created by the meter manufacturing company. Once the session was stablished, the monitoring computer accessed all the information that it needed. For this monitoring, a user intervention was not needed thanks to the

implementation of the software application developed by our laboratory, AMT monitor. To begin a communication session, the monitoring computer entered the meter parameters through AMT monitor, and the application took care of retrieving the energy consumption. Once the communication session was over, the AMT Monitor left a log file containing the concerning information.

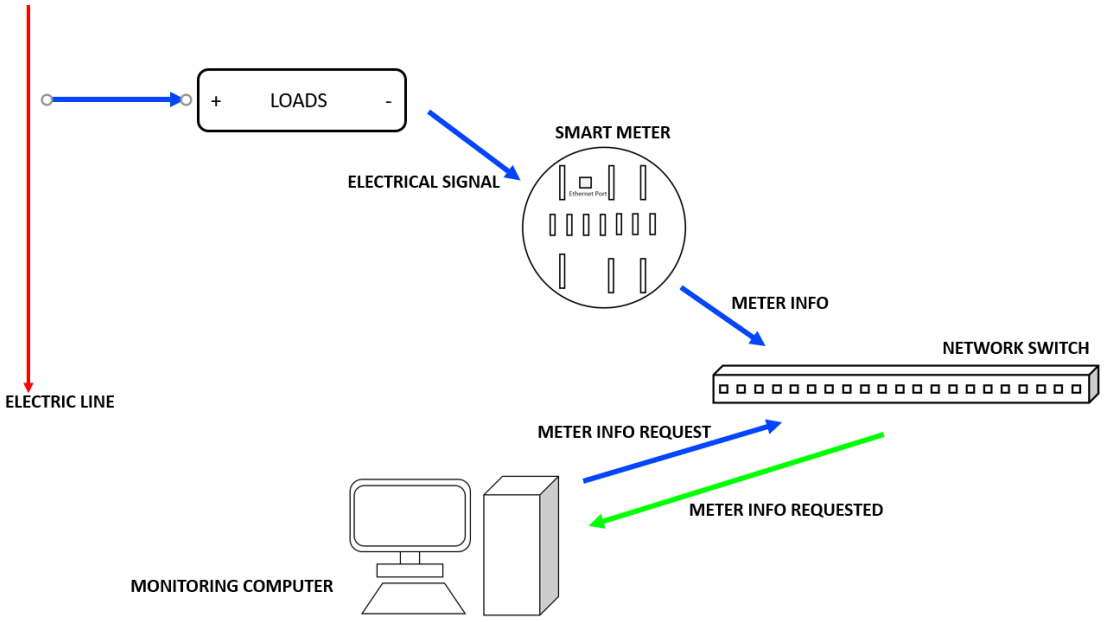

Figure 36. Steps in the smart grid to read, store, and retrieve information.

During the first successful test, the communication was stable along with the rate of change of watthour consumption. For the 200 watts load, the meter was able to read an average of 201 watthours with a standard deviation of 1 watt.

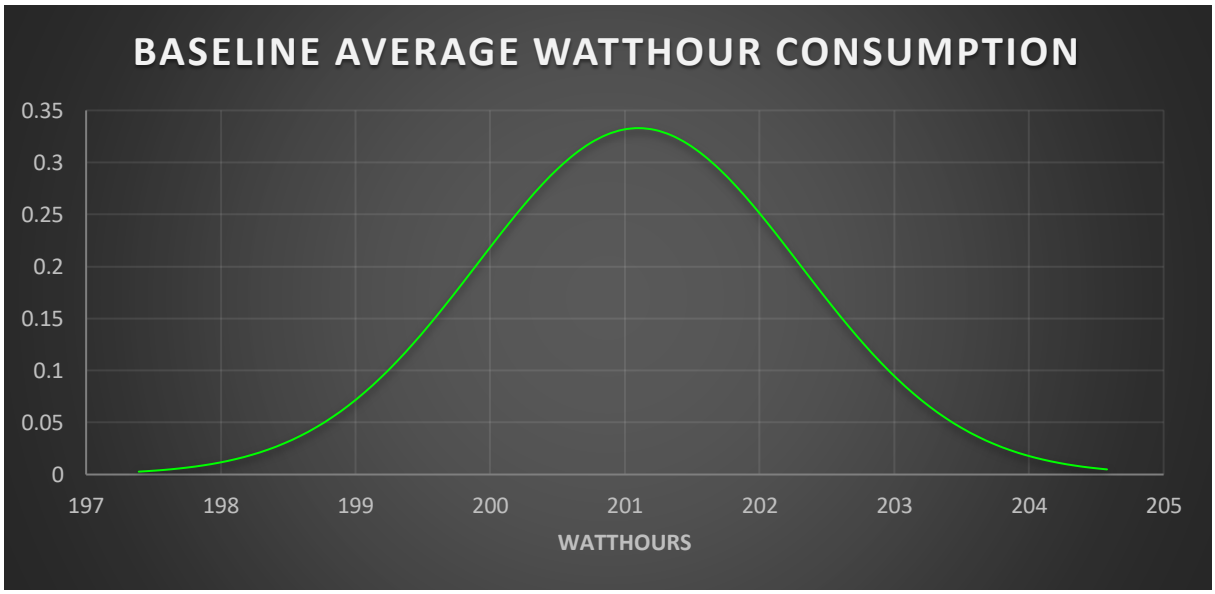

Figure 37. Average kilowatt-hour consumption in 72 hours recorded by the S4x Ethernet meter.

4.4 Ping Flood Testing

This experiment began with the system acting under normal conditions. After a planned time, the performance tester started to send a series of ping requests to all meters. During the flood time, AMT monitor attempted to build its report on the basis it was indicated to. The initial parameter for the performance tester had a bandwidth of 22.83 Mbps. The total time of the system being under attack was eighteen hours. After the attack ceased, the system was let to run under normal conditions for another eighteen hours.

After the test ended, the AMT monitor log file was analyzed. The file presented several failures when retrieving data. It was practically impossible for AMT Monitor to ensure a proper reading. This, meaning that connection to the meter was impossible. Therefore, the log file showed no readings during the first 18 hours of testing, which is the period were the meter was under attack, the remaining 18 hours were tested with no attack, here is where the log file

started to report values normally. This experiment was repeated several times and displayed the same results on all three meters.

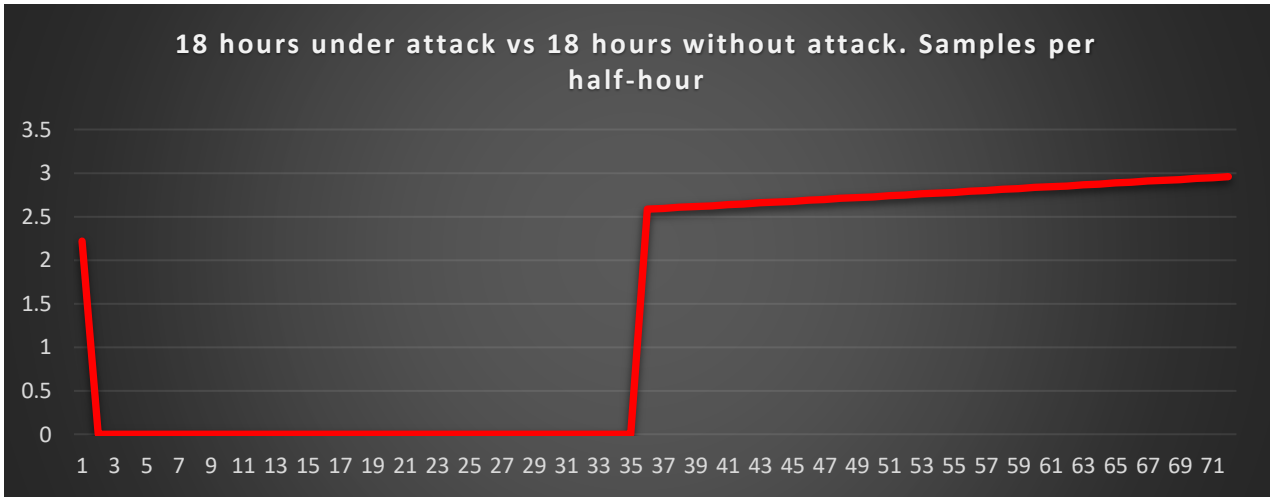

Figure 38. Values recorded by the S4x Ethernet meter.18 hours under attack vs 18 hours without attack. Hours vs. kilowatt-hours.

4.5 Smurf Attack Testing

After trying ping flood attacks, the next type of attack in the list was the Smurf attack. The experiment was executed in the same way as ping flood did and using the same bandwidth (22.83 Mbps). After the experiment was done, the data was analyzed, and it reflected very similar results than in the experiment with the ping flood. In fact, the results were so similar that if a picture were to be placed in here, it could be easily confused with previous picture. All results were the same with all three meters.

4.6 TCP SYN Attack Testing

The final experiment to try on this list was the TCP/SYN attack with the same attack bandwidth as in previous attacks (22.83 Mbps). Surprisingly, this final attack presented the same results as in previous two types. The communication stopped almost immediately after the

attack started, AMT monitor could not determine the watthour readings. Like on previous attacks, the results were the same for all three meters.

4.7 First Analysis

The experiments in this section provided a broad insight about the behavior of smart meters when an external component in their communication system is introduced, in this case, a traffic-disturbance cyber-attack. By using a load of 200 watts for experimentation, three different 144-hour runs were done, and an average consumption was calculated from all the runs.

Figure 39 displays a run of 144 hours which was obtained from the average of all three runs. The real consumption data in the graph can be divided in three periods: the hours were the meter ran under normal conditions, the hours were the meter ran with a ping flood applied, and the hours were the meter ran with a smurf attack applied. The first period which corresponds to the first 48 hours is when the meter ran under normal conditions. The second period corresponds to the following 48 hours between hour 48 and hour 96; and it is when the meter received a ping flood cyber-attack. The last period corresponds to the last 48 hours of the experiment between hour 96 and hour 144; and it is when the meter received a smurf cyber-attack. The expected consumption data was calculated from the average watthour consumption obtained from the first 48 hours of experimentation (meter running under normal conditions).

It is important to mention that AMT Monitor returned values of zero when the communication with the meters was impossible. Therefore, the real consumption graph has values of zero when the meter was under attack. Figure 39 shows the differences in consumption between the real consumption and the expected consumption. Although there

exists a difference in consumption between both graphs, it is minimal. Sample A was taken at hour 96 right after the ping flood attack ceased and reported a consumption of 19.1673 kilo watthours compared to the expected value of 19.1468 kilo watthours; the difference between both values is 0.0205 kilo watthours or 20.5 watts above the expected value. Sample B was taken at hour 144 right after the smurf attack ceased and reported a consumption of 28.7341 kilo watthours versus the expected value of 28.7202 kilo watthours. The difference between the final readings was 0.0139 kilo watthours or 13.9 watthours above the expected value. Since the difference between the final samples was less than the first samples, the results are not sufficient to determine whether if the meter was in fact affected by the attacks or if the differences are only fluctuations acceptable within the standards.

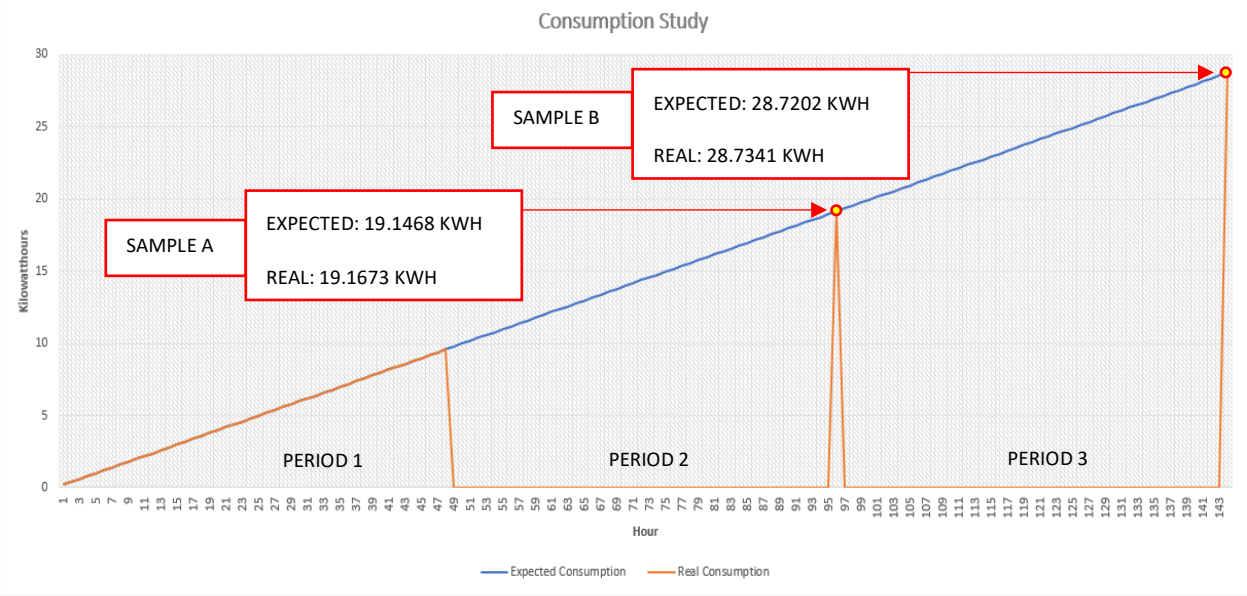

Figure 39. Consumption study. Expected values versus real values of meter readings when the meter was under cyber-attacks.

4.8 Connectivity Focus

For technical practicality, this work refers to the availability of information as the connectivity capability of smart meters in the network. If the connection is stable, the information is available. Since the focus of research changed to the connectivity status, there was no point on keeping track of the loads read by the meter. The data graphs changed its layout from being sample vs watt-hour to sample vs connection status. There were only two statuses considered for this investigation: connected, not connected.

The research goals changed to determine the following questions:

1. What is the minimum attack bandwidth needed to completely stop the smart grid communication?

2. How fast can a flood attack stop the communication in the smart grid?

3. Which type of cyber-attack is the most efficient to affect smart grids?

4. Is there any relationship between the time that the smart meter spends being under a flooded network versus the effect in the smart grid?

5. Is there a relationship between the attack's bandwidth and the effect in the smart grid?

6. Is there any possible way, a smart meter can stop communication for good after being under attack?

To determine the answer to these questions meant that the AMT monitor was not the best solution anymore. The reason of this is because smallest sample interval that the AMT monitor can create is 2 minutes, and samples as small as one second were required.

4.9 Smart Grid Overseer (SG Overseer)

SG Overseer is another software application developed in our laboratory that assists determining the connectivity status of devices in the grid. The science behind this application relies in the phenomena that occurs when a smart meter is under attack. Taking into consideration the ICMP protocol defined in [58], a ping response was enough evidence to determine the connectivity status of any device connected in the local network. 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, it meant that the communication between the monitoring computer and the smart meter was active. If the smart meter would not send the ping response, it meant that there was a problem in communication. When meters were under attack, the communication got cut between the monitoring computer and the smart meter. Therefore, any ping request done by the monitoring computer resulted in a request timeout, because the meter was unable to communicate, and hence, the communication was considered as inactive. SG overseer allowed the user to make readings of any size of time, and it achieved this by sending ping requests to the smart meter. The readings samples can be done from even less than a second, up to any value the user may come up to. Regardless of the status in communication between the meter and the monitoring computer, SG Overseer reflected this result through log files. Like AMT monitor, SG Overseer became an essential tool for the work performed in this thesis. It was developed using Visual Studio and the .NET

platform. While AMT monitor was used to study energy consumption, SG Overseer was used to study the communication stability between user and meter.

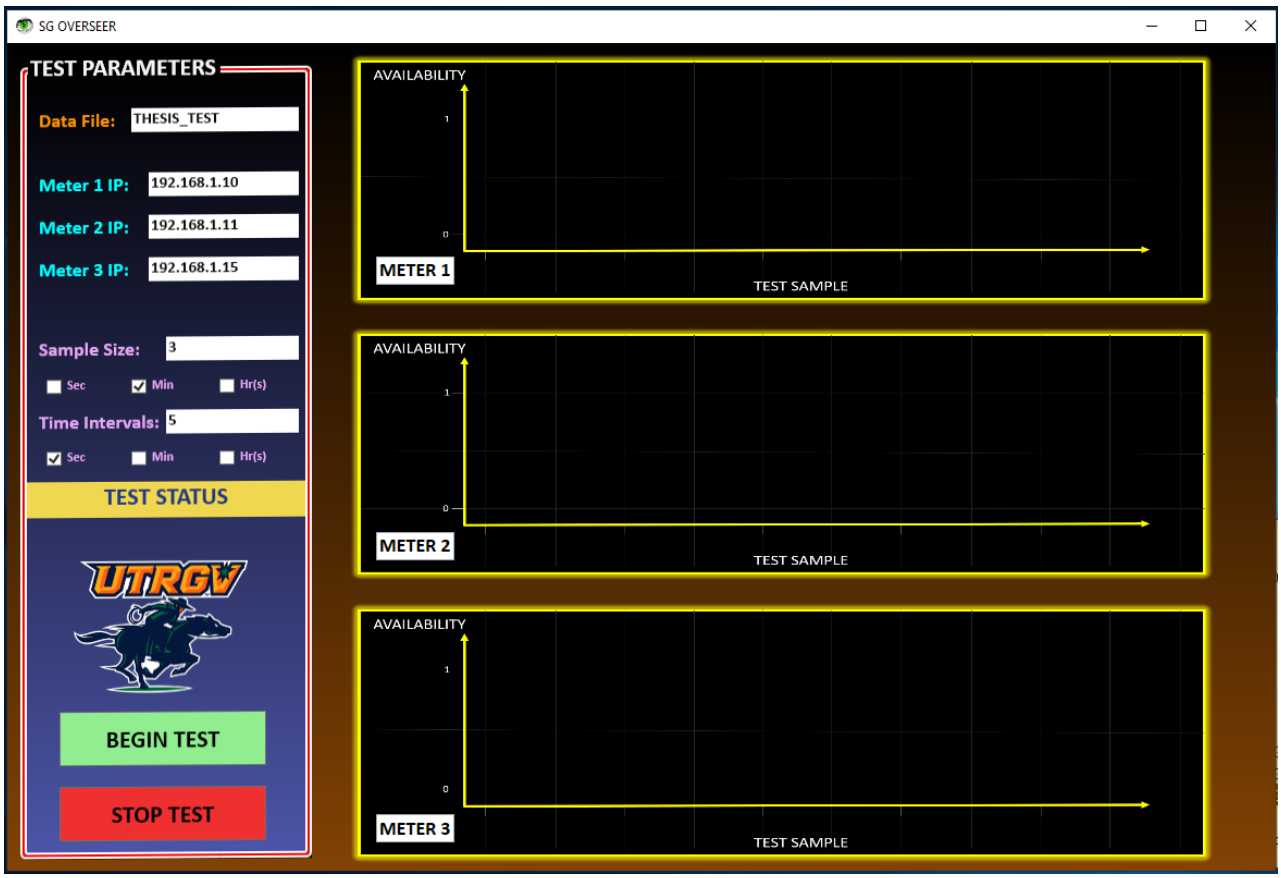

Figure 40. Smart Grid Overseer (SG Overseer)

The Data File field specifies the name the user entered to create the log file; the log file would have the name entered. As the name implies, the following three fields are the meter IP addresses, if one if these is wrong, the application will not be able to retrieve any information from that specific address. The Sample Size field indicates how much will the test last. Time Intervals is the field used to determine the sample intervals at which each reading will take place.

Once the test begins, the log file is immediately created, and it gets dynamically filled as the application gets executed. When the test is finished, the graphs in the interface will display the status of the last group of five readings. Green dots mean connection normal, while red dots indicate communication failure.

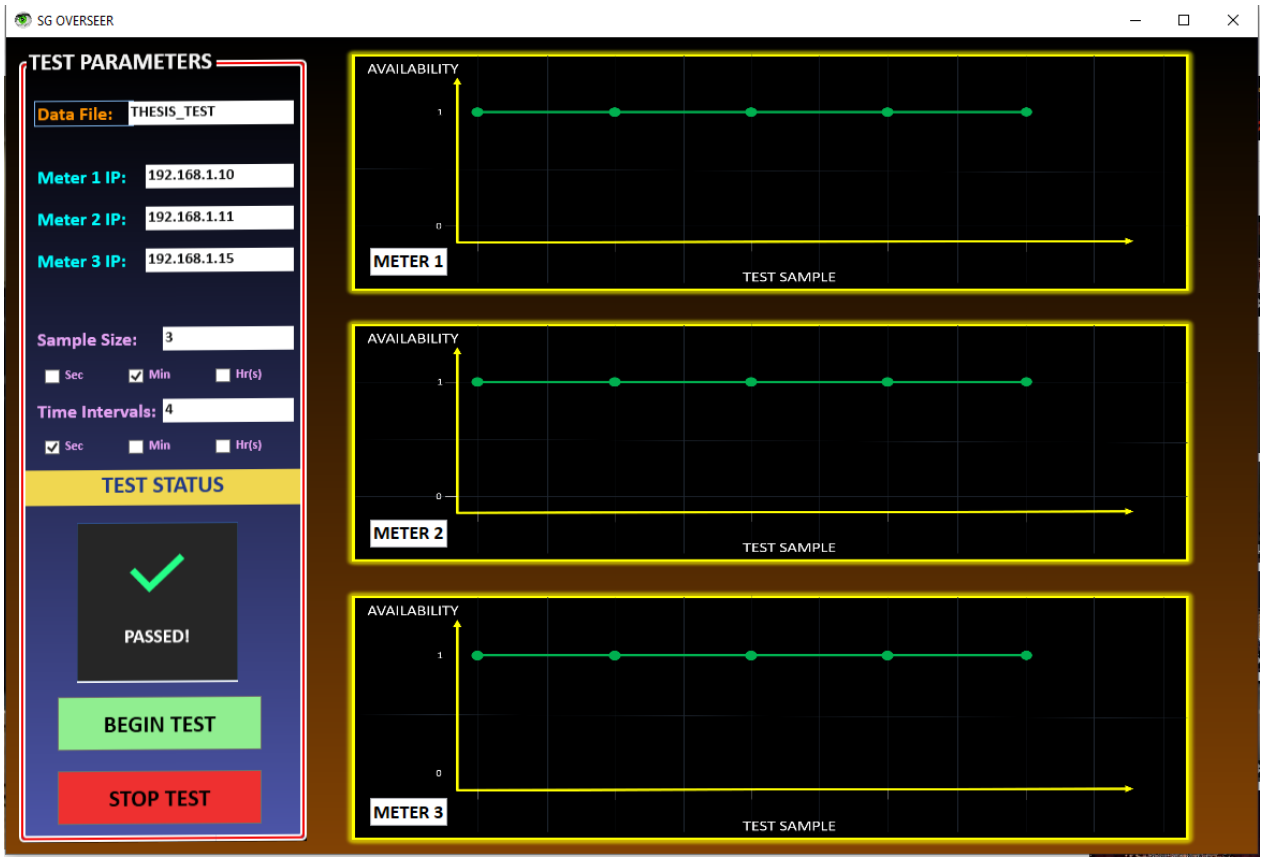

Figure 41. SG Overseer after a communication session were all three meters shown successful connectivity.

4.10 Connectivity Reports

The log files present the information with the structure of a table with four columns and a user defined number of rows. The first column specifies the exact date at which the sample (ping request) started execution, the second, third, and forth column indicates the connectivity status. SG Overseer will report only 0's and 1's as the status values. 0's means that the ping

failed, and therefore, the communication was broken. 1's indicate that the meter successfully responded to the request, and hence, the communication was possible.

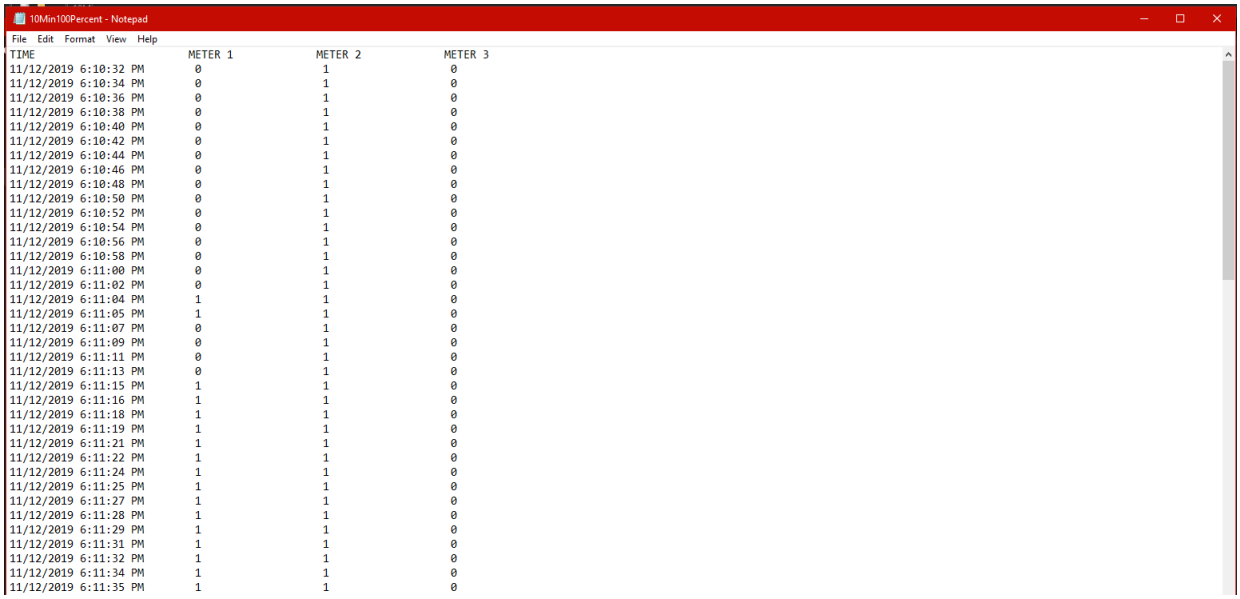

Figure 42. SG Overseer sample log file.

CHAPTER V

RESULTS

5.1 Consumption Reporting

The data in this section describe the results from the experiments performed when evaluating the consumption reports for both cases (when a meter worked under normal conditions and when it was subjected to cyber-attacks). The meter used for these experiments was the Landis+Gyr S4x Ethernet. The theory in discussion was to determine a possible data corruption caused by a severe traffic attack to the meter communication module. This experiment was based on the hypothesis that exhausting the processor with tasks, could lead to incorrect internal operations such as inaccurate energy readings, or memory corruption.

5.1.1 Baseline

For this experiment, the loads consisted of two 100-watts light bulbs. Therefore, the expected consumption was 200 watthours. The baseline would set a reference for a normal consumption in a certain period. Three different experiments of 168 hours (one week) were done. The graph below summarizes the average watthour consumption recorded from the three

experiments. The results indicated that there was an average consumption of 201 watthours with a standard deviation of 1.198 watthours. Data ranged from 196 to 206 watthours.

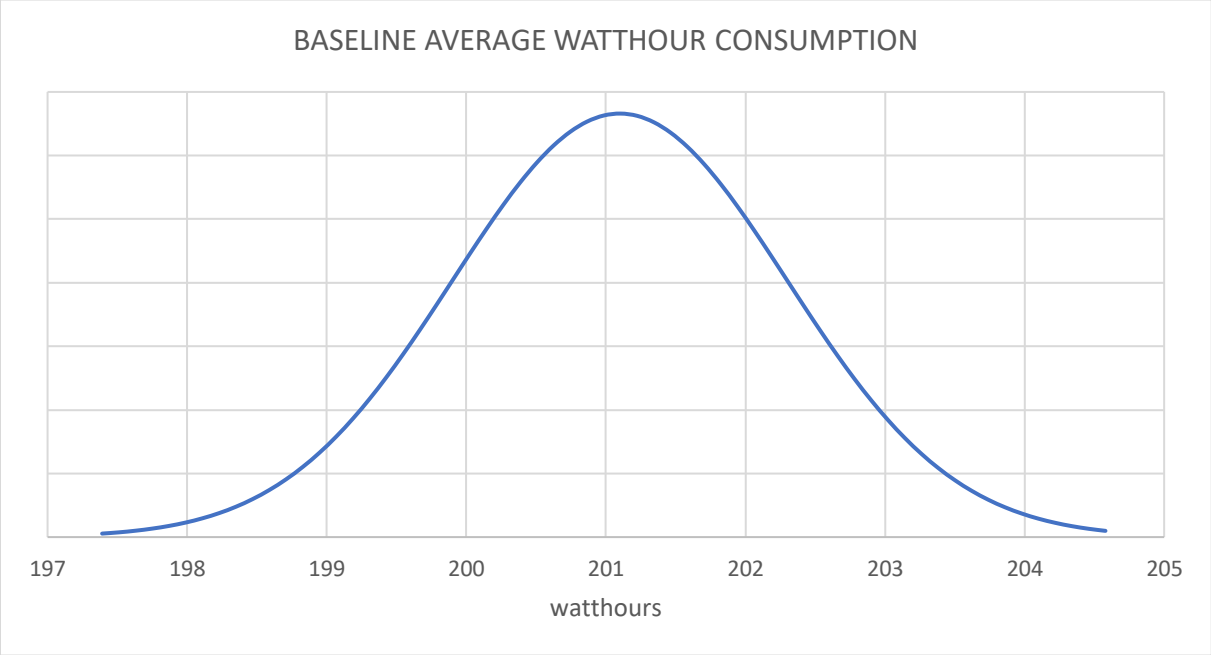

Figure 43. Baseline used to set a reference for the next experiments.

5.1.2 System Reporting Under Flooding Attack

This experiment consisted of setting the traffic simulator to create data packets in the form of echo requests (pings). Since ear echo request has their own size in bytes, sending multiple requests per second requires bandwidth resources. The traffic simulator software has the option to set the maximum resource bandwidth used for data transfer. For this experiment, the bandwidth set for data transfer 500 Mbps. This means that the simulated attack had a bandwidth of 500 Mbps or 62.5 Megabytes per second. This bandwidth will be referred for the rest of this work as the attack bandwidth.

This experiment was executed three different times. The meter was set under a constant cyber-attack, and at different times, a sample was taken. The sample consisted of recording the current watthour consumption. Sample 1 was taken after 48 hours, sample two after 144, and sample 3 after 168 (one week). The figure below shows the baseline in a blue line and three different color dots. Each dot represents the value obtained at each sample taken. All three samples fall within three standard deviations from the mean. This concluded that the data is not sufficient to declare the effectiveness of a flooding cyber-attack against the meters' capability to record consumption.

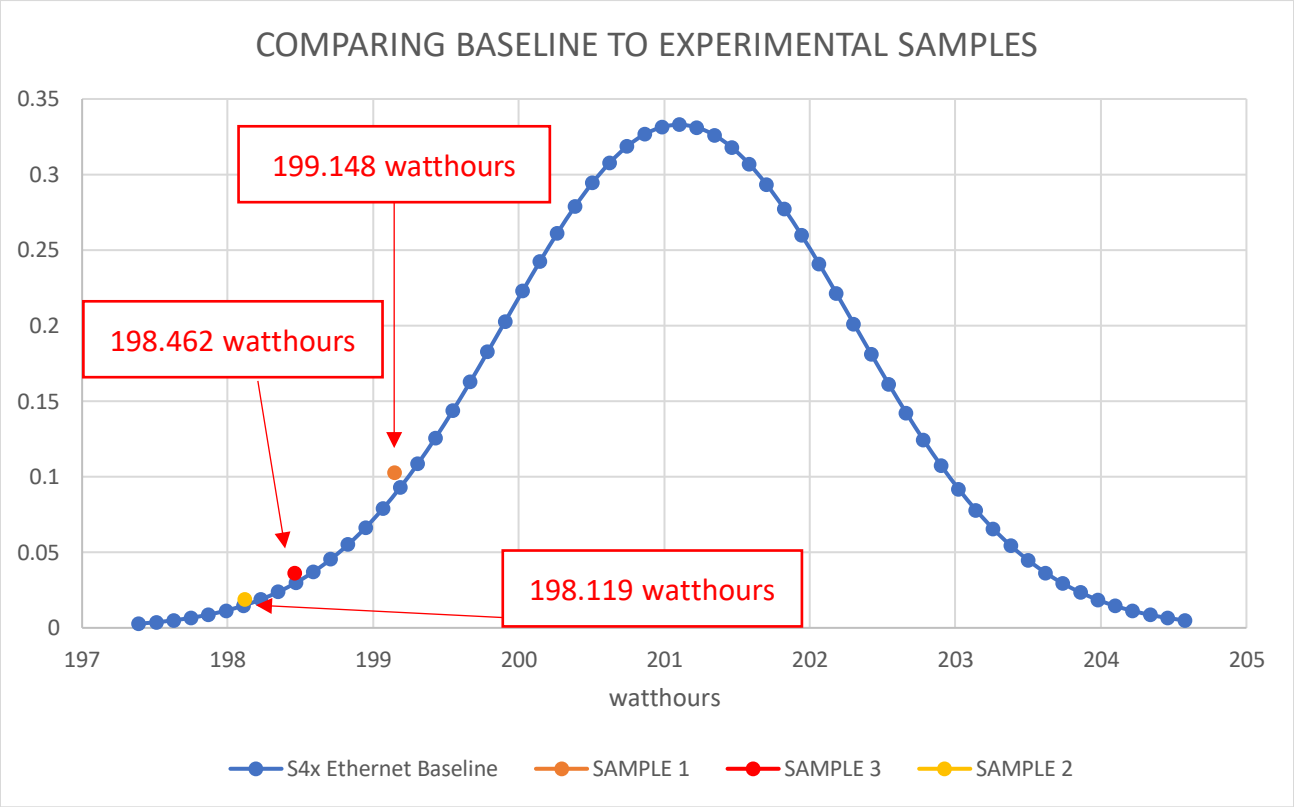

Figure 44. Results of consumption reporting under cyber-attacks.

5.2 Communication Availability

Given that previous experiments revealed that the attacks produced a total loss of communication between the monitoring computer and the meters, the next stage of experiments focused on analyzing the effects of attacks in the communication availability for smart meters. All three meters were tested equally by setting the same traffic loads. For a deep analysis, different bandwidths and periods were tested and helped determining a relationship between the severity of the attack and these two parameters. These experiments revealed three important observations: a minimum effective attack bandwidth to make effects noticeable, the final effect of flooding attacks on smart metering communication, and the posterior effects on communication after a cease in the attack.

5.2.1 Ping Flood Experiments

All experiments from section 5.2.1 were executed with the application of ping floods. The performance tester was set to automatically and programmatically sent multiple ping packets to all three meters. The sub sections below describe the observations of the effects created by ping floods in smart metering communication.

5.2.1.1 Minimum Effective Attack Bandwidth (MEAB) to Affect Connectivity. As the attack bandwidth increased, it was observed that all three meters started to present communication problems. After a certain bandwidth for each of the three meters, communication ceased completely. This value for bandwidth was referred as the minimum effective attack bandwidth (MEAB). Once the MEAB is applied, the communication gets instantly interrupted, and users are not able to establish communication with the meter. All three meters presented a different MEAB.

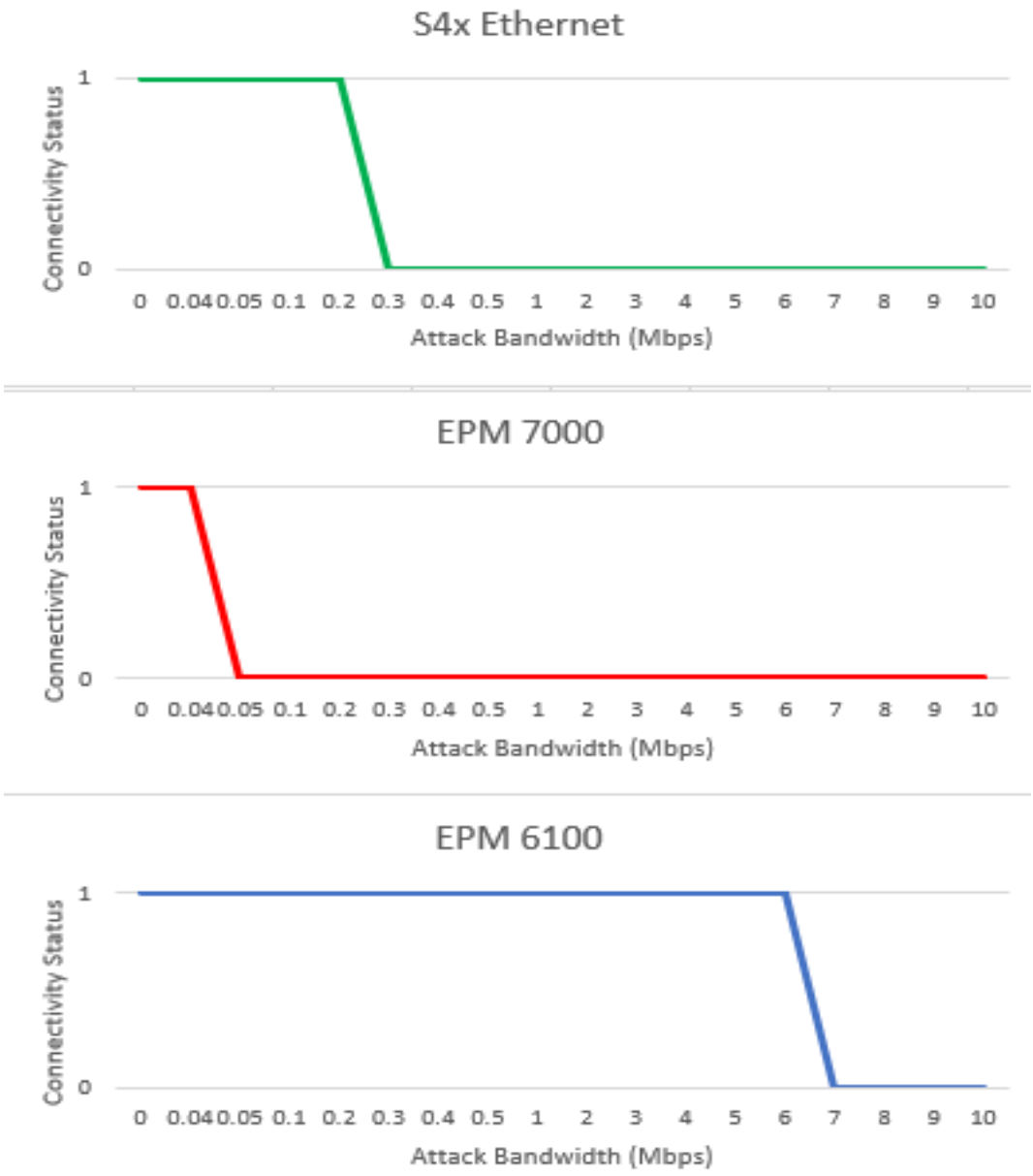

Figure 45. Ping flood's minimum effective attack bandwidth for each meter used.

Our data results shown that while S4x Ethernet meters present a more robust defense against traffic attacks compared to EPM 700, it is less robust compared to EPM 6100.

5.2.1.2 Final Effect. Before reaching the MEAB for each of the meters, the communication did not seem to be affected in any way. As the attack bandwidth got closer to the MEAB, the communication stability became inconsistent, meaning that successful communication sessions with the meter became less common while some ended in failures. Once the MEAB was reached, the communication with meters became impossible. This implies that the attack does breach the availability aspect of the smart metering communication system, and therefore, a Denial of Service (DOS) attack exists. The final effect consists of not letting any authorized user access any of the meter data including billing, current consumption, or any other feature designed in the smart meter.

5.2.1.3 Posterior Effects of a DOS Attack. The last observation is the effect in the communication system that occurs after the attack ends: communication with meters does not come back to normal immediately. After the attack ends, a recovery time is needed to have the meters go back to normal. The following set of experiments were done to determine the relationship between the recovery time, the attack bandwidth, and the attack period. Since the recovery time exists only after an attack is effective, all the experiments were done surpassing the MEAB. If the attack bandwidth is equal to the MEAB, the recovery time tends to be zero. As the attack bandwidth increases getting farther from the MEAB, the recovery time also increases up to the point where it reaches a common average time. All our experiments were done combining both parameters: attack bandwidth, and attack duration. Results tend to be consistent regardless of the modification of both parameters. As long as the MEAB is surpassed, the recovery time seemed to be independent of how the attack bandwidth increased and how the attack duration increased as well.

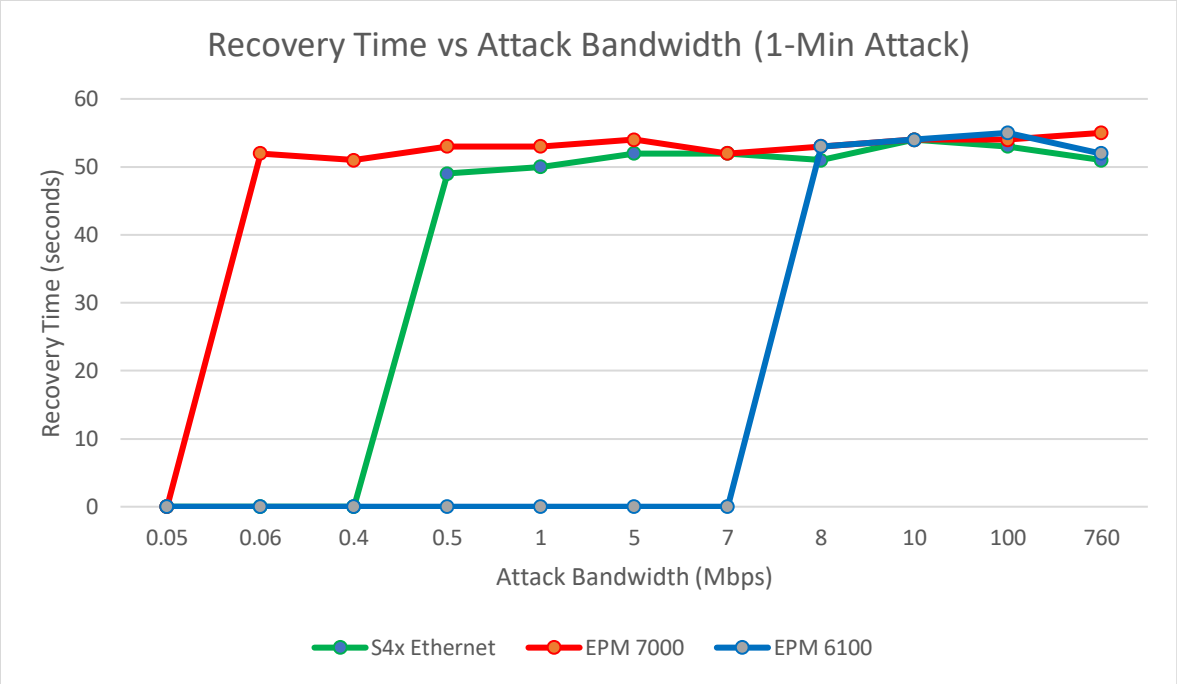

Figure 46. Recovery times for 1-minute attacks using different attack bandwidths.

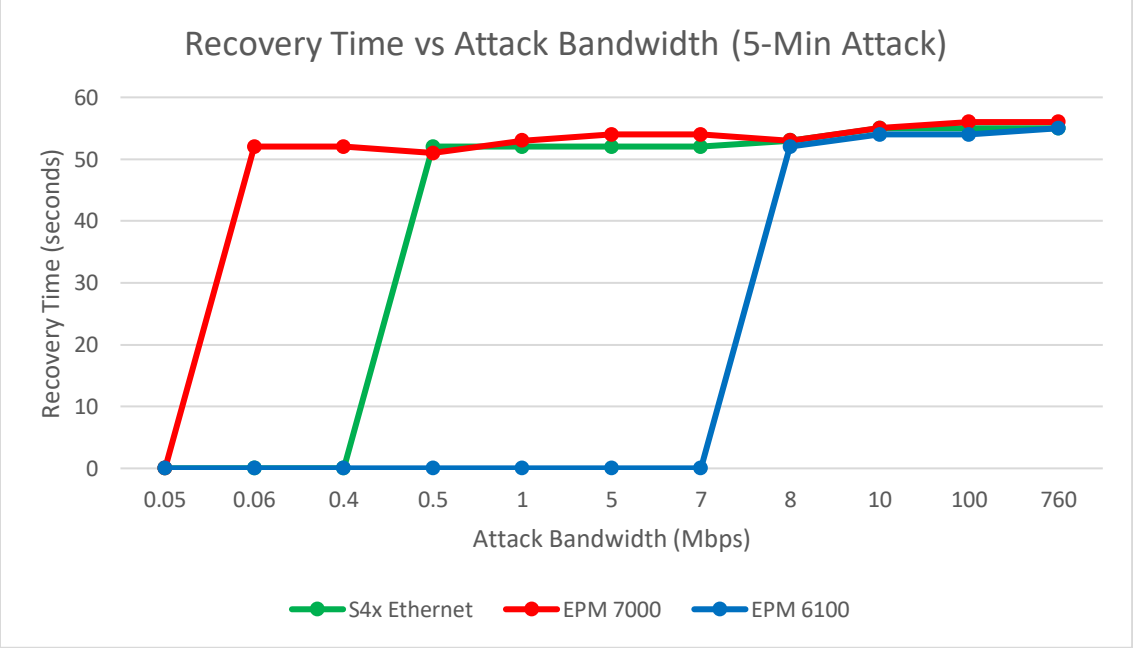

Figure 47. Recovery times for 5-minute attacks using different attack bandwidths.

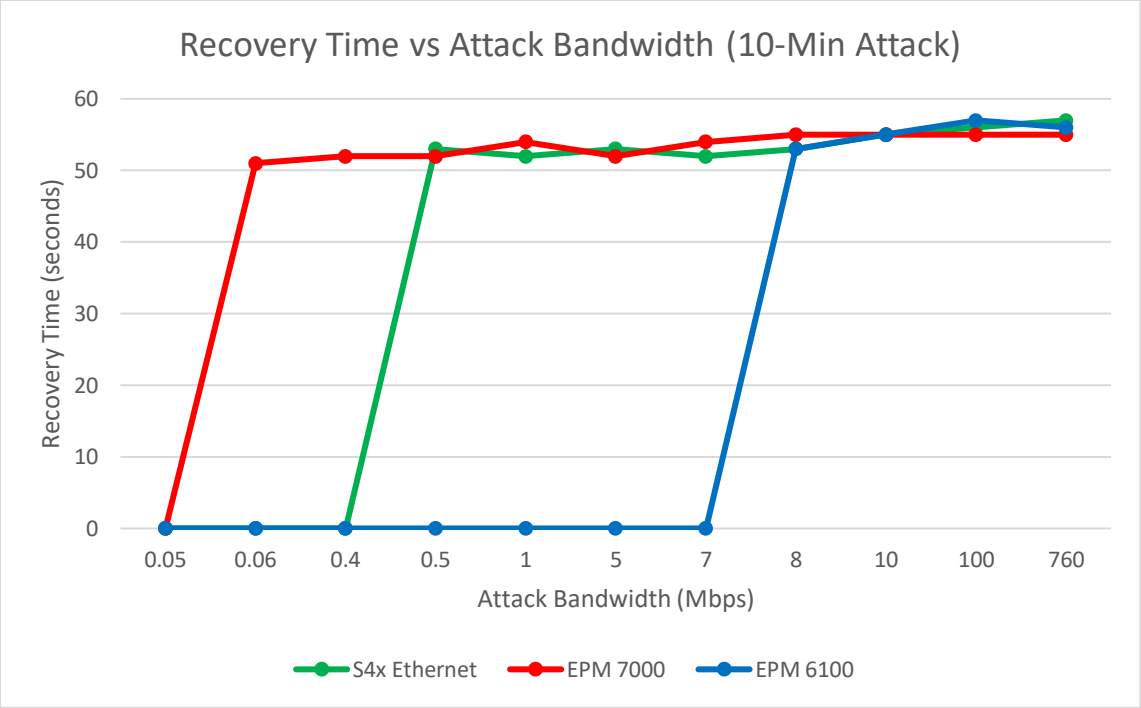

Figure 48. Recovery times for 10-minute attacks using different attack bandwidths.

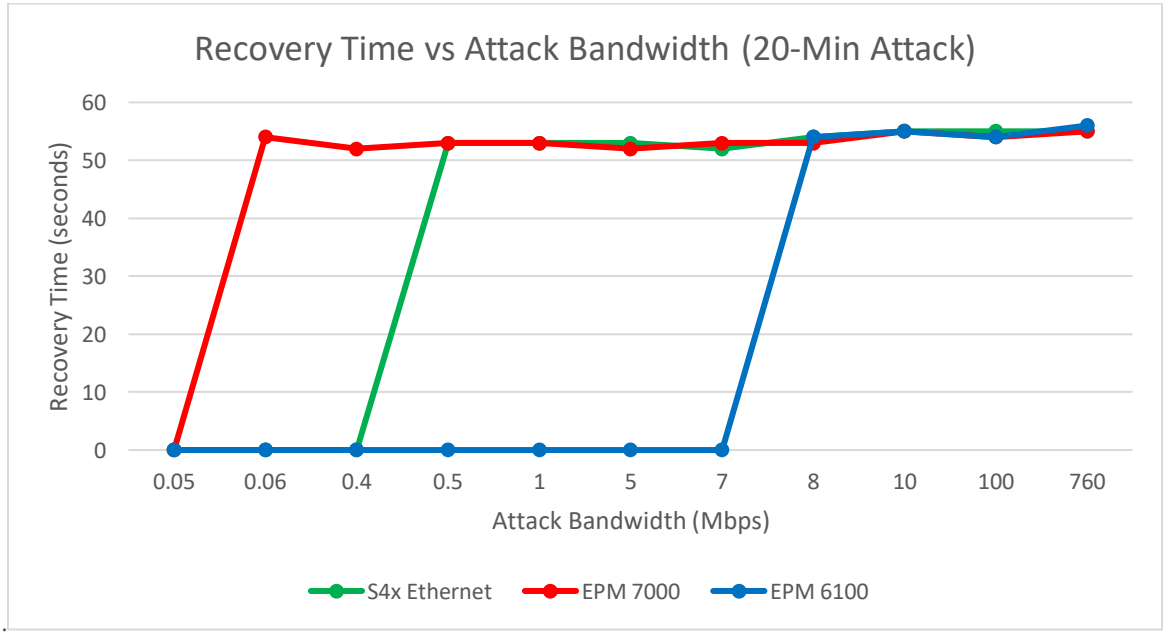

Figure 49. Recovery times for 20-minute attacks using different attack bandwidths.

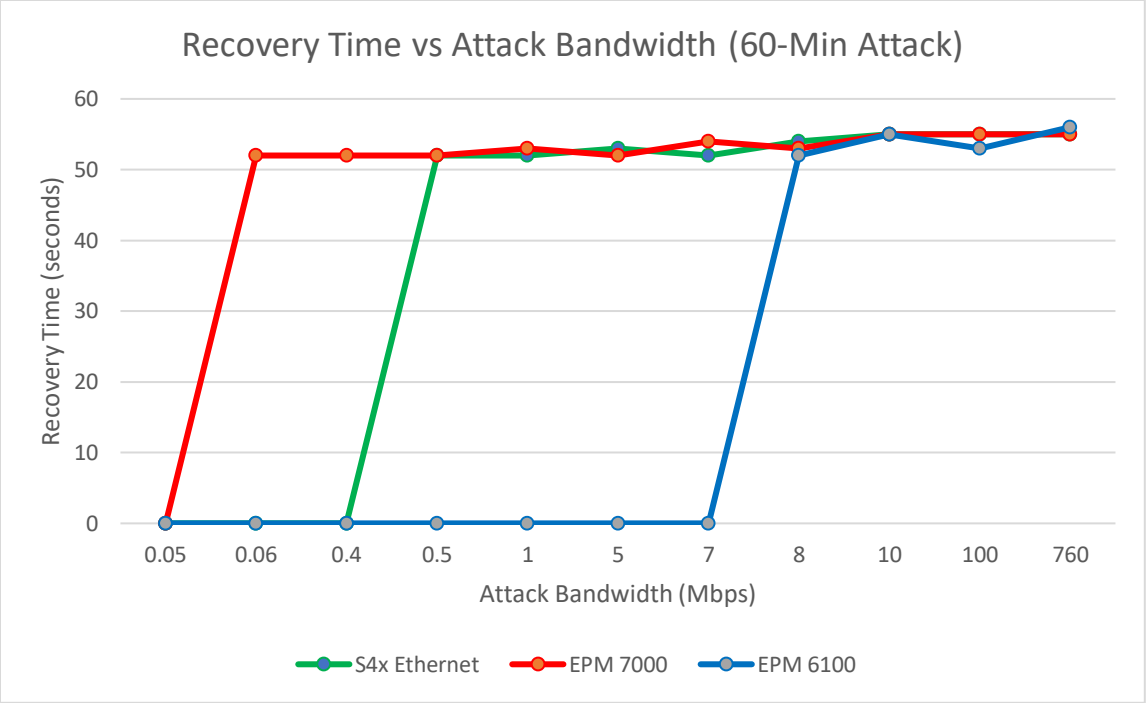

Figure 50. Recovery times for 60-minute attacks using different attack bandwidths.

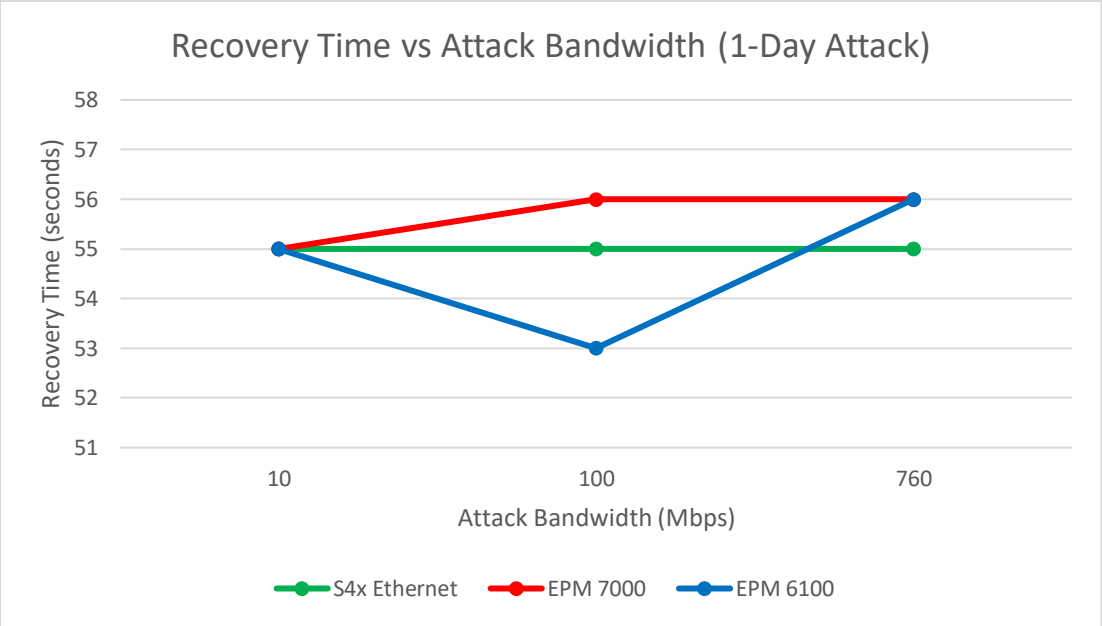

Figure 51. Recovery times for 1-day attacks using different attack bandwidths.

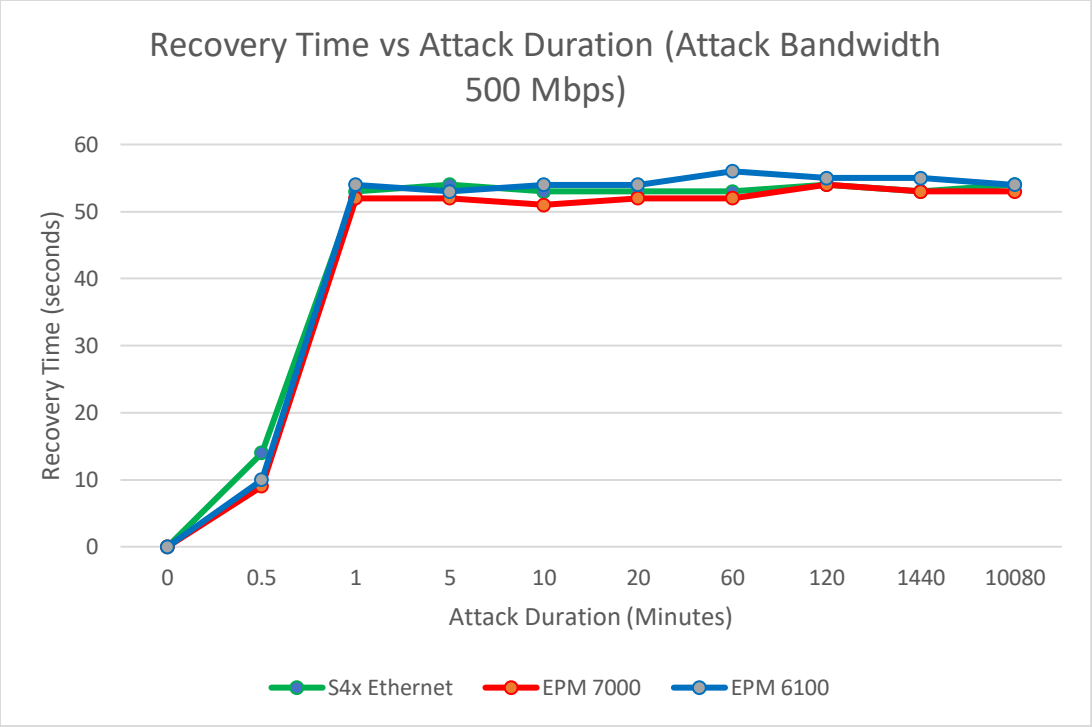

Figure 52. Results of recovery times versus attack duration.

As a conclusion to the experiments, both, the attack bandwidth, and duration become irrelevant once the MEAB is passed. Therefore, for a successful DOS attack it is only required to apply a ping flood with a bandwidth stream higher than the MEAB to cause a total cease of communication (which will return approximately 50 to 60 seconds after the attack ceases).

5.2.2 Smurf Attack Experiments

The next set of experiments were performed similarly to previous, but instead of using ping flood as the method to induce a DOS, a smurf attack was simulated. As previously mentioned, a smurf attack uses the same protocol as ping flood. Instead of using echo requests like ping does, smurf consists of sending echo responses with the victim's address as the source of the packets to all the elements in the LAN. These experiments displayed how after setting the attack, all the elements in the network started to send packets to the targeted meter. Three

observations were made: the MEAB values for all three meters is different than when ping flood was used, the final effect is the same (DOS confirmed), and the recovery time does not exist, meaning that once the attack ends, the meters come back to regular operations instantly.

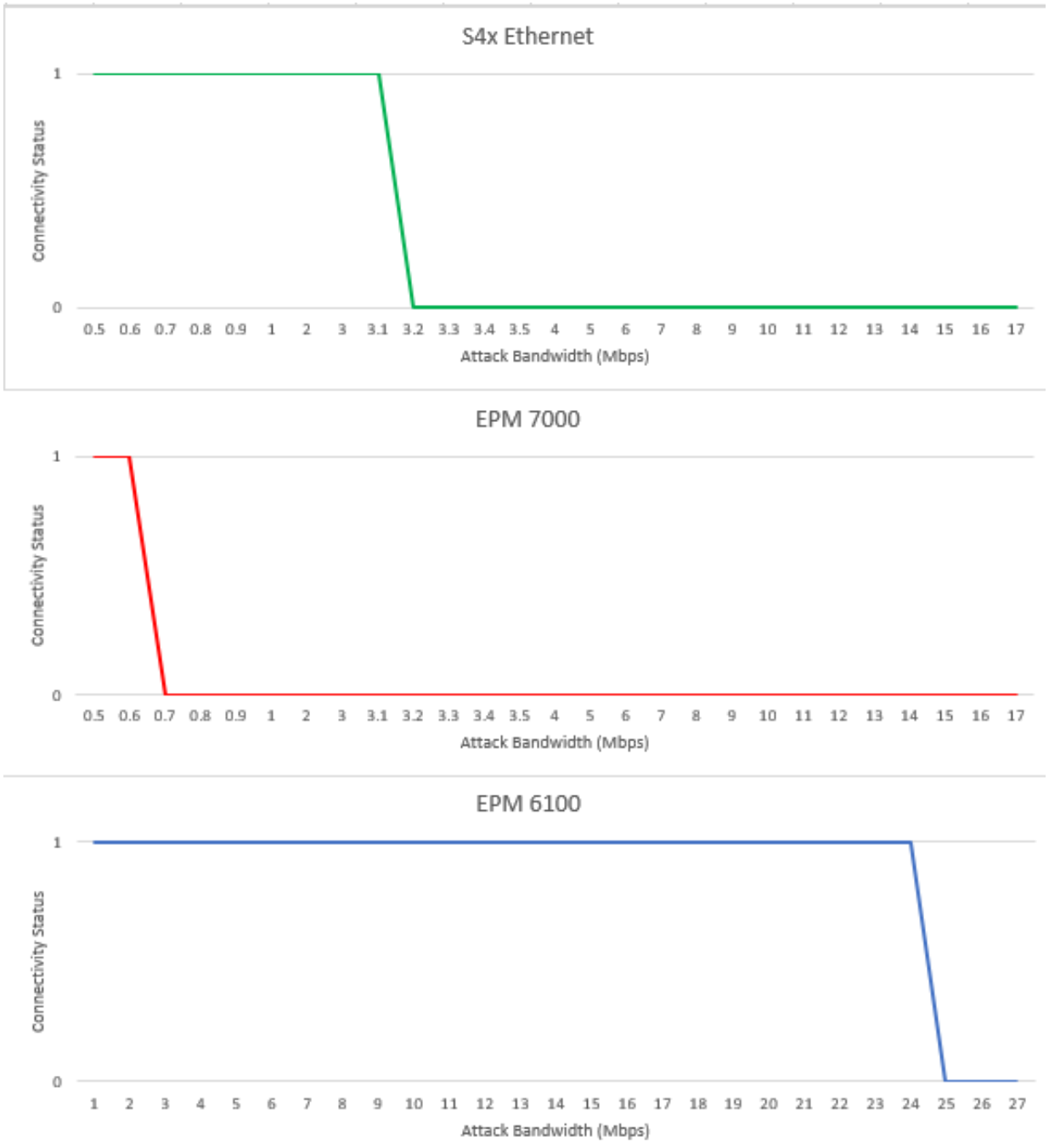

Figure 53. Smurf attack's minimum effective attack bandwidth for each meter used.

5.2.3 TCP/SYN Attack Experiments

The last type of attack used for experimentation was the TCP/SYN attack. In this scenario, the traffic simulator used the protocol TCP/IP and send multiple synchronization request packets to all three meters without waiting for responses. The effects of the TCP/SYN attacks were similar to the ping flood attack. Three observations were also made: there exists a MEAB, the final effect is also a DOS, and recovery times also exist.

5.2.3.1 Minimum Effective Attack Bandwidth (MEAB) to Affect Connectivity. As in the cases before, each meter presented a different MEAB. However, surprisingly, the effects of this type of attack reflected that the EPM 6100 was weaker in robustness compared to the other meters, when in previous attacks was shown to be the most robust. In case of TCP/SYN attacks, the EPM 7000 meter seemed to be the most robust.

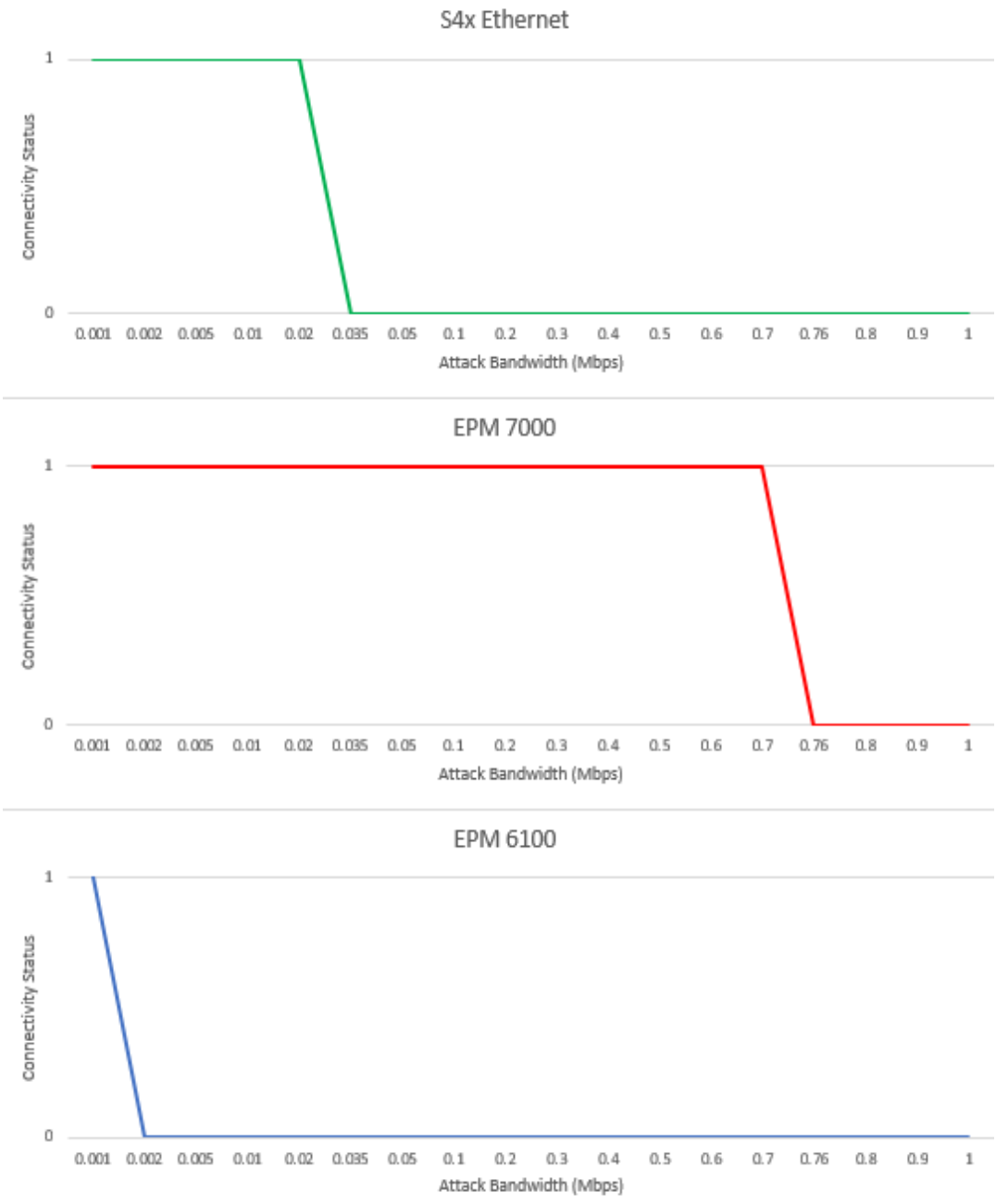

Figure 54. Minimum effective attack bandwidth required on each meter for a TCP/SYN attack to be successful.

5.2.3.2 Final Effect. After the MEAB is reached, the final effect is also a total loss of communication. Like with previous attacks, a DOS can be created with the use of TCP/SYN attacks in a smart metering communication system.

5.2.3.3 Posterior Effects of a DOS Attack. Like with ping floods, an observable recovery time is needed for meters to start communicating normally after ending the application of a TCP/SYN attack. A noticeable difference of the effects of a TCP/SYN attack compared to a ping flood is that all the meters presented different recovery times. In ping floods, the recovery times for all meter ranged between 50 and 60 seconds. In TCP/SYN attacks, the range is different per meter. However, a similar effect occurs in terms that after applying the MEAB, the recovery time for each meter tends to normalize. The graph below represents multiple experiments using an attack bandwidth of 500 Mbps and the variable parameter is the attack period. The difference between meters is noticeable. In regard to recovery time after the application of a TCP/SYN attack, the S4x Ethernet meter seems to be the one that recovers faster, while the EPM 6100 takes longer.

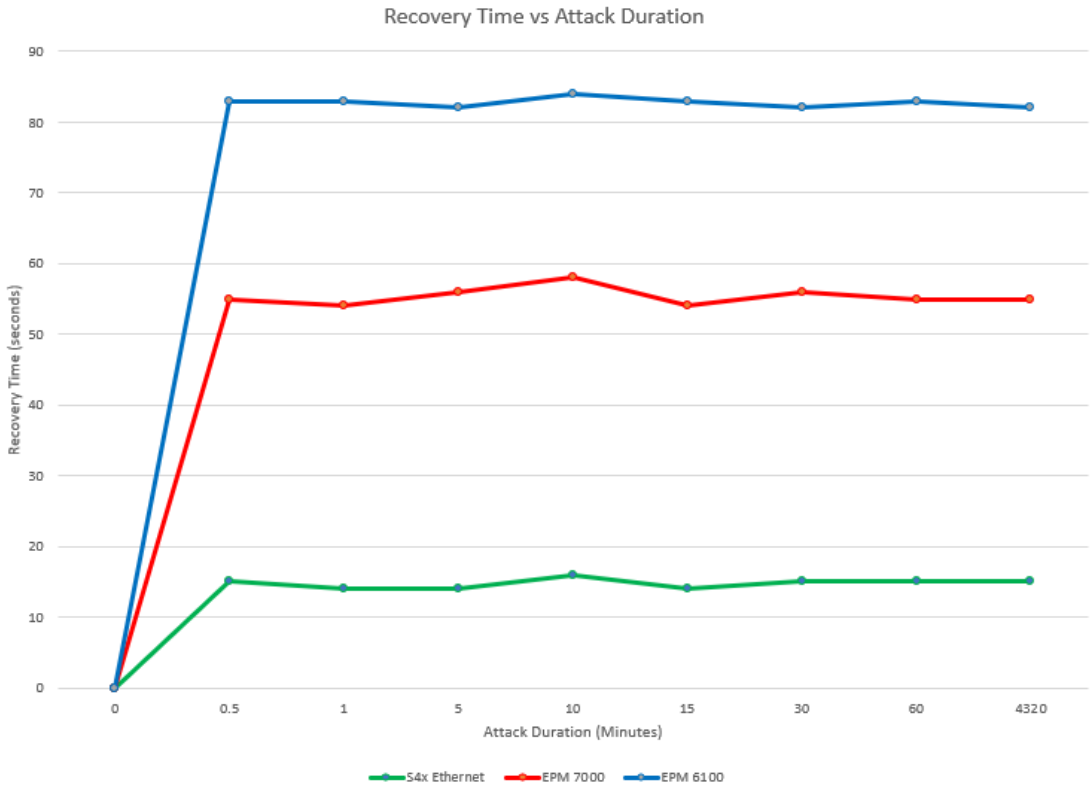

Figure 55. Recovery times for all three meters after setting a 500 Mbps TCP/SYN attack for different periods.

The graphs below are of multiple experiments performed with TCP/SYN attacks and using different attack periods. The variable parameter is the attack bandwidth.

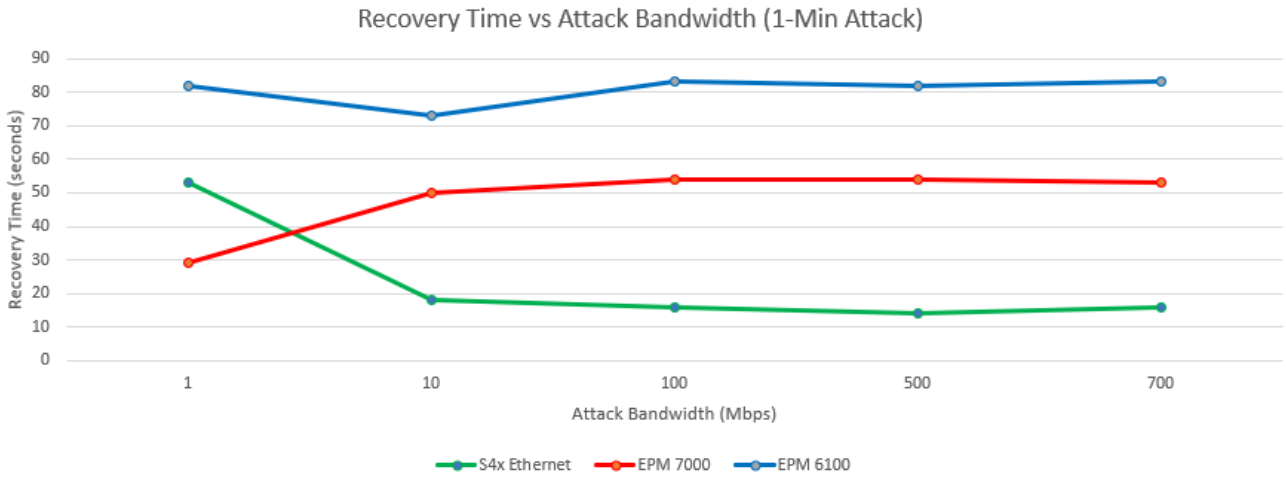

Figure 56. Recovery times for 1-min attacks with different bandwidths.

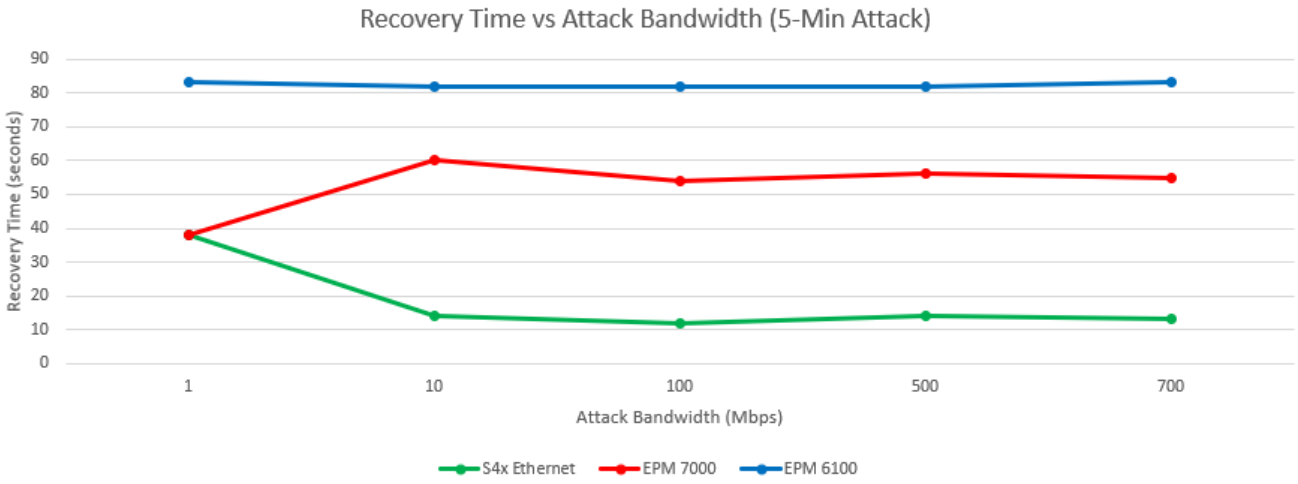

Figure 57. Recovery times for 5-min attacks with different bandwidths.

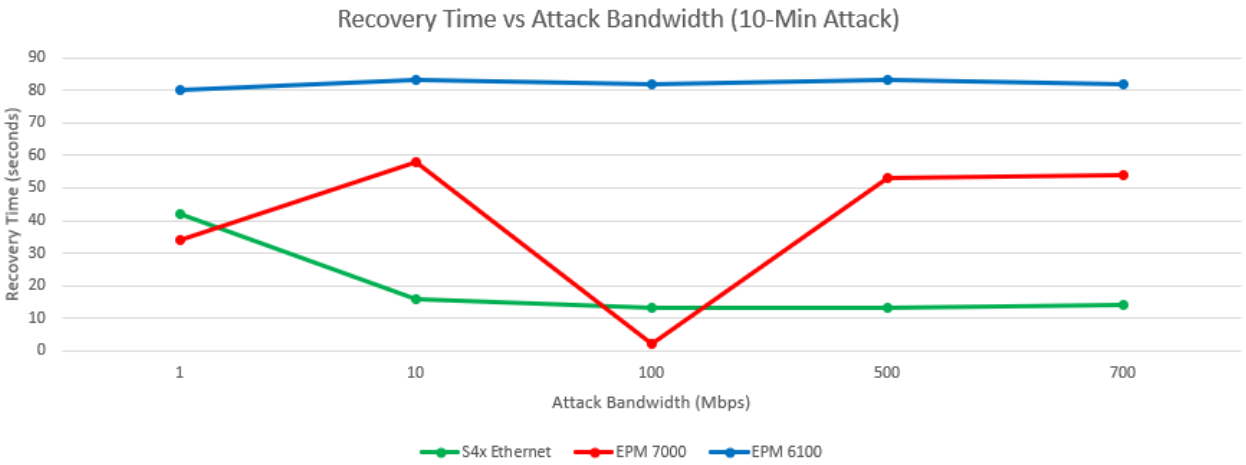

Figure 58. Recovery times for 10-min attacks with different bandwidths.

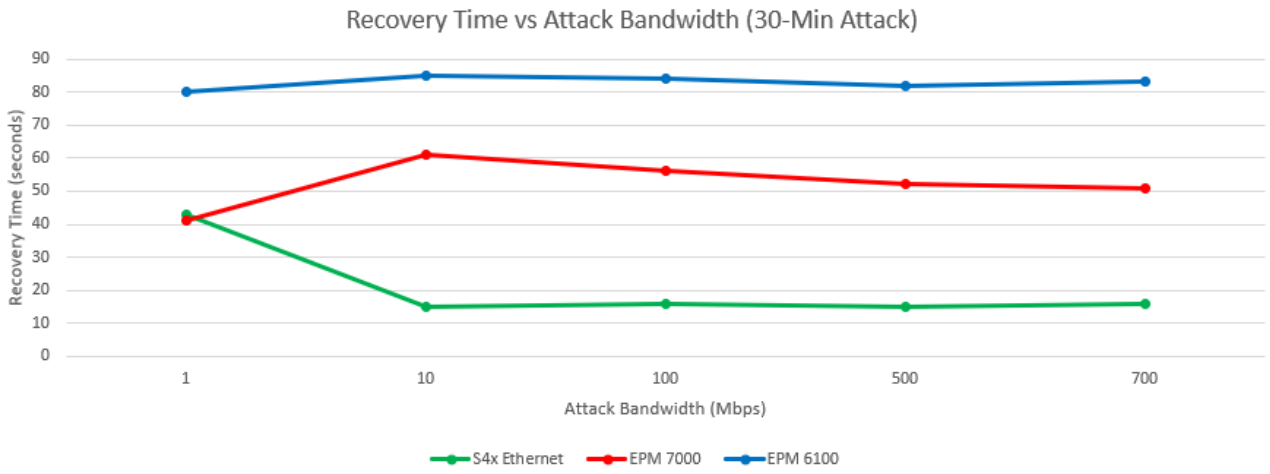

Figure 59. Recovery times for 30-min attacks with different bandwidths.

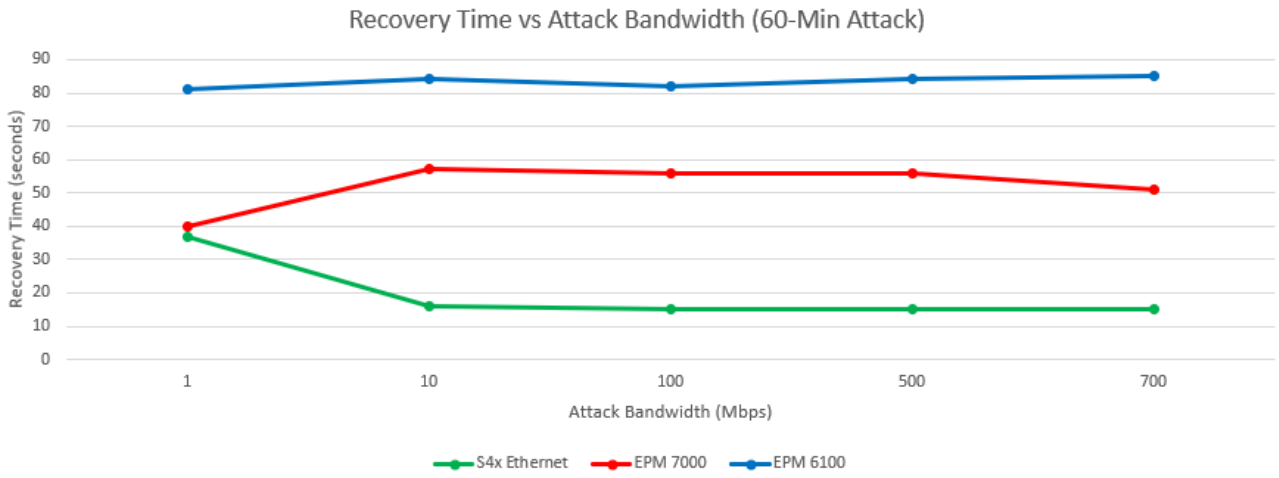

Figure 60. Recovery times for 60-min attacks with different bandwidths.

Although definite conclusions cannot be inferred from the results with the EPM 7000, it can be generally assumed that its recovery times are usually shorter than with the EPM 6100 and longer than with the S4x Ethernet. The recovery times with the S4x Ethernet range from 10 to 20 seconds, the recovery times with the EPM 7000 tend to range between 50 to 60 seconds, and the recovery times with the EPM 6100 range between 80 and 90 seconds. Using these results along with the defined MEABs, it can be concluded that out of all the three types of attacks experimented in this chapter, TCP/SYN attacks are the most harmful to EPM 6100 meters.

5.3 Comparing Impacts of Ping Flood, Smurf Attack, and TCP/SYN Attacks

The MEAB values are different for all three meters, the graphs below show a comparison of the different MEABs found on each meter. The only conclusion that can be drawn is that in regards of MEAB and recovery times, smurf attacks are less powerful than ping floods. TCP/SYN attacks are most effective against EPM 6100 in terms of MEAB and recovery

times. Although the MEAB in TCP/SYN attacks to affect a S4x Ethernet meter is slightly less than with the ping floods, in terms of recovery times, they seem to be less effective.

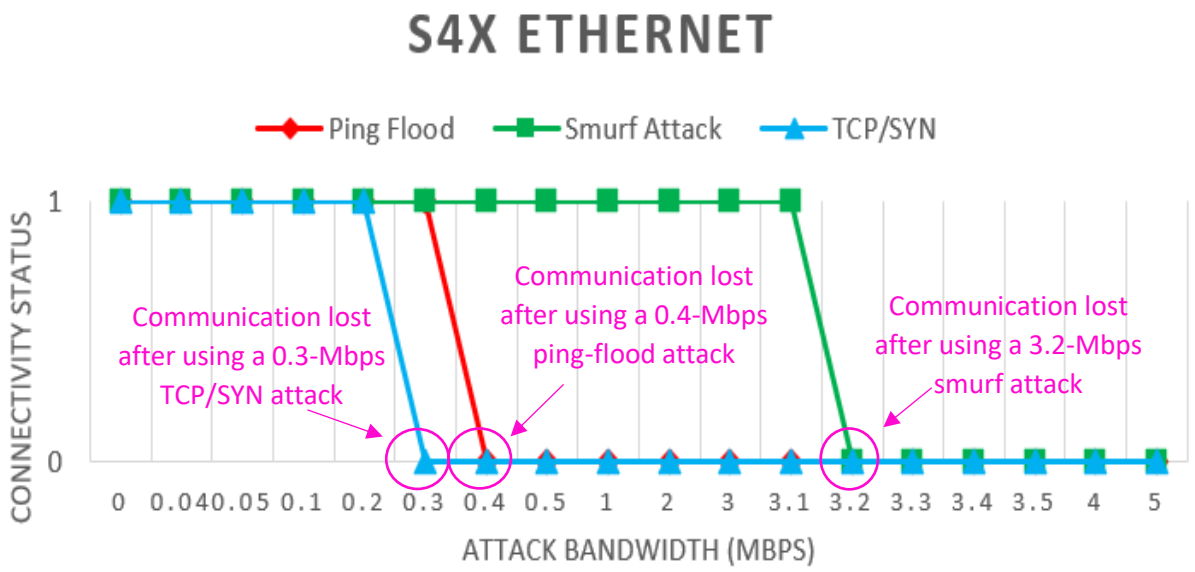

Figure 61. MEABs from different attacks on a S4x Ethernet meter.

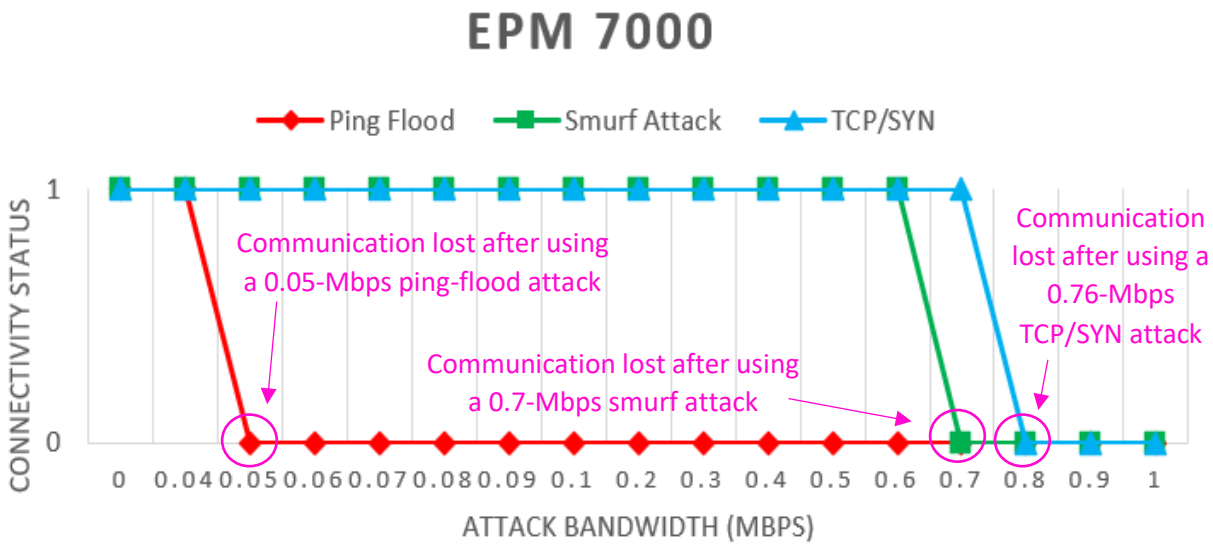

Figure 62. MEABs from different attacks on a EPM 7000 meter.

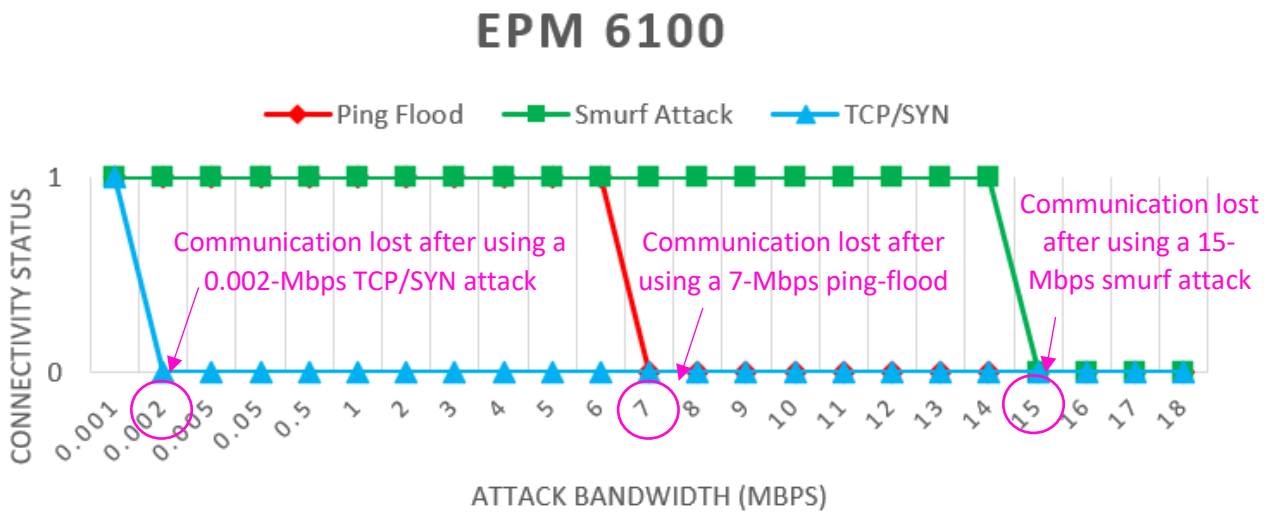

Figure 63. MEABs from different attacks on a EPM 6100 meter.

Table 7. All minimum effective attack bandwidths recorded.

METER	PING FLOOD MEAB (Mbps)	SMURF ATTACK MEAB (Mbps)	TCP / SYN ATTACK MEAB (Mbps)
S4x Ethernet	0.35	3.2	0.3
EPM 6100	6.5	15	0.002
EPM 7000	0.05	0.7	0.76

5.4 Optical Communication Performance

Optical communication with the S4x Ethernet meter was established thanks to an AIP200 optical probe [60]. Taking into consideration that this meter does not have a password, another application was developed to establish a successful connection with the meter through optical communication and make access to the meter possible. Using ANSI C12.18 as protocol of communication, a session was stablished consisting of sending data packets to log into the meter and have access to its stored data. Once the access was granted, the communication was terminated.

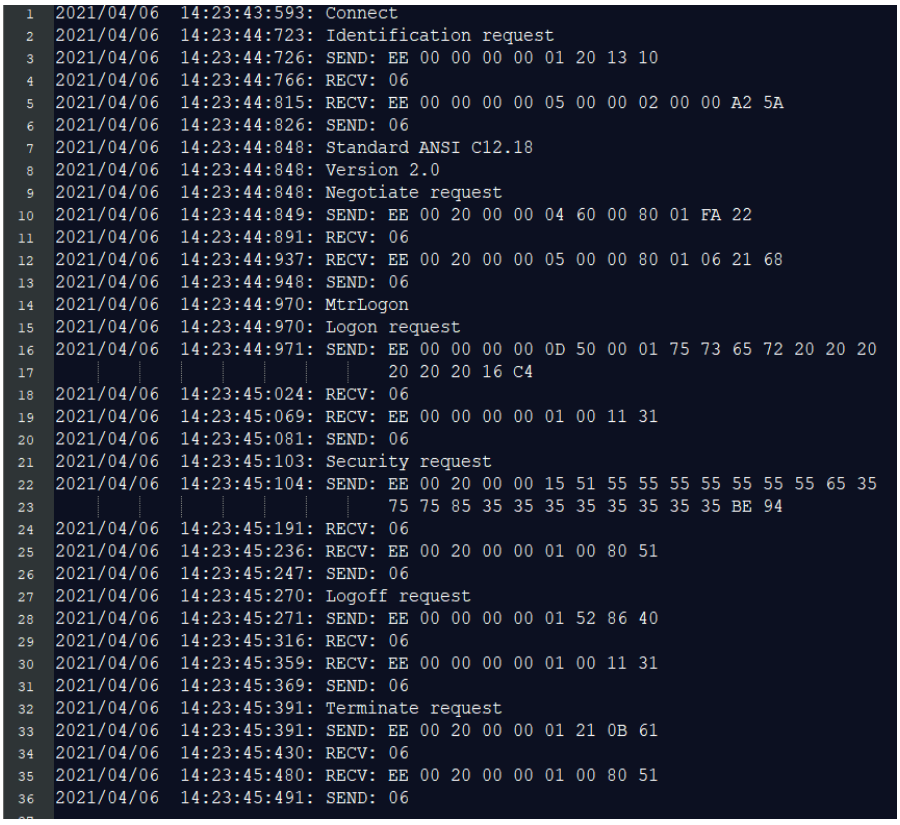

Figure 64. Optical communication session done using ANSI C12.18.

When the meter was subjected to large amounts of traffic data, there was no change in the optical communication session. No delay between data packets was observed or any other type of anomaly. More testing consisted of setting week-lasting attacks and testing multiple communication sessions along the way. Neither the bandwidth nor duration of attack reflected any effects that made a difference between communication sessions established during normal conditions (system not being under attack) and when the system was under attack. Therefore, the results indicate that ethernet-based DOS attacks make no effect on the optical communication system of the meter. Further analysis continued with the hardware design of the meter.

Figure 65. S4x Ethernet internal circuitry.

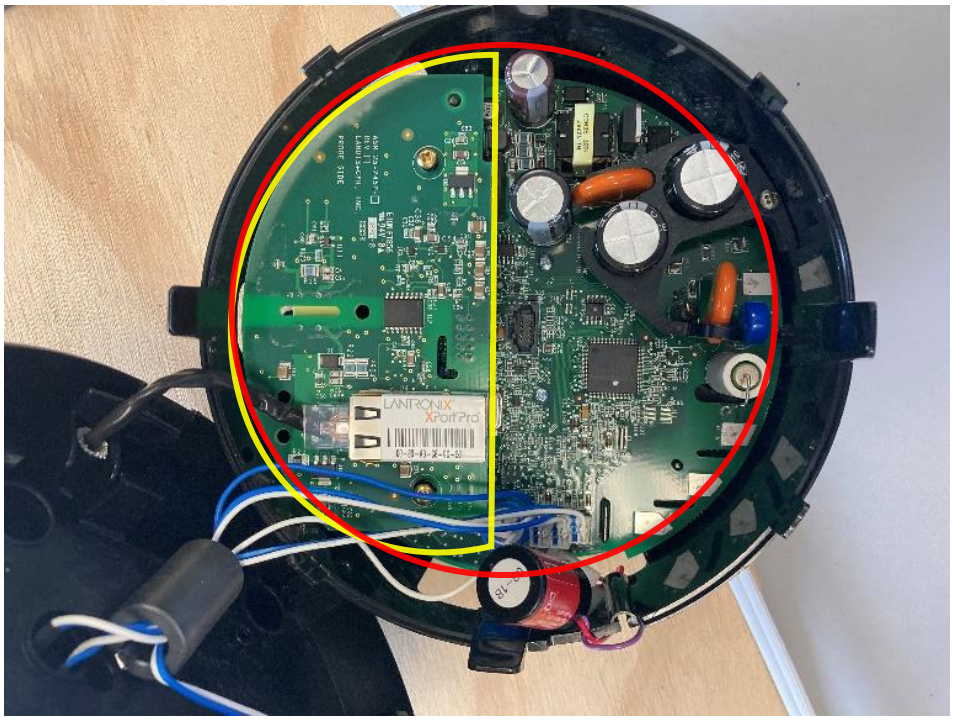

Figure 66. Communication enclosed in a yellow perimeter while the metrology board is enclosed in a red perimeter.

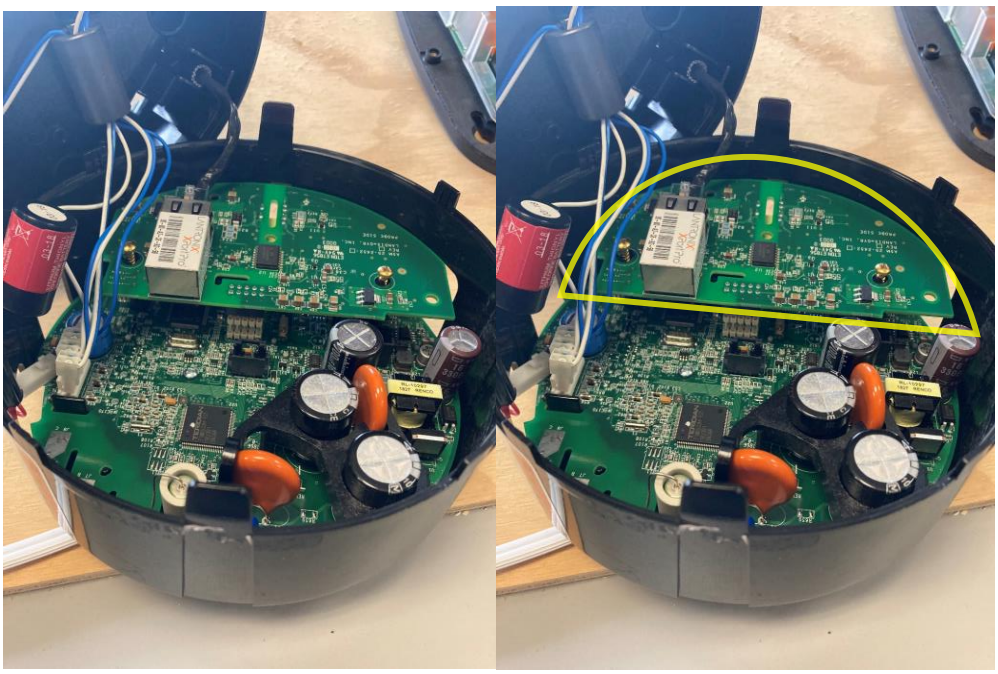

Figure 67. Different angle of S4x Ethernet internal circuitry. The communication module is enclosed in a yellow perimeter.

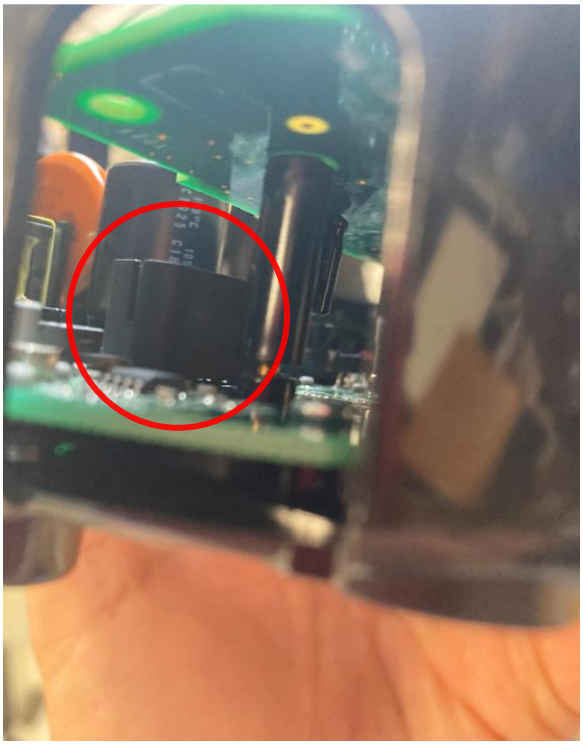

Figure 68. Optical port in a S4x Ethernet meter is part of the metrology board.

From Figures 65, 66, 67, 68, and 69**,** it can be noticed that the smart meter consists of the integration of two electronic boards. The board at the top is the communication module, which contains the RJ-45 ethernet connection and a Lantronix XPort embedded device server [61]. The board at the bottom is the metrology board, which oversees translating the received signal from the power line and determine the values of current, voltage, and energy, among others. The metrology board is the one that stores all the meter data such as the readings, user-configurations, time, and date information, and it is also the one that has the optical port attached. Another experiment consisted of establishing a successful optical communication session after disconnecting the communication module from the metrology board. Like in previous attack experiments, no effect was noticeable during the session. This lead to conclude that both boards are independent of each other. If the ethernet communication is down, meter data can still be retrieved using optical communication. Based on the analysis, Figure 70 below represents the flow of data from the power line to the monitoring computer.

Figure 69. (Left) Metrology module and communication module from a S4x Ethernet meter disassembled. (Right) S4x Ethernet communication module.

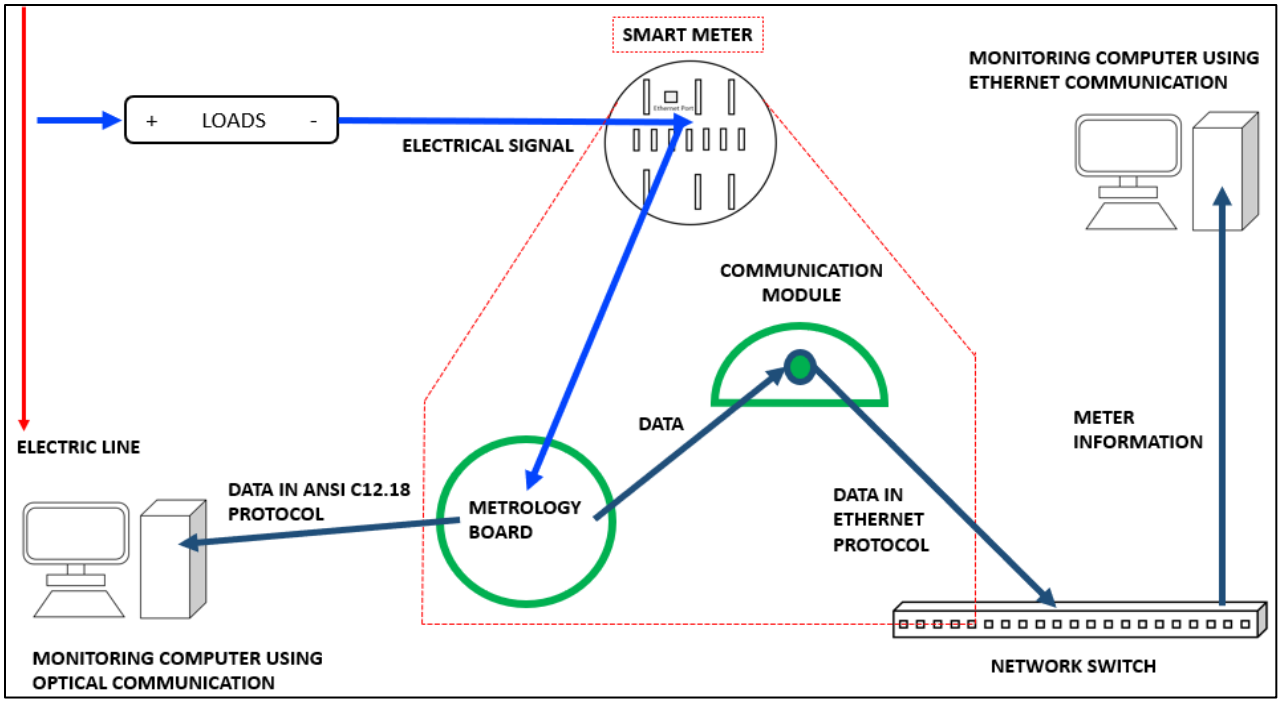

Figure 70. S4x Ethernet metering data flowing

CHAPTER VI

DISCUSSIONS, CONCLUSIONS, AND FUTURE WORK

6.1 Comparing Differences Between Meters in the Market

A last analysis was done after the observation that all three meters presented different values of resiliency against DOS attacks. The technology constituting the network interface cards of the meters are not the same. Using the finding that the metrology board did not seem to be affected, left the conclusion that the element of the smart meter that was directly affected was the communication module. This module is different between all three meters, as this could be the reason for the difference in results. For both Landis+Gyr S4x Ethernet and General Electric EPM 7000, the modules are physically independent. In the case of the General Electric EPM 6100, both, the metrology board and the communication module seem to be integrated in the same board, yet both maintain their individuality.

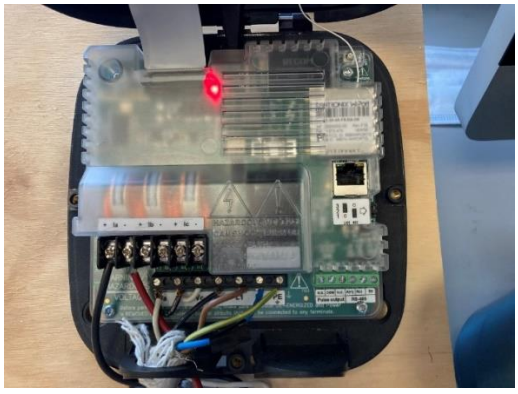

Figure 71. EPM 6100 Internal Circuit.

Figure 72. S4x Ethernet internal circuit.

Figure 73. EPM 7000's network interface card.

6.2 Consequences of Traffic Attacks in Smart Grids

Although the data was not sufficient to conclude that traffic attacks cause a significant impact when it comes to meter consumption data, there was enough evidence to prove that it does cause a Denial-of-Service Attack. A minimum effective attack bandwidth (MEAB) was identified for all meters tested to cause the DOS, and as long as this one is reached, communication with the targeted meter is impossible. Using the tools provided by the meter manufacturing companies does not help identifying the source of the interruption in communication. In other words, the meter manufacturing companies, and the utility companies

would not be able to identify the system failure as an actual intended DOS. From the point of view of all users, the nature of the problem would be interpreted as a simple meter malfunction.

The other effect caused by traffic attacks is a delay that meters take to resume communicating after an effective ping flooding or TCP/SYN attack takes place. To create the maximum possible delay, two parameters were involved: attack bandwidth, and attack duration. Results indicate that applying an attack bandwidth higher than the MEAB for a minimum duration of 60 seconds would ensure a delay effect. Increasing either the attack bandwidth or the duration of the attack does not cause a significant difference.

Since the DOS attack does not leave traces in the smart grid system, meter service providers would have no other choice than treating the problem caused as if the source is a meter malfunction. This implies the useless intervention of a technician and a probable replacement of equipment. In conclusion, for every meter attacked, there will be a cost of money wasted in replacements and man-labor without mentioning that the meters replaced would not have any real defect, plus meter manufacturing companies will be forced to spend money in investigations to detect the source of the defect within the meter limits, when the source is out of the meter boundaries.

6.3 Conclusion

As a conclusion from our experiments, the following eight observations were made:

1. Ping-Floods, Smurf attacks, and TCP/SYN attacks create the effect of complete loss of communication in smart meters (DOS attack).
2. A minimum effective attack bandwidth must be reached for a successful DOS attack.

3. There is an apparent positive relationship between the recovery time and the duration of attack, but this is only visible for short term durations (less than one minute). Once the attack duration surpasses one minute, the recovery times will stabilize in a defined range regardless of how long the attack lasts.
4. There is also an apparent positive relationship between the recovery time and the attack bandwidth, but this is only visible if the MEAB is not surpassed. Once the attack bandwidth passes the MEAB, the recovery times will stabilize in a defined range regardless of how long the attack lasts regardless of how much the attack bandwidth increases.
5. For effective ping-flood attacks, the communication will return to normal between 50 to 60 seconds after the attack ceased. In the case of TCP/SYN attacks, the recovery times are different per meter.
6. Based on the required MEABs, ping-flood attacks seem to be more damaging than Smurf attacks when applied in smart metering communication.
7. The technology used for the network interface card of the meters, determines the resilience of them against certain data traffic attacks. Hence, based on the results obtained from the experiments performed in this research, the EPM 6100 meter was the most resilient against ping-flood and smurf attacks, but extremely weak against TCP/SYN attacks.
8. For the case of S4x Ethernet meter, network-based attacks do not interfere with the optical communication capabilities because of the separation of modules in the internal hardware of the smart meter.

Is apparent from these observations that smart metering communication is vulnerable to common DOS attacks. The purpose of this research was to analyze and learn about the final effect, and how is the overall communication system being affected by the attacks. These results would help companies understand the resilience of their meters against these common cyber-attacks, and they could define security mechanisms to identify traffic loads that surpass their MEABs and reject them before a successful DOS occurs. Although the occurrence of DOS attacks is less likely now due to current implemented security mechanisms like firewalls, companies must be aware that such mechanisms have been defeated before and having this security hole, makes the smart grid vulnerable.

6.4 Future Work

Some experiments raised the suspicion that performing several consecutive streams of traffic attacks, could lead to a total communication blockage of the meter victim; this meaning that the communication would not return unless the meter undergoes a power cycle. Future research should investigate how to replicate this scenario since its existence would represent a major thread.

Another area to investigate is the possible attacks using optical communication. Since the metrology board of the meter is shared with the optical communication system, there is a strong possibility that by affecting the optical communication system would indirectly affect the metrology system. A DOS attack may turn into a resource depletion attacks that attacks a battery power node by forcing it to respond or send several messages until the power is depleted [58]. Learning how to build data packets with ANSI C12.18 would provide the opportunity to investigate how to create dummy data packets similar to the ICMP's echo requests and

responses. Since the idea of the attack relies on the fact that the attacker does not wait for acknowledge packets and responses, using ANSI C12.18 to create identification packets without the need to wait for the acknowledgment packet would replicate the same scenario as the already mentioned DOS attacks. The string EE0000000001201310 is the basic identification request using ANSI C12.18. Numbers 0001 indicate that the data packet consists of only one byte, number 20 indicates the data packet is using an identification request service and number 1310 is the CRC.

Figure 74 is a snippet of a portion of Figure 64 to focus on the possible area to introduce the concept. As it can be seen from Figure 84, there exists a time gap of 20 milliseconds between the identification packet and the acknowledgment packet. The next time gap is around 49 milliseconds, which is the time that took the user's device to receive the response packet from the smart meter. In total, the approximate time that takes between sending the identification request and receiving the response is 69 milliseconds.

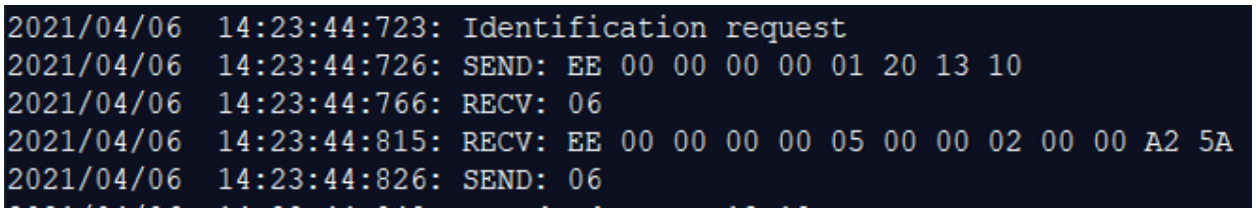

Figure 74. Log file showing details of the sending of an identification request packet and the response from the smart meter.

Optical communication attacks are an area that has not been studied in the smart metering communication science, and therefore, further studies can be done in this regard.

REFERENCES

[1] SmartGrid.gov. What is the Smart Grid? US Department of Energy, Office of Electricity Delivery & Energy Reliability. Retrieved on 2019 from https://www.smartgrid.gov/the_smart_grid/smart_grid.html

[2] Le, Nghia & Chin, Wen-Long & Truong, Dang & Nguyen, Tran. (2016). Advanced Metering Infrastructure Based on Smart Meters in Smart Grid. 10.5772/63631.

[3] Gungor V. C., Sahin D., Kocak T., Ergut S., & Bucella C. (2011). Smart Grid Technologies: Communication Technologies and Standards. Retrieved from IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 7, NO. 4.

[4] Gungor, V.C. & Lambert, Frank. (2006). A Survey on Communication Networks for Electric System Automation. Computer Networks. 50. 877-897. 10.1016/j.comnet.2006.01.005.

[5] V. C. Gungor, B. Lu, & G. P. Hancke, Opportunities and challenges of wireless sensor networks in smart grid. IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3557–3564, Oct. 2010.

[6] D. M. Laverty, D. J. Morrow, R. Best, & P. A. Crossley, Telecommunications for smart grid: Backhaul solutions for the distribution network. in Proc. IEEE Power and Energy Society General Meeting, Jul. 25–29, 2010, pp. 1–6.

[7] Uribe-Pérez, Noelia & Hernández-Callejo, Luis & Vega, David & Angulo, Itziar. (2016). State of the Art and Trends Review of Smart Metering in Electricity Grids. Applied Sciences. 6. 68-92. 10.3390/app6030068.

[8] Public Utility Commision of Texas. Smart Metering. Retrieved on 2021 from https://www.puc.texas.gov/consumer/electricity/Metering.aspx.

[9] U.S Department of Energy. Electric Meters. Retrieved on 2020 from https://www.energy.gov/energysaver/appliances-and-electronics/electric-meters.

[10] Koponen, Pekka & Saco, Luis & Orchard, Nigel & Vorisek, Tomas & Parsons, John & Rochas, Claudio & Morch, Andrei & Lopes, Vitor & Togeby, Mikael. (2008). Definition of Smart Metering and Applications and Identification of Benefits.

[11] U.S Energy Information Administration. How Many Smart Meters are Installed in the United States, and who has them? Retrieved on 2020 from https://www.eia.gov/tools/faqs/faq.php?id=108&t=3

[12] R. R. Mohassel, A. Fung, F. Mohammadi and K. Raahemifar, "Application of Advanced Metering Infrastructure in Smart Grids," 22nd Mediterranean Conference on Control and Automation, 2014, pp. 822-828, doi: 10.1109/MED.2014.6961475.

[13] V. C. Gungor, D. Sahin, T. Kocak, & S. Ergüt, Smart grid communications and networking. Türk Telekom, Tech. Rep. 11316-01, Apr. 2011.

[14] Landis+Gyr. RFmesh. 2009. Retrieved on 2021 from https://www.landisgyr.com/webfoo/wp-content/uploads/2012/12/RFMeshBrochure.pdf

[15] M. Rafiei, S. M. Elmi and A. Zare, "Wireless communication protocols for smart metering applications in power distribution networks," 2012 Proceedings of 17th Conference on Electrical Power Distribution, 2012, pp. 1-5.

[16] W. Li and X. Wang, "Notice of Retraction: The Research of AMR in Smart Meter," 2010 Asia-Pacific Power and Energy Engineering Conference, 2010, pp. 1-4, doi: 10.1109/APPEEC.2010.5448275.

[17] Li Li; Xiaoguang Hu; Jian Huang; Ketai He. Research on the architecture of Automatic Meter Reading in Next Generation Network. IEEE international conference on industrial informatics , 13-16 july 2008 , pp. 92-97.

[18] U. S. Department of Energy, Office of Electricity Delivery and Energy Reliability: Advanced Metering Infrastructure and Customer Systems. (2016). Retrieved on 2020 from: https://www.energy.gov/sites/prod/files/2016/12/f34/AMI%20Summary%20Report_09-26-16.pdf

[19] U. S. Department of Energy, Office of Electricity Delivery and Energy Reliability: Advanced Metering Infrastructure. (2008). Retrieved on 2020 from: https://netl.doe.gov/sites/default/files/Smartgrid/AMI-White-paper-final-021108--2--APPROVED_2008_02_12.pdf

[20] M. Wagner, M. Kuba and A. Oeder, "Smart grid cyber security: A German perspective," 2012 International Conference on Smart Grid Technology, Economics and Policies (SG-TEP), 2012, pp. 1-4, doi: 10.1109/SG-TEP.2012.6642389.

[21] Murrill, Brandon J.; Liu, Edward C. & Thompson, Richard M., II. Smart Meter Data: Privacy and Cybersecurity, report, February 3, 2012; Washington D.C.. (https://digital.library.unt.edu/ark:/67531/metadc87204/: accessed February 7, 2020), University of North Texas Libraries, UNT Digital Library, https://digital.library.unt.edu; crediting UNT Libraries Government Documents Department.

[22] Pallotti, Emiliano & Mangiatordi, Federica. (2011). Smart grid cyber security requirements. 10.1109/EEEIC.2011.5874564.

[23] S. Ahmed, T. M. Gondal, M. Adil, S. A. Malik and R. Qureshi, "A Survey on Communication Technologies in Smart Grid," 2019 IEEE PES GTD Grand International Conference and Exposition, 2019, pp. 7-12.

[24] Hafeez, Ayesha & Kandil, Nourhan & Al-Omar, Ban & Landolsi, T. & Al-Ali, A.R.. (2014). Smart Home Area Networks Protocols within the Smart Grid Context. Journal of Communications. 9. 665-671. 10.12720/jcm.9.9.665-671.

[25] Mendes, T.D.P. & Godina, Radu & Rodrigues, Eduardo & Matias, João & Catalão, João. (2015). Smart Home Communication Technologies and Applications: Wireless Protocol Assessment for Home Area Network Resources. Energies. 8. 7279-7311. 10.3390/en8077279.

[26] John Sonnenberg. Serial Communications RS232, RS485, RS422. 2018. Raveon Technologies. Retrieved on 2020 from: https://www.raveon.com/wp-content/uploads/2019/01/AN236SerialComm.pdf

[27] Kugelstadt Thomas. The RS-485 Design Guide. Texas Instruments. 2016. Retrieved on 2020 from: https://www.ti.com/lit/an/slla272d/slla272d.pdf?ts=1638808796487&ref_url=https%253A%252F%252Fwww.google.com%252F

[28] European Telecommunications Standards Institute. ETSI TS 104 001 V2.1.1 (2016-12) Technical Specification Open Smart Grid Prototol (OSGP); Smart Metering/Smart Grid Communication Protocol. Retrieved on 2020 from: https://www.etsi.org/deliver/etsi_ts/104000_104099/104001/02.01.01_60/ts_104001v020101p.pdf

[29] National Electrical Manufacturers Association. 1996. Protocol Specification for ANSI Type 2 Optical Port.

[30] National Electrical Manufacturers Association. 2014. ANSI C12.19-2012 American National Standard for Utility Industry End Device Data Tables.

[31] National Electrical Manufacturers Association. 1996. Protocol Specification for Telephone Modem Communication.

[32] American National Standards Institute. National Electrical Manufacturers Association. Protocol Specification For Interfacing to Data Communication Networks. 2008

[33] Z. Lipošćak and M. Bošković, "Survey of smart metering communication technologies," Eurocon 2013, 2013, pp. 1391-1400, doi: 10.1109/EUROCON.2013.6625160.

[34] Acromag. INTRODUCTION TO MODBUS TCP/IP. 2005. Retrieved on 2019 from: https://www.prosoft-technology.com/kb/assets/intro_modbustcp.pdf

[35] Modbus-IDA. MODBUS MESSAGING ON TCP/IP IMPLEMENTATION GUIDE V1.0b. 2006. Retrieved on 2019 from: https://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf

[36] Modbus.org. MODBUS/TCP Security. 2018. Retreived on 2019 from: https://modbus.org/docs/MB-TCP-Security-v21_2018-07-24.pdf

[37] International Telecommunications Union. Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3 PLC networks. 2017

[38] Landis+Gyr: Company Profile Financial Year 2015-2016. Retrieved on 2019 from https://www.landisgyr.eu/webfoo/wp-content/uploads/2012/09/landis-gyr-company-profile-financial-year-2015-2016-ENGLISH-ds-1.pdf

[39] Beroset, Edward. (2014). On the interaction between checksums and cyclic redundancy codes in communications protocols. 1-3. 10.1109/ISGT.2014.6816439.

[40] Snyder, Aaron & Ramirez, P.. (2007). The newly revised ANSI C12.19 and its application across the utility enterprise. 10.1109/PSAMP.2007.4740905.

[41] AL-Madani, Basem & Ali, Hassan. (2017). Data Distribution Service (DDS) based implementation of Smart grid devices using ANSI C12.19 standard. Procedia Computer Science. 110. 394-401. 10.1016/j.procs.2017.06.082.

[42] Snyder, Aaron & Garrison Stuber, Michael. (2007). The ANSI C12 protocol suite - updated and now with network capabilities. 117 - 122. 10.1109/PSAMP.2007.4740906.

[43] S. Rana, H. Zhu, C. W. Lee, D. M. Nicol and I. Shin, "The Not-So-Smart Grid: Preliminary work on identifying vulnerabilities in ANSI C12.22," 2012 IEEE Globecom Workshops, 2012, pp. 1514-1519, doi: 10.1109/GLOCOMW.2012.6477810.

[44] R. P. Lewis, P. Igic, & Z. Zhongfu, Assessment of communication methods for smart electricity metering in the U.K. in Proc. IEEE PES/IAS Conf. Sustainable Alternative Energy (SAE), Sep. 2009, pp. 1–4.

[45] Shongwe, Thokozani & Vinck, Jan. (2013). Interleaving and nulling to combat narrow-band interference in PLC standard technologies PLC G3 and PRIME. 258-262. 10.1109/ISPLC.2013.6525860.

[46] M. Malek, D. Ketel, H. Hirsch and M. Trautmann, "Investigation of smart meters using G3 PLC," 2016 International Symposium on Electromagnetic Compatibility - EMC EUROPE, 2016, pp. 162-166, doi: 10.1109/EMCEurope.2016.7739276.

[47] Wenpeng Luan, D. Sharp and S. Lancashire, "Smart grid communication network capacity planning for power utilities," IEEE PES T&D 2010, 2010, pp. 1-4, doi: 10.1109/TDC.2010.5484223.

[48] Landis+Gyr. Commercial + Industrial: E650 S4x Ethernet. Retrieved on 2020 from: https://www.landisgyr.com/product/e650-s4x-meter/

[49] General Electric. EPM 6100 Power Quality Meter. Retrieved on 2020 from: https://www.gegridsolutions.com/multilin/catalog/epm6100.htm

[50] General Electric. EPM 7000 Power Quality Meter. Retrievedon 2020 from: https://www.gegridsolutions.com/multilin/catalog/epm7000.htm

[51] Nakashima Ellen. Foreign hackers targeted U.S. water plant in apparent malicious cyber attack, expert says. 2011. Retrieved on 2021 from: https://www.washingtonpost.com/blogs/checkpoint-washington/post/foreign-hackers-broke-into-illinois-water-plant-control-system-industry-expert-says/2011/11/18/gIQAgmTZYN_blog.html

[52] V. Aravinthan, B. Karimi, V. Namboodiri and W. Jewell, "Wireless communication for smart grid applications at distribution level — Feasibility and requirements," 2011 IEEE Power and Energy Society General Meeting, 2011, pp. 1-8, doi: 10.1109/PES.2011.6039716.

[53] Khaed S., Zouheir T., Mohammad A., Ahmed G., & Mahmoud Alahmad. Resiliency of Smart Power Meters to Common Security Attacks. Procedia Computer Science 53, pp. 145-152, 2015.

[54] N. Liu, J. Chen, L. Zhu, J. Zhang, & Y. He. A key management scheme for secure communications of advanced metering infrastructure in smart grid. IEEE Trans. Ind. Electron. 2013;60(10):4746–4756.

[55] M. Nabeel, S. Kerr, Xiaoyu Ding and E. Bertino, "Authentication and key management for Advanced Metering Infrastructures utilizing physically unclonable functions," 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), 2012, pp. 324-329, doi: 10.1109/SmartGridComm.2012.6486004.

[56] Kumar, Sanjeev. (2006). PING attack – How bad is it?. Computers & Security. 25. 332-337. 10.1016/j.cose.2005.11.004.

[57] S. Kumar. Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet. IEEE Computer Society. 2007.

[58] Posel J. RFC 792. Internet Control Message Protocol. http://www.faqs.org/rfcs/rfc792.html September 1981.

[59] S. Kumar. Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet. IEEE Computer Society. 2007.

[60] Landis+Gyr. ANSI and IEC Optical Probe AIP200. Retrieved on 2020 from: https://www.landisgyr.com/product/ansi-iec-optical-probe-aip200/

[61] Lantronix. Xport. Retrieved on 2021 from: https://www.lantronix.com/products/xport/#tab-overview

BIOGRAPHICAL SKETCH

The author, Oscar A. Alvarez, was born on December 7, 1991, in Mexico and lived the first eighteen years of his life in his home city, Reynosa, Tamaulipas. In June 2010, after being awarded a technical degree in Mechatronics, Oscar came to the United States to pursue a higher-level education, and in December 2019, Oscar married his wife, Adelaeda Barrera, and since, he has been living in Edinburg, Texas.

In May 2015, Oscar obtained his bachelor's degree in Engineering Physics and Computer Engineering from the University of Texas at Brownsville. While completing his university studies, Oscar participated in NASA design competitions where he was presented with multiple first place awards. After obtaining his engineering degree, Oscar was given the opportunity to work as a Software Development Engineer for Landis+Gyr, where he mastered skills and knowledge of smart grid science, and in April 2021, the company promoted him to become the Software Applications Supervisor.

In December 2021, he was awarded with a master's degree of science in Electrical Engineering. Oscar's master studies specialized in cyber-security and network engineering. He has presented posters in HESTEC (Hispanic Engineering, Science, and Technology) week and at the ICDIS (International Conference on Data and Information Security) and participated in the creation of two research papers in smart metering cyber-security. For more information, Oscar A. Alvarez can be contacted via email at oscaralvarez5675@gmail.com.