Intrusion Detection of Flooding DoS Attacks on Emulated Smart Meters

Yousef Akbar

Thesis submitted to the faculty of the Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science
In
Electrical Engineering

Chen-Ching Liu, Chair
Virgilio A. Centeno
Jaime De La Ree Lopez

April 27, 2020
Blacksburg, Virginia

Keywords: Denial of Service (DoS), Advanced Metering Infrastructure (AMI), Wireless Mesh Network (WMN), Cyber-Physical System (CPS), Power Grid, Supervisory Control And Data Acquisition (SCADA), Cyber Security of Smart Meters.

Intrusion Detection of Flooding DoS Attacks on Emulated Smart Meters

Yousef Akbar

ABSTRACT

The power grid has changed a great deal from what has been generally viewed as a traditional power grid. The modernization of the power grid has seen an increase in the integration and incorporation of computing and communication elements, creating an interdependence of both physical and cyber assets of the power grid. The fast-increasing connectivity has transformed the grid from what used to be primarily a physical system into a Cyber- Physical System (CPS). The physical elements within a power grid are well understood by power engineers; however, the newly deployed cyber aspects are new to most researchers and operators in this field. The new computing and communications structure brings new vulnerabilities along with all the benefits it provides. Cyber security of the power grid is critical due to the potential impact it can make on the community or society that relies on the critical infrastructure. These vulnerabilities have already been exploited in the attack on the Ukrainian power grid, a highly sophisticated, multi-layered attack which caused large power outages for numerous customers. There is an urgent need to understand the cyber aspects of the modernized power grid and take the necessary precautions such that the security of the CPS can be better achieved. The power grid is dependent on two main cyber infrastructures, i.e., Supervisory Control And Data Acquisition (SCADA) and Advanced Metering Infrastructure (AMI). This thesis investigates the AMI in power grids by developing a testbed environment that can be created and used to better understand and develop security strategies to remove the

vulnerabilities that exist within it. The testbed is to be used to conduct and implement security strategies, i.e., an Intrusion Detections Systems (IDS), creating an emulated environment to best resemble the environment of the AMI system. A DoS flooding attack and an IDS are implemented on the emulated testbed to show the effectiveness and validate the performance of the emulated testbed.

Intrusion Detection of Flooding DoS Attacks on Emulated Smart Meters

Yousef Akbar

GENERAL AUDIENCE ABSTRACT

The power grid is becoming more digitized and is utilizing information and communication technologies more, hence the smart grid. New systems are developed and utilized in the modernized power grid that directly relies on new communication networks. The power grid is becoming more efficient and more effective due to these developments, however, there are some considerations to be made as for the security of the power grid. An important expectation of the power grid is the reliability of power delivery to its customers. New information and communication technology integration brings rise to new cyber vulnerabilities that can inhibit the functionality of the power grid. A coordinated cyber-attack was conducted against the Ukrainian power grid in 2015 that targeted the cyber vulnerabilities of the system. The attackers made sure that the grid operators were unable to observe their system being attacked via Denial of Service attacks. Smart meters are the digitized equivalent of a traditional energy meter, it wirelessly communicates with the grid operators. An increase in deployment of these smart meters makes it such that we are more dependent on them and hence creating a new vulnerability for an attack. The smart meter integration into the power grid needs to be studied and carefully considered for the prevention of attacks. A testbed is created using devices that emulate the smart meters and a network is established between the devices. The network was attacked with a Denial of Service attack to validate the testbed performance, and an Intrusion detection method was developed and applied onto the

testbed to prove that the testbed created can be used to study and develop methods to cover the vulnerabilities present.

Acknowledgements

I am grateful to my parents and siblings for supporting me throughout my life and pushing to achieve my goals.

I would like to thank the Kuwaiti government for providing me the opportunity and sponsoring my higher education. Without the support of my government I would have never been able to pursue of my academic ambitions.

Much thanks and gratitude go to the faculty of PEC at Virginia Tech. I am very grateful to my advisor Dr. Chen-Ching Liu for his continuous guidance, encouragement, and wisdom throughout my work and studies. I could not imagine going through this experience without his continual support and patience. I am also very thankful to Dr. Virgilio Centeno and Dr. Jaime De La Ree Lopez for their endless support while being a student in PEC, and for providing me with guidance as members of my committee.

I have had many great experiences and memories during my time at Virginia Tech, thanks to the people I have met here. I am thankful to many of my fellow graduate students at PEC for the support and the good times we have had. I am grateful to the life-long relationships I have made at Virginia Tech.

I finally would like to thank all the professors during my undergraduate years at that pushed me to pursue a graduate degree. Much thanks to Dr. Raymond DeCarlo for his unforgettable lesson s, and for his immense wisdom and support.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

1.1 Motivation

There has been a major shift in creating and modernizing the power grid to what is now called a smart grid. Many elements play a role to make a smart grid “smart,” this is mainly achieved by increasing computing power, communication, and automation within the system for the purpose of improving the reliability and efficiency of the grid. By utilization of Information and Communications Technology (ICT) and transforming the grid into a cyber-physical system (CPS), power system operators and automatic system applications have much more data to work with in order to complete their tasks more effectively while also given the capability to remotely operate and control devices. However, the new data transfer and remote-control capabilities deployed on the grid also bring vulnerabilities and opportunities for adversaries to conduct malicious actions against the CPS, with the potential to cause serious damage. This was the case for Ukraine in 2015 [1], a large scale sophisticated and coordinated cyber-attack was launched against the Ukrainian power system, leading to major power outages. The attackers took many steps in advance of the main attack, the operation of the power system was monitored remotely, with the help of malware. The attacks managed to remotely control devices that can be accessed through communication capabilities, causing outages across the power system. The adversaries continued to conduct attacks to complicate and inhibit the restoration process through a Denial of Service (DoS) attack on the telecommunication system, such that telephone calls were unable to reach the call-center, inhibiting the outage management system. Malware was also used to stop the operation of software that was installed to help power system operators gather information about the outages for the system restoration efforts. The operators were blinded by the inability to know the affected areas of outages, thereby increasing the duration of customer outages. This attack is proof that there exist many vulnerabilities within power systems that utilize ICT.

Smart meter deployment is also increasing significantly in power systems[2]. Current deployment of smart meters globally is at approximately 800 million units. The AMI system has evolved from the Automatic Meter Reading (AMR) meters. There is interoperability between older units and newer smart meters. AMI makes it possible for energy usage data to be recorded at a much higher detail, while also giving operators the ability to remotely control access to power by customers. AMI is developed with the intended purposes of customer load forecast, demand response, and dynamic pricing, and outage management. The power system is becoming more dependent on AMI, since it provides these features that can increase efficiency and reliability of the power grid. This makes AMI a potential target for attackers. As mentioned previously, the call-centers of the Ukraine power grid were attacked to inhibit outage management efforts. An attack on AMI not only hurts the outage management systems, but also other systems that depend upon smart meter data. Consequently, the cyber security of AMI has become a great concern. Data privacy is an important issue for customers, while data integrity and availability are crucial for power system operation and services. These vulnerabilities have been acknowledged by researchers and power industry; however, the intrusion detection methods proposed often neglect the limited computational resources of the smart meter environment. Highly secure routing protocols are proposed; however, issues of the computational overhead and practical applicability remain to be addressed.

A smart meter and AMI testbed can help in demonstrating the limitations and vulnerabilities of the real AMI system. AMI is usually simulated on network simulators such as ns-3 or SIMULINK. However, with simulations it is difficult to develop a holistic and fully encompassing simulation of a given system. There exist testbeds created by national labs for SCADA systems such is the case for Idaho National Laboratory (INL) with NSTB, [3]. However, this does not focus on AMI, this test bed is also a large-scale costly project. Some physical devices have been used to emulate the smart meters [4], but not for cyber security assessment. Reference [5] has emulated devices; however, the devices used in the testbed are software development boards provided by industry for the development of applications on a given smart meter rather than the testing the cyber security of the smart meter device in AMI.

1.2 Objectives and Contributions

The reliance and utilization of AMI and smart meter data in power systems is increasing. Consequently, the deployment of smart meters is also common in the power industry. Cyber security of AMI in the smart grid is hence becoming more urgent. AMI's performance and security requires a cost-effective method to improve the security while maintaining normal operation of the network.

The main contribution of this thesis is the development of a realistic emulated testbed of smart meters within an AMI system with the goal to provide a platform for evaluation of

IDSs and other applications. The testbed creates a physically comparable device within a system, while having the flexibility to allow different types of attacks to be conducted and evaluated. The attacks can be induced on an emulated device that represents a smart meter in the AMI network, the consequent behavior of the device is very important such that they can be used for IDS and network analysis applications. This thesis demonstrates a flooding DoS attack with a simple IDS which is put in place within the testbed to validate the usability and realistic behavior of the emulated devices in the testbed.

1.3 Survey of the State-of-the-Art

The evolution of the power grid into a CPS that is heavily dependent on communication and networking systems is bringing about serious vulnerabilities. Many researchers have observed these vulnerabilities. Techniques to solve the cyber vulnerability problems have been proposed , e.g., [6]–[11]. The AMI system is a large new system that is being utilized heavily by the power industry. Hence, it is essential to assess and resolve the inherent vulnerabilities through different means. Machine learning methods are applied in order to design and implement IDSs on the AMI network, [12], [13]. Machine Learning methods, Support Vector Machine (SVM), for IDS is intuitive and effective as an application for this problem. However, the inherent limitation is that the lack of computational power needs to be taken into account for the AMI system. The AMI system is a type of Wireless Mesh Network (WMN) and uses routing protocols of Ad-Hoc nature. Extensive research has been done on WMN and a significant vulnerability within WMN is the Ad-Hoc routing protocols implemented on them [14], [15]. A common approach is to change the routing protocols or modifying them such that they are more secure, especially against DoS attacks [16]–[18] There have also been preventive measures, in which the network operators would send out a malware or status check of the existing smart meters within the AMI network [19]–[21]. While these checks are sent out to the smart meters in intervals, the system is still vulnerable within the interval window. These status checks also increase the burden and load on the AMI network. The IDS's, new modified routing protocols, and preventative status checking messaging increase the overhead computation of the AMI network as well as network traffic. Network traffic can be affected by the lack of consideration made in the proposed methods to increase security of the smart meters and the AMI system. When addressing vulnerabilities within a given network, the so called CIA triad is often used as the requirements, i.e., Confidentiality, Integrity, and Availability of the data packets [22]. A practical, realistic, and relatively low-cost testbed is necessary to validate the practicality of IDSs and network or system modifications.

1.4 Organization of this Thesis

This thesis includes 6 chapters. The remainder of this thesis is organized as follows: Chapter 2: provides an introduction to the AMI system and the discusses the cyber security vulnerabilities of the system. Hardware choices, modelling, and configuration of the testbed are covered in Chapter 3:. Chapter 4: provides the model for attack and IDS for the validation of the testbed. Chapter 5: contains the results of a flooding DoS cyber-attack conducted on the testbed and the use of the IDS. The results are discussed and provide validation of the developed testbed. Chapter 6: includes the conclusions of the work along with ideas and recommendations for the future work.

Chapter 2: AMI and Cyber Security

2.1 AMI

Power systems are separated into the transmission system and the distribution system. Details of the ICT in transmission systems and SCADA is outside the scope of this thesis; however, a brief overview is needed to provide the context. The transmission system's main task is to deliver power from the power plants to load concentrations at a distance. SCADA's primary purpose is to allow the power system to be better monitored and controlled from a remote control center. In SCADA, measurements are acquired from and control commands are communicated to the substations where measurement instrumentation and switching devices are located.

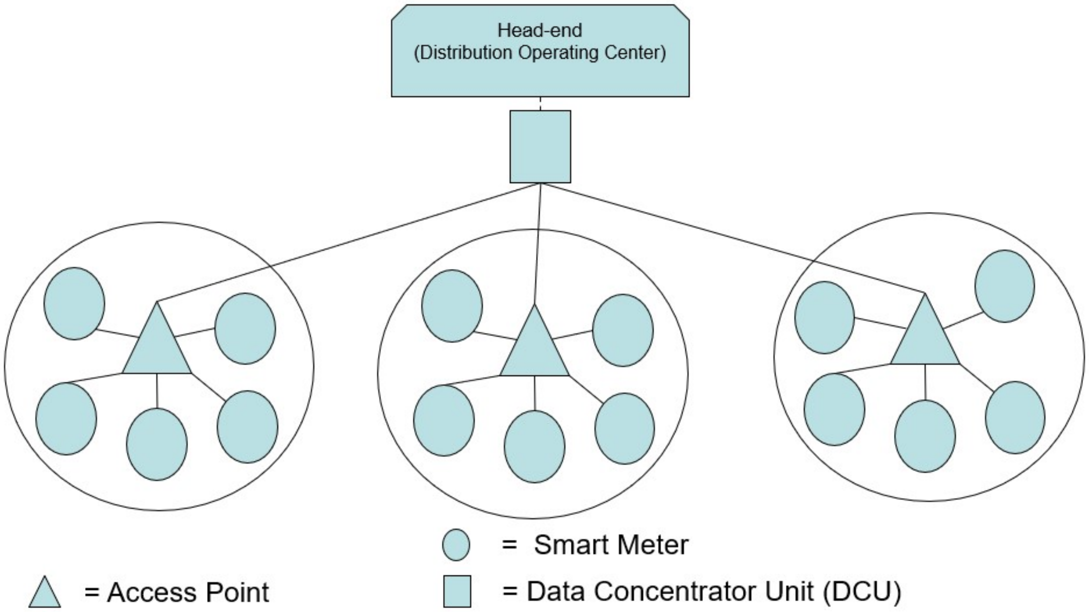

Head-end
(Distribution Operating Center)
= Smart Meter
= Access Point
= Data Concentrator Unit (DCU)

Figure 1. General Topology of AMI

ICT in distribution systems have multiple parts; AMI is an ICT system operating in the distribution level. The AMI's primary purpose is data collection from customers for billing, thus it was developed independently from SCADA. Distribution Automation (DA) is another system which lies within the ICT of distribution systems. AMI is the main ICT system that this thesis will focus on. Distribution systems have seen an increase in digitization of the devices used and the systems put in place. The digital devices provide wireless control (automated) capabilities. The remote monitored devices include smart meters, distributed energy resources and smart inverters, voltage regulators, and remote-controlled switching devices (e.g., circuit breakers). The smart meters within the AMI network are commonly seen to operate using Ad-Hoc routing protocols to communicate and add new devices into the network [23]. The choice of an Ad-Hoc routing protocol is due to the ease and convenience for new devices to be added to the infrastructure. This is important for AMI, as the deployment of smart meters is increasing rapidly and the network needs to be flexible to accept new devices into the network [2]. The choice of routing protocol has its drawbacks; for example, it is vulnerable to attacks and was not developed with the main goal of security. Outage management systems have been developed to utilize these devices to support distribution system restoration [24]. The method has become more advanced and effective in efficient restoration efforts.

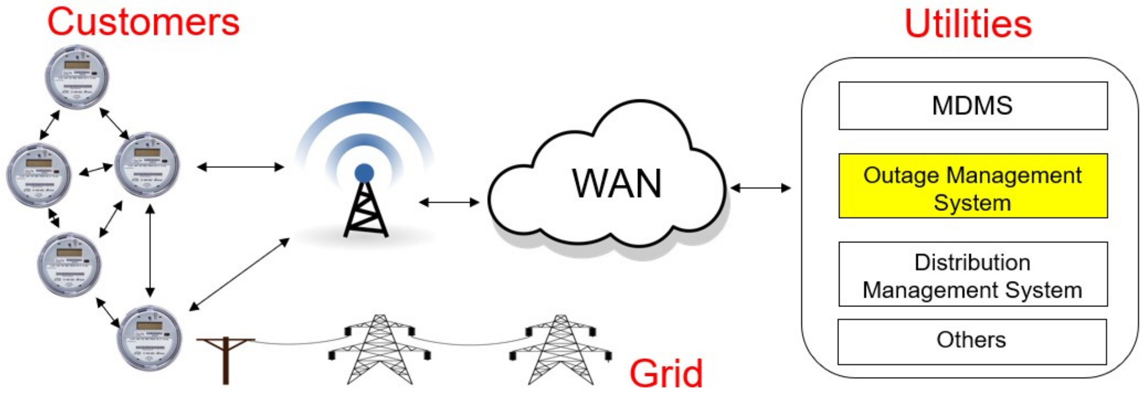


Figure 2. Customer and Utility ICT in AMI

2.2 Smart Meters

AMI is an extension of the AMR system; however, AMI includes more functions and could provide a higher resolution of data through smart meters together with better controllability. Modern smart meters have a higher data transmission rate. Furthermore, control commands can also be received, which is not possible for AMR [10]. The new smart meters with AMI have a larger scope of functionality. The increase in data resolution and rate of transmission as well as the full-duplex communication functionality of smart meters provide load demand flexibility. AMI makes it possible for the development of customer energy markets, in which consumers can choose to produce power through roof-top solar, wind generation, or electric vehicles. A great deal of flexibility and functionality is added within the distribution system due to smart meters and AMI.

The networks within AMI can be separated into several network architectures. The communication path from the control center to the field devices or smart meters, and vice versa, is achieved using multiple network architectures and communication protocols with the capability to interface between themselves. Home Area Network (HAN) is the network of customer devices including the PC(s) and other personal devices. Neighborhood Area Network (NAN) is the network which encompasses the smart meter devices in the AMI. Wide Area Network (WAN) is the network area where long distance transmission is conducted between larger entities or network, e.g. from utilities to the NAN. Local Area Network (LAN) refers to any network that operates within a specified enclosure, e.g., a home network or the network within the control center. Figure 3 shows a simplified network within the AMI in the distribution system. This thesis will focus mainly on the vulnerabilities and modelling of the NAN in AMI.

For a smart meter to have the functionality mentioned, it must be relatively complex internally, such is the nature of digital devices. The most distinguishing components of a smart meter are the current and voltage sensors. A digital communications module or card is needed for the wireless communication. The sensors and communication module are the essence of a smart meter. The components include a part of a computer or microprocessor with RAM and storage. Smart meters can have varying meter reading data transmission intervals for communication with a control center. The rate may vary from 5 to 60-minute intervals depending of the configuration of the meter and network traffic, the most common interval time is 15 minutes between meter reading transmissions [25]. While having a set interval to report the measurement data, smart meters have been observed to transmit the data in short bursts lasting over to 130ms [26]. Smart meters send data packets in pulses or bursts averaging around 100ms wide, rather than only sending one packet at a given interval period.

Smart meter specifications have changed since they were first deployed. The first deployed smart meter's communication modules had a Baud rate of 9600 while newer smart meters' communication modules have a much higher Baud Rate of 115200. The communication modules also vary in networking protocols between ZigBee and IEEE 802.15.4g. Taking that into consideration, the newer smart meters can handle higher data transmission and reception rates in comparison with older smart meters. The smart meters are the bottom of the hierarchy within the AMI system as illustrated in Figure 1. The AMI network's structure consists of smart meters that communicate to Access Points (AP) and Data Aggregators which then continue to move up to the Distribution Operation Center. The Distribution Operation Center has the Meter Data Management System (MDMS), Outage Management System (OMS), and Distribution Management System (DMS), etc. The AMI communication is defined in the IEEE 802.15.4 standard [27], and Ad-Hoc routing protocols are used [23]. Prior to AMI, customers had to call into call-centers to report their outages. This process could take minutes to hours. With smart meters, operators can receive the outage data within seconds or minutes following an outage, enhancing the restoration efficiency, and reducing the outage duration.

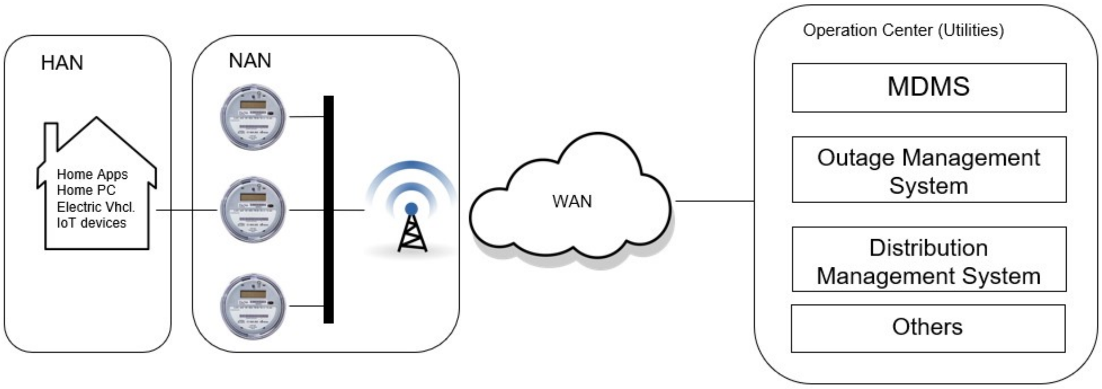


Figure 3. Communication and Network Model of a Distribution System

2.3 Cyber Security and Vulnerabilities of AMI

2.3.1 Network Vulnerabilities and Malicious Attacks

Smart meters are installed on the customer side within the AMI network, in contrast to most other devices within the smart grid. The ease of access makes the meters more susceptible to intrusions and attacks relative to other devices in the power system. Most of the devices in the power systems are located at the substations and on the utilities side. Smart meters provide utilities with energy consumption data for each customer, detailed consumption data, whilst the customer is billed based upon those measurements. This has prompted adversaries to attempt to either manipulate smart meter data to steal energy or monitor private customer data with a malicious intent [28], [29]. Smart meters are also susceptible to DoS attacks, as smart meter networks resemble WMNs. DoS attacks are a serious vulnerability for WMNs [30]. A DoS attack on smart meters would put a halt to the energy consumption data transmission, stopping it from reaching the utilities.

2.3.2 Smart Meter Vulnerabilities

Smart meters deployed in North America use a combination of both Zigbee and the IEEE 802.15.4g standard. The frequency bands used by both standards fall in the Industrial, Scientific, and Medical (ISM) region of the spectrum available, 900MHz or 2.4GHz. These frequency bands are widely used by commercial devices; thus, sniffers and other means of spectrum analysis and modulation are widely available to adversaries. An adversary can attack a smart meter through different means, as shown in Figure 4. The smart meter data packets can be targeted through the network. Tampering with the physical device is also possible by accessing the optical fiber port on the smart meter. An adversary can also target the voltage and current sensors of a smart meter such that the device reads and hence communicates false energy consumption data. The scope of this thesis will focus on the attacks that target the packets out of the communication module in the smart meter. However, the testbed to be established is aimed to be flexible enough to have the capability to implement attacks on different internals and hardware of a smart meter.

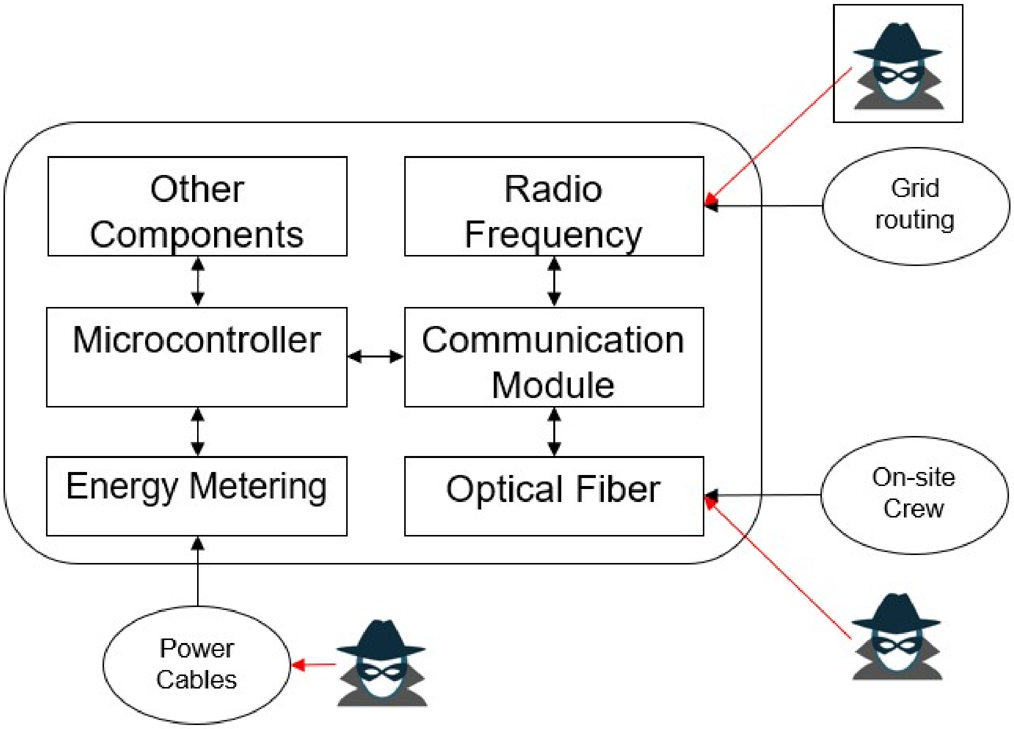


Figure 4. Smart Meter Vulnerable Targets for Attack

Integrity and Confidentiality of packets within the AMI network can be addressed using encryption on the packets being communicated. The Availability of packets is secured by changing routing protocols and using a more interconnected communication and network architecture. However, even with the efforts to satisfy the CIA triad requirements, vulnerabilities and flaws have been uncovered within the network architecture and protocols. Therefore, improvement on the security of the network is necessary and can be achieved.

Chapter 3: Hardware Modelling & Testbed Configuration

A smart meter is made up of many parts as mentioned in chapter 2. There are 5 main components on what makes the meter smarter and they provide the functionality that it has. Before thinking about modelling a smart meter, the internal hardware needs to be modeled and understood. See Figure 4 for an illustration of the internal hardware. The consideration of each component and understanding each of their vulnerabilities is important to modelling and emulating the devices. First, the main part of any digital device with computational capabilities is the CPU or microprocessor. The smart meter has a microprocessor with the ability to do simple tasks, this reflects the core capability of the device. The smart meter is not meant for computationally demanding tasks; rather, it is meant to send and receive data. There is no intention for complex calculations to be done within the smart meter. Hence, attempting to implement an IDS on smart meters is not a practical method for cyber security. A detection architecture with a centralized approach would be more practical. Second, the communication module, this is used for wireless transmitting and receiving data within the AMI network. This is a key component in a smart meter that allows it to communicate in a wireless network, using the Zigbee or IEEE 802.15.4g standards. The other components have less communication related vulnerabilities, including, RAM, Flash memory, and the sensor (CT and VT). The components mentioned are all part of what makes a smart meter; hence, an adversary may choose to attack and exploit any vulnerability within them. The flexibility and adaptability of a testbed is important, such that all possible vulnerabilities can be considered when establishing IDSs. To create and implement a holistic IDS, the flexibility and adaptability can be considered when creating an IDS on a network simulator alone. The scope of this thesis is to establish a flexible and realistic emulated testbed that resembles the physical smart meter device as closely as possible such that it can be used for cyber security evaluation and feasibility validation of the applications.

3.1 Hardware Modelling Options

There are many options and relevant technologies to choose from to build a smart meter. Some devices and technologies available may be too costly, have a steep learning curve, or have limited documentation for users. These factors can make future implementation, learning, and development difficult. The testbed also needs to factor in costs and availability of the products. An expensive product would make the testbed impractical for academic institutions that would like to have a smaller scale implementation of applications. The availability of a product allows the testbed to be easily maintained and documentation is more readily available for troubleshooting. A widely available product allows a flexible solution, as more hardware and software are developed and supported. A device that is supported by more vendors and products means the device's longevity and versatility should be higher. This means the device can be modified easily and updated along with a smart meter vendor and AMI network changes and developments. The hardware choice is a crucial decision before the establishment of a smart meter and AMI testbed.

3.1.1 Raspberry Pi, Arduino, and Smart Meter Dev Kits

When one wants to select a device, the base of the device needs consideration. For the processor of the device, there are three reasonable options to choose from. However, the smart meter dev kits automatically can be ruled off, as they are not compliant with the flexibility and availability requirement for the intended use case. The dev kits closely resemble the real smart meters, as they are provided by the smart meter manufacturers. The cost of purchasing the dev kits is also high, the intended usage of the kits is for software applications using smart meters. Cyber security, vulnerability assessment, and IDS applications are not the intended uses for the dev kits, making them a less viable option for the testbed although it is the most closely resembling and easiest option to go for.

The other two choices are the Arduino and Raspberry Pi. They are both widely available with extensive documentation and manuals. The two devices can interface with a wide range of hardware and devices, largely due to the popularity and availability of both devices. These options are perfect for creating a flexible and future resistant testbed. The Arduino is a micro-controller, while the Raspberry Pi is a full computer. The Arduino is only capable of repeatedly running a single program, while a Raspberry Pi has the functional flexibility of a normal computer. The Arduino uses its own proprietary programming language for its ease of use and simplicity. It is also well documented and popular for robotics applications [31].

Table 1. Raspberry Pi, Arduino, and Smart Meter Specification Comparison

	Raspberry Pi 4 – 1 – 4GB RAM	**Arduino Uno R3**	**GPRS CENTRON**
Price	$ 30 - $ 55	$ 29.95	n/a
CPU	ARM v8 – 64 bit	ATmega328P	ARM processor

	1.5GHz	16Mhz	– 32 bit
RAM	Up to 4GB	2KB	256KB
Storage	microSD Flash	32KB Flash	512 KB Flash
GPI/O	40	20	n/a
Operating System	Linux	n/a	n/a

The Raspberry Pi is the better option for the work of this thesis due to its flexibility with hardware attachments, ease of use, good documentation, and existence of a microprocessor, which is a functionally full computer and more flexible. The Raspberry Pi's hardware is similar to a typical smart meter's hardware as seen in Table 1 and [32]. The Raspberry Pi has 2 main board configurations, Raspberry Pi A and B. The difference between A and B is the IO locations on the board. The raspberry Pi 4 B is chosen. The configuration is more user friendly for the intended application. Three options for RAM capacities are available for the Raspberry Pi, i.e., 1GB, 2GB, and 4GB. A smart meter has a RAM capacity lower than 1GB, so a Raspberry Pi with 1GB of RAM is more than enough. Raspberry Pi is not tied to any specific programming language like the Arduino is, granting it the greater flexibility factor. Co-simulation and other interoperation of devices with simulations is much easier since Raspberry Pi is a Linux based machine. The Arduino requires less initial configuration as compared to Raspberry Pi; however, lacks the freedom and flexibility of using bash scripts to modify and configure the operations of the device and its connected hardware.

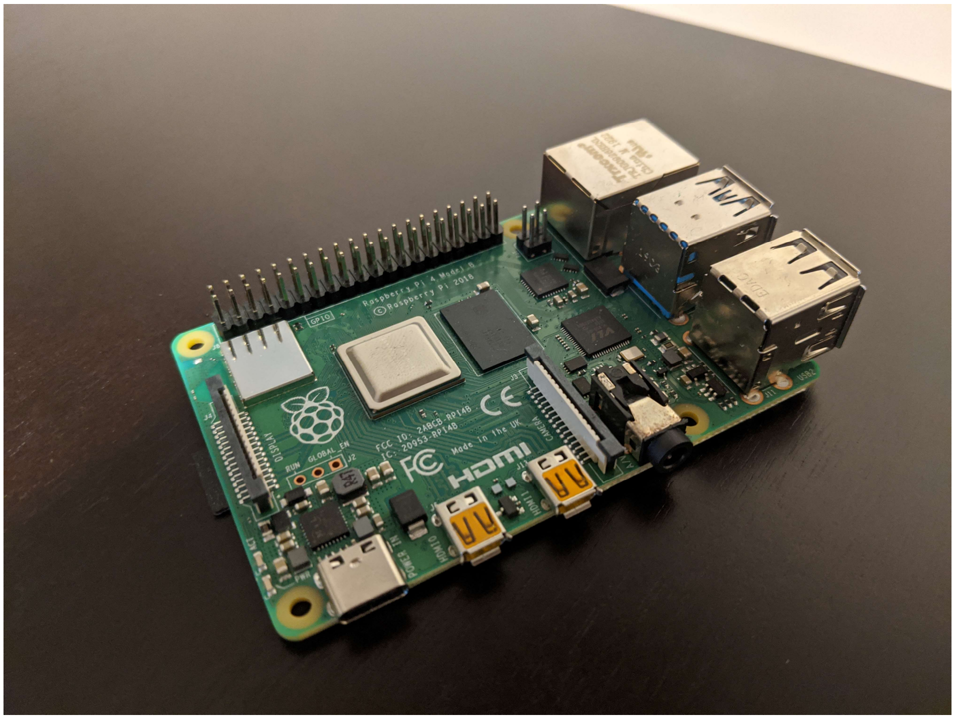


Figure 5. Raspberry Pi 4 model B

3.1.2 DIGI XBee Communication Modules

Smart meters have a communication module that communicates using Zigbee and IEEE 802.15.4g, the XBee communication module can handle both communication standards as well as BLE protocols [33]. The XBee module is a communication module that transmits and receives serial data and is compatible with Raspberry Pi. The protocol variety and flexibility of the XBee 3 module makes it a great choice for the proposed application, considering the variety of protocols that exist within the deployed smart meters in North America. The modules can interface directly through the GPIO of Raspberry Pi; however, this method is tedious. Alternatively, a USB adapter for the XBee modules can be used to plug into Raspberry Pi. The Sparkfun XBee Explorer USB was chosen to be used to interface the XBee modules with Raspberry Pi. The latest version of the XBee module is the series 3 module, an XBee series 3 Pro module is also available.

The XBee series 3 Pro is like the default module except that is has a longer range, which is unnecessary for our application of the module. Hence, the “Pro” module was not chosen to be used. The module can be configured into multiple topologies, point-to-point, star, and mesh. The mesh topology is a mixture of both point-to-point and star. The AMI network is a meshed network with elements of both star and point-to-point, thus the XBee module fulfills this requirement. In a network there are three roles that a device can be assigned, the coordinator, router, and end point nodes. A network must have a coordinator node, it cannot have more than one coordinator node. The coordinator node can send and receive data from other nodes, while also maintaining the established network. The coordinator node is what defines and establishes a given network. If it does not exist or goes offline in a network, the network will cease to exist along with it. Router nodes can send and receive data, and they can also route data through themselves, a network can have multiple routers. An endpoint can also send and receive data; however, it cannot route any data through itself, a network can have multiple end nodes.

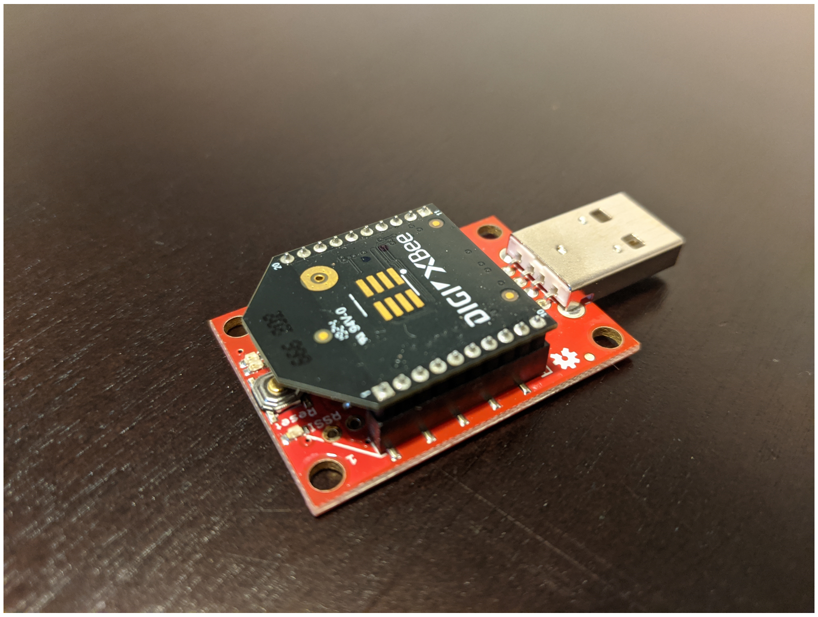


Figure 6. XBee 3 Communication Module with Sparkfun XBee Explorer USB adapter

3.2 Raspberry Pi and XBee configurations

The testbed that is to be configured will use three Raspberry Pi’s with three XBee communication modules connected using a Sparkfun XBee Explorer USB adapter for each XBee module. A final XBee module with an Explorer USB adapter will be interfaced with a PC running a Linux Operating System. Each Raspberry Pi and XBee module can represent a smart meter device in an AMI network in the NAN. Each Raspberry Pi will be configured to be an End Node, just as a smart meter or adversary would behave in the NAN. The PC with the XBee module will behave as the coordinator node of the network and will represent the operation and head-end of an AMI network. The programming that is used to configure and create functions is Python. Python is an open-source programming language that is a regarded as a strong general-purpose programming language, with a vast standard library along with other packages available for use.

Table 2. Testbed Hardware List & Pricing

	Price Per Unit	**Number of Units**	**Total Price**
Raspberry Pi 4 B – 1GB RAM	$30	3	$90
Power Supply	$7.95	3	$23.85
SD card 16GB	$5.99	3	$17.97
XBee 3 Module – PCB Antenna	$ 17.95	4	$71.8
Sparkfun XBee Explorer USB	$25.95	4	$103.8

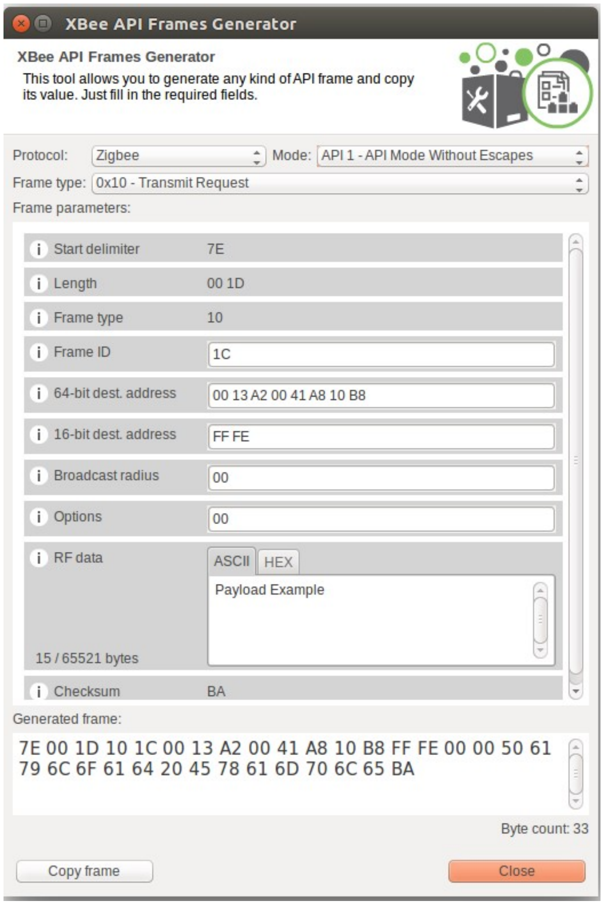
PC	n/a	1	$0
Total Price			$ 307.42

3.2.1 XBee Configuration

The configuration of the XBee module can be done through the XTCU application that Digi provides [33]. The XTCU module can be used to establish the different nodes for individual XBee module. The configuration of all the XBee modules is set up on the PC, as the XTCU application requires some processing power while the PC is also the most comfortable and familiar to use computer. The Network is configured for each module to be the same network, using a Personal Area Network (PAN) ID, to define and establish the network. It is important to note that the PAN ID of each module must be the same; otherwise, the modules will be operating in different channels. The Baud Rate range of the XBee modules goes up to 921600, it can operate between any Baud Rate from 1200 to 921600 by configuration. Each module is configured to have a Baud rate of 9600, while the XBee affiliated with the PC has a Baud rate of 115200. This can be reconfigured for the different test cases to be conducted on the testbed. When reconfiguring the Baud Rate of an XBee communication module, the serial port of the device connected needs to be configured to comply with the reconfigured Baud Rate, otherwise communication will not be possible. Once the PAN ID and each module has its role set, the modules are now communicating, and the network is established. There are some issues to note when working with these devices, and when working with hardware. The devices often receive update and firmware updates, in some cases the updates can cause mis-operation of existing configurations and applications. The DIGI website forums provide assistance in resolving these issues [34]. Another method to avoid this problem is to deny or block firmware and software updates.

3.2.2 Raspberry Pi Configuration

The system network is established by the XBee modules, the Raspberry Pi's will need to be configured to utilize the communication modules to send and receive packets as a smart meter does. A Raspberry Pi can be configured with Raspbian, a Linux based operating system that is user friendly provided on the Raspberry Pi website [35]. The SD cards are to have the operating system downloaded onto them through a different computer, and finally installed on each computer. The computers must be configured to allow access to their UART serial port such that the XBee modules can be interfaced. Using Python and packages available for serial communication, the "serial" package allows for data to be converted into a serial format to be transmitted by the XBee. The script editor used for programming in Python was vim, an editor provided with the installation of the Raspbian Operating System. Python is used to program and configure the different packets and frames sent by each module, manipulating the address fields etc. To Generate frames that comply with the network protocol, the XTCU program has the function to create the API frame desired. The type of frame desired to be sent can be specified, along with the protocol one wishes to communicate with. See Figure 7.



XBee API Frames Generator

This tool allows you to generate any kind of API frame and copy its value. Just fill in the required fields.

Protocol: Zigbee

Mode: API 1 - API Mode Without Escapes

Frame type: 0x10 - Transmit Request

Frame parameters:

```
Start delimiter        7E
Length                 00 1D
Frame type             10
Frame ID               1C
64-bit dest. address   00 13 A2 00 41 A8 10 B8
16-bit dest. address   FF FE
Broadcast radius       00
Options                00
RF data                Payload Example
15 / 65521 bytes
Checksum               BA
```

Generated frame:

```
7E 00 1D 10 1C 00 13 A2 00 41 A8 10 B8 FF FE 00 00 50 61
79 6C 6F 61 64 20 45 78 61 6D 70 6C 65 BA
```

Byte count: 33

Figure 7. XTCU Frame Generator Example

The goal is to set up the testbed of an AMI network, from the smart meters to the Head-end, while accurately complying with the topology of the network. APs and the distribution operation center will need to be included within the emulation. Each Raspberry Pi can be configured to operate as a smart meter, AP, and data concentrator. Multiple smart meters are assumed and emulated within each device, such that each device is seen as a cluster of smart meters communicating to an AP. Raspberry Pi communicates to the PC which acts as the data concentrator and head-end nodes. See Figure 8 and Figure 9. The Raspberry Pi's can be programmed to send and receive packets to each other in the network established among XBee module, configured beforehand. The implemented Dos attack and IDS will be implemented and applied similarly using Python in Chapter 4.

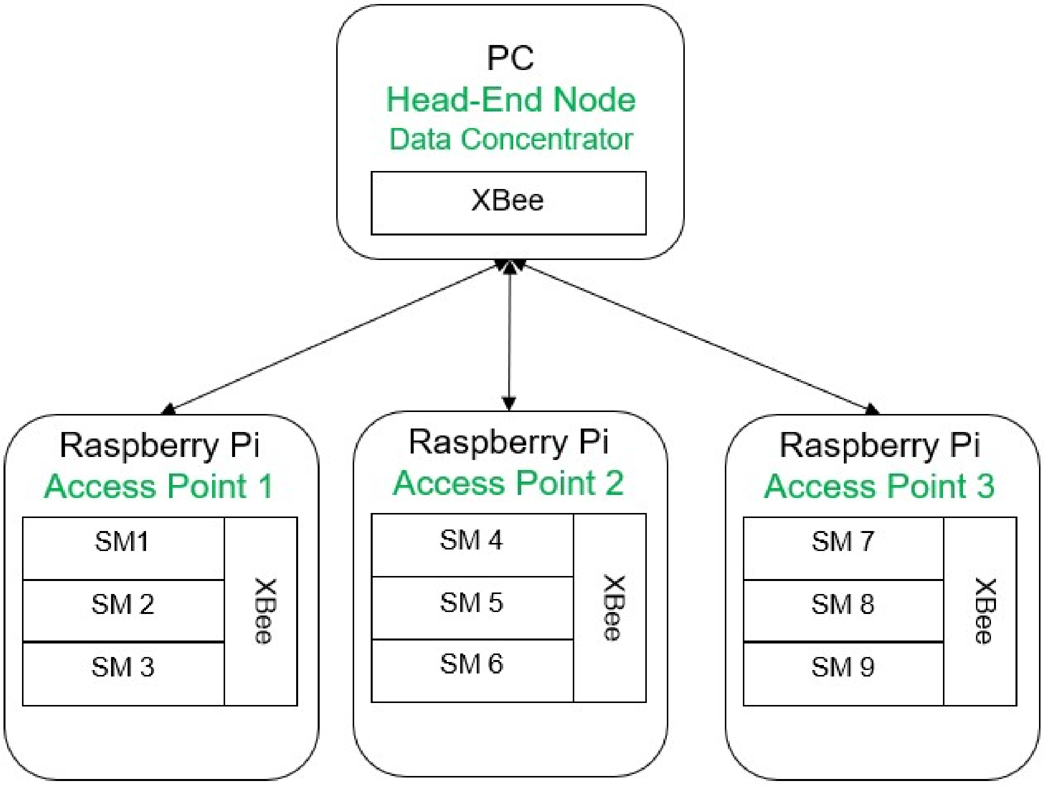
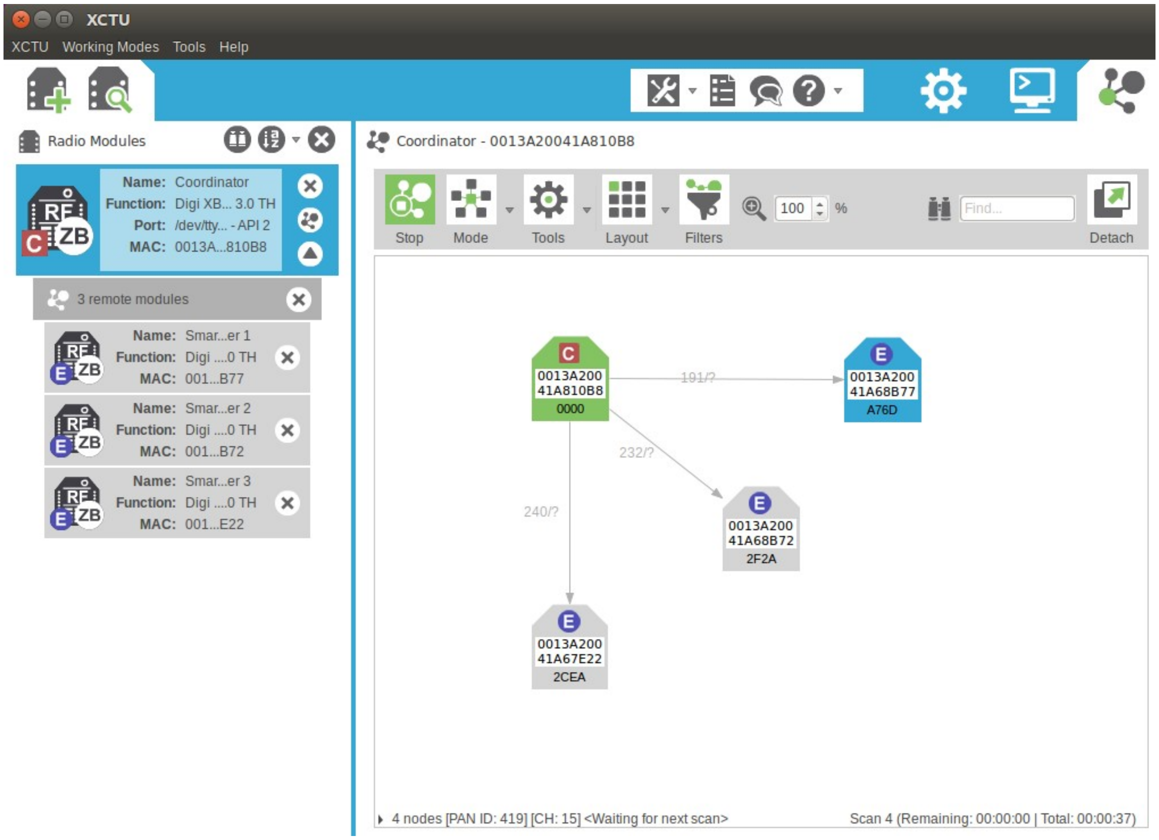


Figure 8. Testbed Hardware and Emulated Topology



Name: Coordinator
Function: Digi XB... 3.0 TH
Port: /dev/tty... - API 2
MAC: 0013A...810B8

3 remote modules

Name: Smar...er 1
Function: Digi ....0 TH
MAC: 001...B77

Name: Smar...er 2
Function: Digi ....0 TH
MAC: 001...B72

Name: Smar...er 3
Function: Digi ....0 TH
MAC: 001...E22

4 nodes [PAN ID: 419] [CH: 15] <Waiting for next scan>

Scan 4 (Remaining: 00:00:00 | Total: 00:00:37)

Figure 9. Emulated Testbed Topology

Chapter 4: Intrusion Detection System and Attack Model

4.1 Network Traffic and Normal Operation

Normal operation of the network of the testbed is of great importance for it to be a testbed. A benchmark must be known such that the introduction of an IDS does not affect the normal operation of the network by slowing down traffic or increasing overhead of the smart meters. The operation of smart meters in real applications has been measured and studied based upon location, type of application and traffic type [36], [37]. The studies analyzed the behaviors of the network and the traffic trends throughout a week. The patterns of smart meter usage can be studied such that they can be applied onto the testbed created as future work, this is outside the scope of this thesis.

A weakness of a testbed with devices like these is the scalability as mentioned in Chapters 1 and 2. It is unrealistic to simply speed up the traffic of the devices on the network. A great way to patch this weakness is through co-simulation. A co-simulated environment would have the scalability of network simulated with the realism and holistic merits that an emulated device has. The traffic can still be somewhat handled by the emulated devices such that the network resembles the AMI with several smart meters and their APs.

As discussed in Chapter 2, APs typically have a duty cycle of less than 5%. Data packet transmission is random in nature, stochastic, for simplicity within this testbed it will have a deterministic network traffic behavior. This should not be a problem since the main purpose of the testbed is security and not network capacity and traffic analysis. The case used to validate the testbed will have each device representing multiple smart meters under an AP. For a medium sized coverage area of an AP it will be assumed that there are about 900 smart meters. Each smart meter sending measurement data in 15-minute intervals, meaning that with a deterministic model of traffic the emulated device will send 1 packet every second. The focus is to see if the network is under attack, and to apply preventative or mitigative measures. Hence it is safe to use a deterministic traffic model.

4.2 DoS Attack

The AMI network has many elements of a WMN and other networks using Ad Hoc routing protocols have an exploitative vulnerability to DoS attacks. There are a number of ways this attack can be carried out [6], [14], [28], [30], [38]–[40]. A DoS attack is when a network is attacked in such a way that the communication within devices in the network is crippled, or "denied." A DoS can happen by different means, over exhaustion of computational ability of devices, exhaustion of the communications data capacity, which are examples of the aim of this attack. A DoS attack can be divided into three main types of attacks [41], a volume based attack, or a spoofed-packet flooding attack, the goal of this type of attack is to saturate the bandwidth of the network. A protocol attack is an attack that serves to exhaust server, computational, or communication equipment resources through packet flooding. Finally, an application layer attack is an attack that targets the application on devices within a network. The attack exploits vulnerabilities in the applications on the devices. There are three main points of attack to consider for a DoS attack on the AMI network. See Figure 10. The black arrows denote normal network traffic, red arrows denote a direct stream of malicious traffic, while the orange arrows denote a path indirectly effected by malicious traffic.

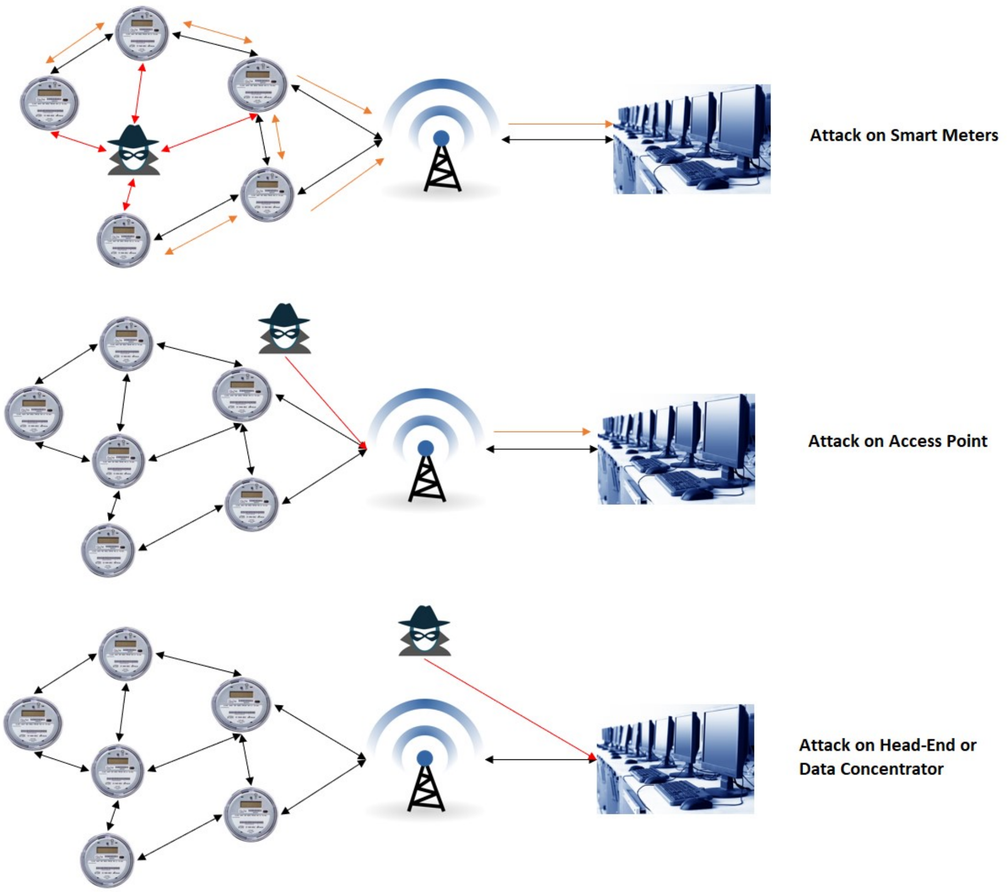


Figure 10. DoS Attack Paths on AMI

The attack on smart meters, a protocol attack, is done by having the adversary behave as a smart meter and take advantage of the Ad-Hoc routing protocol nature. The adversary sends out RREQ, HELLO (beacon), or RouteRequest packets. RREQ packets are used to request to join the network. HELLO packets determine the neighbor nodes within the network. The RouteRequest packet is sent to neighbor nodes and are propagated through the whole network to find the destination the packet specifies. The RouteRequest packet cannot be used unless the adversary has been accepted into the network. These packets are a key feature that makes the routing protocol easy to implement with new devices; however, it is vulnerable to cyber-attacks. The attacks cause the communication channels among smart meters to be occupied with useless traffic and blocking useful traffic; hence, DoS is achieved. This attack is the easiest to carry out, but it does not have as great of an impact as the other attacks, since the attack is targeting the lowest level of the hierarchy. A way to make this attack more impactful is to have a Distributed DoS (DDoS) attack, which is difficult as it required more resources and coordination but is very impactful.

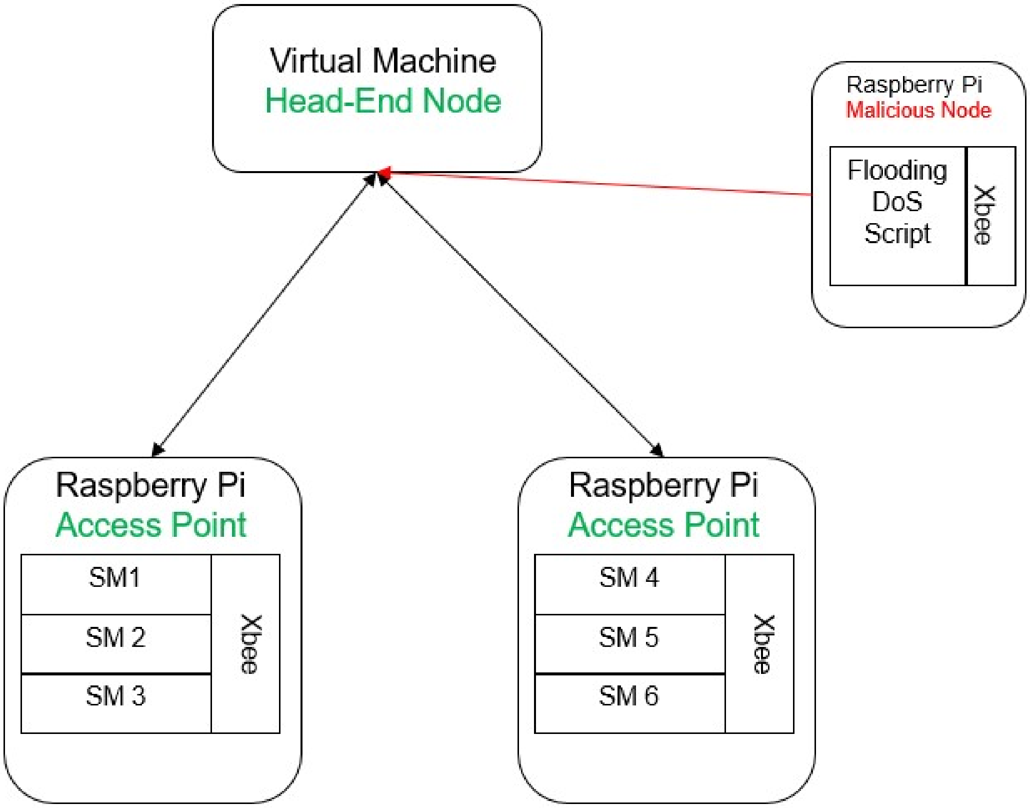


Figure 11. Model of Attack on Testbed

The other two attacks are more complicated to achieve, depending on the method they could either be a volume-based attack or a protocol attack, for the case of this situation it will be assumed to be a protocol attack. These attacks require skilled adversaries, but since the attack is at a higher level of the network and on paths that have all the network traffic, it is more impactful. To attack the AP the adversary will have to be trusted as a smart meter within the NAN and communicate directly with AP. This is done in the same way as it is in the previously described attack on the smart meter level. The attacker exhausts the bandwidth of the communication line to the AP such that the meter data is not routed to the Head-End, while also passing the flooding data through the AP and to the data concentrator and Head-End. This attack can be even more impactful if it is done in a distributed attack, DDoS. The attack on the Head-End or data concentrator directly is the most difficult but most impactful as the target is at the highest level of the network. Once that line is occupied/severed, the whole AMI network is interrupted and is undergoing DoS. This attack can be done by having the attacker spoof as an AP, or by other means that has them gain the trust of that communication line.

4.3 Intrusion Detection Systems

Cyber systems have implemented a variety of different intrusion detection methods. This variety can be categorized into several types and steps withing a detection system. An IDS can be broken down into three parts to complete the system, answering how, where, and what. How - will it determine if an intrusion is present in the system, the detection method or technique. Where - in the system will this IDS be placed, network or host based. What - will the system act or report, the intrusions will be detected (passive) or prevented (active).

4.3.1 Detection and Mitigation Techniques

An IDS has two ways to determine an intrusion method. It can have a database of attack patterns or traces; this is called a knowledge or signature-based detection technique. This technique relies on predefined rules that allow it to determine an intrusion from normal behavior. This technique is very effective and provide few false positives; however, it can only detect what it knows, it is blind to new attack patterns. Behavior or anomaly-based detection technique works by observing the network traffic and noticing changes from the normal traffic operation. Therefore, this method is strong to detect a wider variety of attacks that serve a purpose of effecting the network traffic. However, it is often difficult to determine what is normal for something that is stochastic and bursty in nature. Traffic or transmission when described as bursty, means that the distribution of traffic is concentrated within regions rather than being evenly or Poisson-like in distribution. Two common detection strategies IDS adopt are blacklisting or whitelisting. The use of each strategy varies depending on the application. A blacklist is the act of blocking somebody from one's contacts, a list is created to block a given signature. A whitelist is the opposite of a blacklist, similar to an invitation list. A list is created with the signatures of the packets that can be accepted by the network or device. The two mentioned strategies have a common problem. That is, the created lists need to be updated frequently.

Where an IDS determines the type of data that the IDS is utilizing or monitoring. A network-based IDS monitors traffic flow in different communication lines of a network, using data packet details such as the source and destination addresses. Since these details of packets are within the traffic flow in a network, a network-based IDS uses the protocol knowledge to assess the packet structures. A host-based IDS resides in multiple communication devices in a network, using device data as well as network data that specifically pertain to the specific device it is on. Host-based IDSs focus on the device or host that they are implemented on. IDS mitigation techniques are developed and are limited to where the IDS is based.

What an IDS does after detection depends on the intended application, feasibility of the application, as well as the synergy of the IDS with other systems in the network. An IDS with passive detection reports whenever an intrusion is detection and triggers an alarm. An operator has the responsibility to act upon the alarm from the IDS and conduct the mitigation strategy. However, an IDS with active detection is tasked to detect the intrusion and mitigate it altogether in the same package. If a malicious node is detected, the IDS would disconnect it automatically.

4.3.2 An IDS for the Testbed

An IDS needs to be developed and implemented on the testbed to validate the viability of using the testbed for similar cases. The normal traffic operation of the AMI has been discussed in Chapter 4.1. A simple logic based approach can be taken to develop an IDS that utilizes the traffic operation in AMI. It is known that the highest Baud rate of AMI devices is at 115200. Thus, a rate that exceeds that can be an indication of an intrusion. Smart meters have a transmission burst interval of 100-130 ms, with a 15-minute measurement transmission interval between bursts. These characteristics of smart meters allow for the development of an IDS that uses data rates and interval timing of different smart meters using timestamps. The IDS will be working from the Head-End, the distribution operation center.

The IDS developed has 2 steps to verify that an intrusion is occurring. The interval at which a given device is sending data cannot be longer than 200 ms, giving some tolerances the IDS threshold will be set to trigger at a data transmission window of longer than 200 ms within the given 15-minute measurement data transmission interval. When considering malicious activity for a flooding DoS attack, the data transmission interval is as long as the attack is occurring. Flooding attacks send a continuous stream of garbage data. Hence, the data transmission interval will be easily exceeded, triggering one of two steps of the IDS. The rate of data transmission is another defining feature between AMI devices and an adversary device. AMI devices do not exceed Baud rates of greater than 115200, while an adversary who is flooding the network to cause a DoS will possess devices with much greater Baud Rates. Hence, the data transmission rate from an adversary will be much higher than the AMI devices' data transmission rates. The transmission rate threshold will be limited to the Baud rate of 115200.

Chapter 5: Results

5.1 Testbed Operation

The testbed is setup and configured as mentioned in the chapters above. The test case being emulated is to validate the establishment of a continuous communication path from smart meters to head-end. This test case considers 3 APs communicating to a single head-end node. See Figure 8 . The setup of the physical testbed can be seen in Figure 12. Each AP is in range and is routing measurement data packets from 900 smart meter units. The data traffic is assumed an ideal deterministic model. Each data packet corresponds to data from a different smart meter being routed through an AP. The PC with the XBee 3 module receives the data packets and logs them in real time. The plot in Figure 13 as well as the rest of the plots in this section are generated in MATLAB using the data logged from PC emulating a coordinator control center node. A packet transmission loop script is run on each of the Raspberry Pi's with a 1 second pause between each packet transmission period.

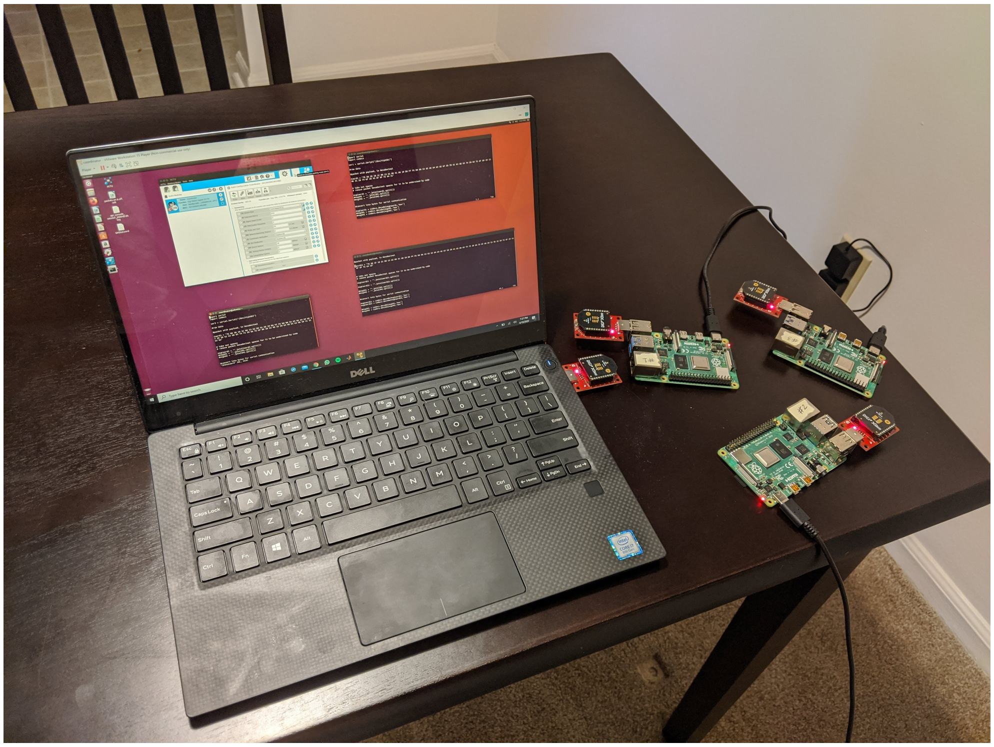


Figure 12. Setup of the Testbed and Devices

Each Raspberry Pi transmits packets that include the source address, and other packet identifiers that include the type of packet that is being transmitted as well as the payload. The logged data contain all this information in Hexadecimal format. This needs to be converted within the system to be better understood. The plot is separated by the AP source addresses; hence the arriving packets can be distinguished from packets received from other sources. The interval of traffic that has been plotted is approximately a 25 second window of data transmission and reception. Provided the traffic profile shown in Figure 13, the function of the testbed to have established a communication path with the emulated devices and log the packet details and structure for analysis is achieved and successful. This ability and functionality provide future work with opportunity and flexibility for advanced and holistic applications.

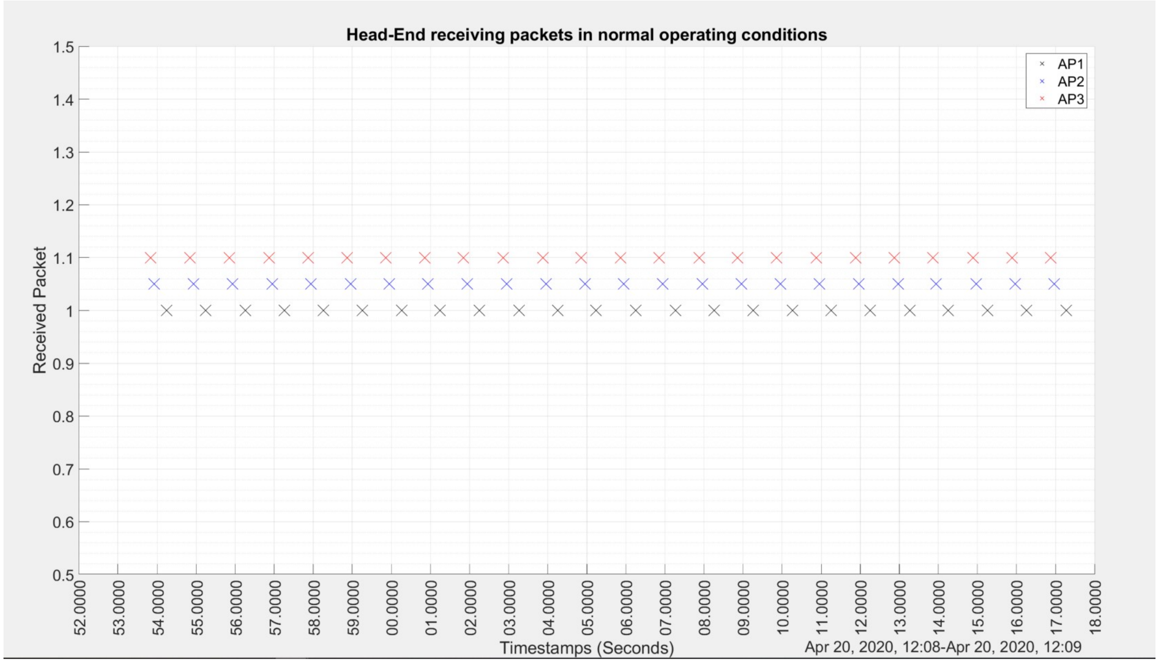


Figure 13. Deterministic Traffic Model on Emulated AMI System

5.2 DoS Attack on Testbed

A DoS attack is conducted on the emulated testbed. The operation of the testbed under normal operation conditions has been validated in the previous subsection. The testbed needs to be validated for the vulnerabilities of real AMI networks. The testbed will undergo a flooding DoS attack and the data packets received by the head-end are to be analyzed. Figure 14 is a plot of the packets received and logged by the head-end node. The DoS attack is conducted on the network connection between the APs and the Distribution Operation Center as illustrated in Figure 11. Two APs send at the normal traffic rate as in Chapter 5.1, a rate of 1 packet per second is sent by each AP to the head-end. An adversary node is then initiated on one of the Raspberry Pi's, it runs a script targeting the head-end that continuously flooded packets through that communication line.

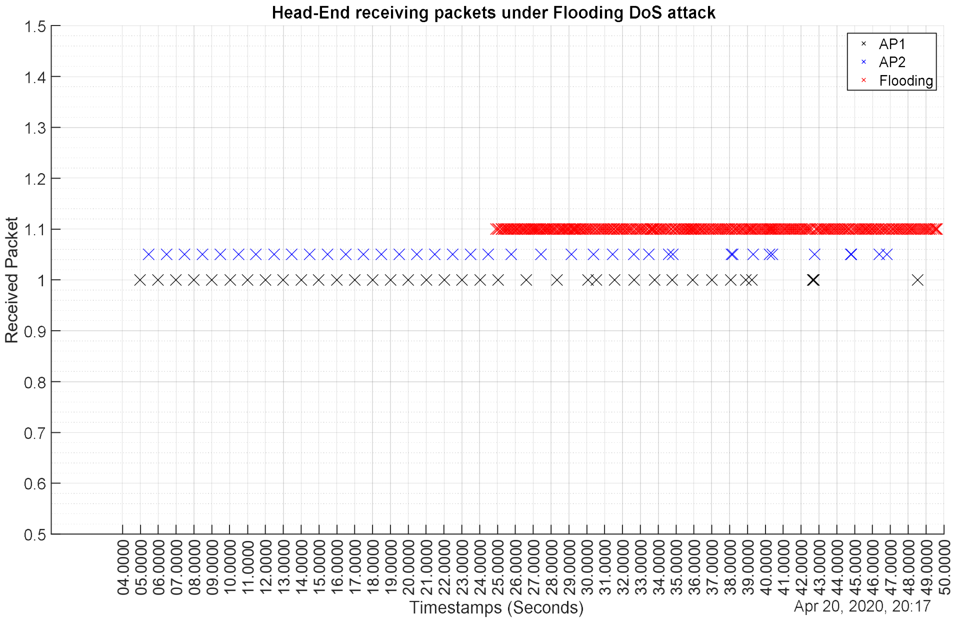


Figure 14. Packets Received by Head-end Under a Flooding DoS Attack

The DoS attack induced on the emulated environment is a success. The testbed devices are emulated while having both adversary and innocent nodes. The innocent nodes' (APs) data packets transmitted are always being sent at a clear interval of 1 packet per second as mentioned in the chapters above. Once the flooding DoS attack is initiated, a clear delay in packet arrival, and eventual packet drop occurs and can be seen in Figure 14. The packet transmission delay can be seen in Figure 15, the delay increases when the flooding attack starts around the 25th second mark and continues to increase. This testbed is able to emulate and induce flooding attacks, and the devices operating on the network are affected as expected from a DoS attack. The communication modules as well as the network are physically overwhelmed by the flooding packets sent by the adversary node. A successful emulation, capturing the realistic behaviors of real AMI and smart meter devices. This test provides evidence that the emulated environment has the same vulnerabilities as the real devices, and the vulnerabilities can be replicated for a variety of tests and applications.

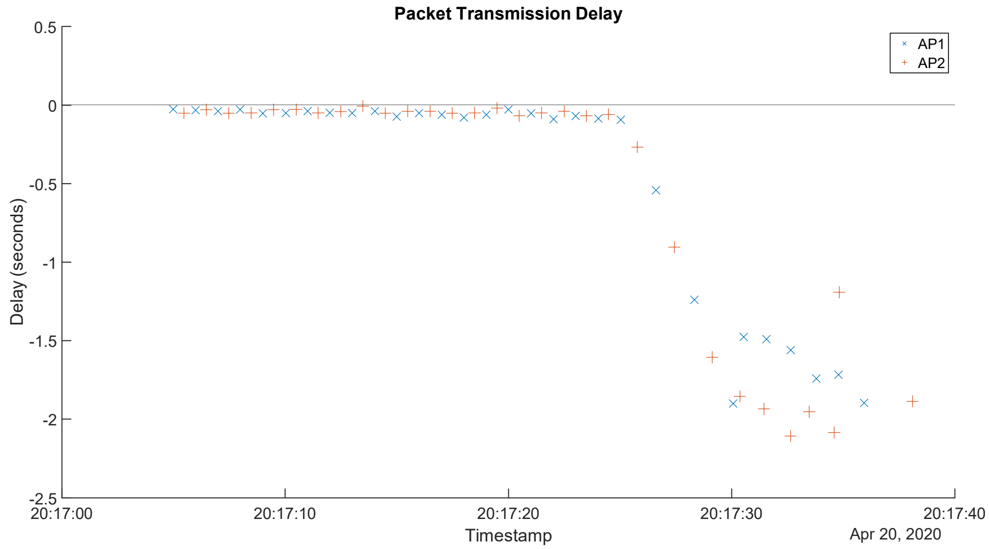


Figure 15. Packet Transmission Delay Under Flooding DoS attack

5.3 IDS on Testbed

An IDS is developed for the developed testbed. This IDS is a proof of concept to show that a sufficient amount of information available in the packets and is transmitted and received by the emulated devices in the testbed. Thus, a simple IDS is developed to calculate the average rate of arrival over a given interval, or window. The interval used for packet arrival rate is determined by a threshold that is set to be greater than the maximum interval of burst packet transmission. The window size is set at 500 ms, which is to not include individual bursts of high packet transmission rates by smart meters. The number of packets arrived is tracked in each 500 ms window. If the arrival rate from a single source exceeds 15 packets per second within a single windowed interval or 10 packets per second within a 1 second window, an intrusion alarm is triggered. The packets have source identifiers on them, and each source address is known within the sent packets. The operator of the testbed receives an alarm that sends a trigger indicating an intrusion has occurred and the corresponding source of the intrusion.

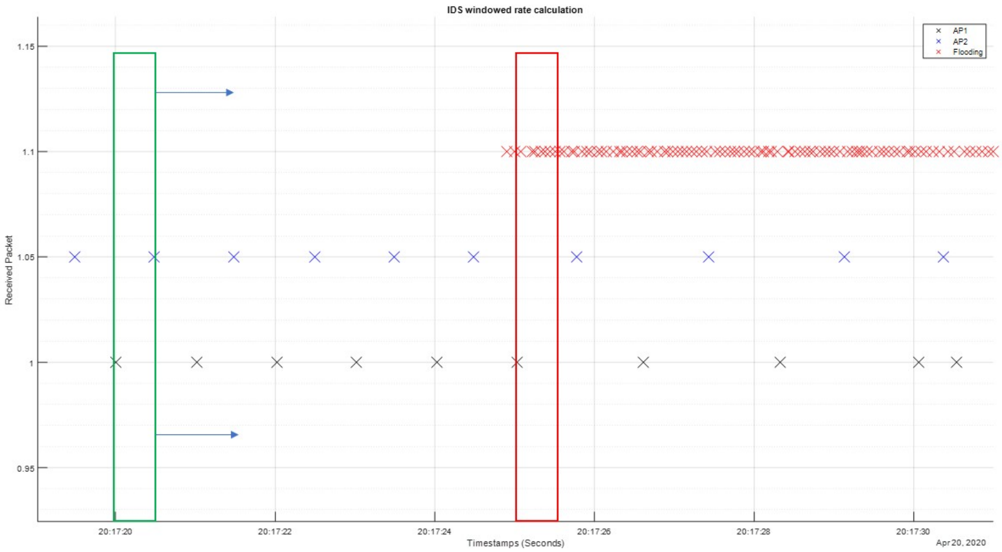


Figure 16. IDS Sliding Window during Flooding DoS Attack

Chapter 6: Conclusions and Future Work

6.1 Conclusions

Modern power systems are heavily connected with and dependent on ICT. The cyber security of the cyber physical power systems must be assured, and the ICT must meet the reliability and stability standards that power systems are held by. The increase of smart meter data integration and reliance in the power system also bring new vulnerabilities. An introduction to the AMI system, and smart meter utilization and vulnerabilities are discussed. Customer side installation of smart meters leads to sources of physical and cyber vulnerabilities to be exploited unlike other cyber system components.

A hardware survey and smart meter study have been completed to develop a flexible and sufficiently realistic physical emulated testbed for vulnerability assessment and IDS implementation. A set of widely supported and available hardware components is chosen and configured for an AMI and smart meter testbed that resembles the physical constraints of smart meter devices. The operation of the testbed under normal conditions has been observed and analyzed. The traffic and behaviors are satisfactory. A DoS flooding attack was carried out by an emulated device on the testbed. The devices on the testbed reacted in a realistic manner. A DoS was included on the network, and the packets transmitted became delayed and eventually dropped. An IDS has been developed and utilized using the logged data packets from the testbed to validate the developed platform. Network traffic operation shows the success of the environment created; the IDS successfully detected the malicious node carrying out a flooding DoS attack.

6.2 Future Work

In order to fully utilize the developed testbed and compensate for the shortcomings of a measurement-based testbed, a co-simulation environment needs to be developed. A Hardware-in-the-Loop testbed lacks scalability. To enhance the scalability, a network simulator working alongside will give the strengths of both testing environments. A real-time IDS can be developed to implement automatic mitigation techniques and halt an intrusion while employing physical device vulnerabilities as intrusion detection criteria. The emulated devices can be further configured to include all device vulnerabilities and further used for host-based IDSs. The rapid development of ICT networking and hardware technologies make the idea of a totally GPS synchronized sensor network possible for the optimization of traffic such that it can be deterministic. Thus, testing such scenarios with time-synchronized Raspberry Pi's is beneficial to the research area. The Raspberry Pi's can also be configured into other distribution system IED devices for further in-depth research concerning other ICT systems that operate in distribution systems.

REFERENCES

[1] Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," *Ics.Sans.Org*, pp. 2–11, 2016, [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[2] "WoodMac: Smart Meter Installations to Surge Globally Over Next 5 Years | Greentech Media." https://www.greentechmedia.com/articles/read/advanced-metering-infrastructure-to-double-by-2024 (accessed Apr. 14, 2020).

[3] U.S. Department of Energy, "National SCADA Test Bed Enhancing Control Systems Security in the Energy Sector," 2009, [Online]. Available: http://www.inl.gov/scada/factsheets/d/nstb.pdf.

[4] M. Forcella, "Creating a Mesh Sensor Network Using Raspberry Pi and XBee Radio Modules," State University of New York, 2017.

[5] C. C. Sun, "Cyber-Physical System Security of a Smart Grid," Washington State University, 2019.

[6] K. I. Sgouras, A. N. Kyriakidis, and D. P. Labridis, "Short-Term Risk Assessment of Botnet Attacks on Advanced Metering Infrastructure," *IET Cyber-Physical Syst. Theory Appl.*, vol. 2, no. 3, pp. 143–151, 2017, doi: 10.1049/iet-cps.2017.0047.

[7] Y. Liu, S. Hu, and A. Y. Zomaya, "The Hierarchical Smart Home Cyberattack Detection Considering Power Overloading and Frequency Disturbance," *IEEE Trans. Ind. Informatics*, vol. 12, no. 5, pp. 1973–1983, 2016, doi: 10.1109/TII.2016.2591911.

[8] Q. Sun *et al.*, "A Comprehensive Review of Smart Energy Meters in Intelligent Energy Networks," *IEEE Internet Things J.*, vol. 3, no. 4, pp. 464–479, 2016, doi:

10.1109/JIOT.2015.2512325.

[9] S. Finster and I. Baumgart, “Privacy-Aware Smart Metering: A Survey,” *IEEE Commun. Surv. Tutorials*, vol. 17, no. 2, pp. 1088–1101, 2015, doi: 10.1109/COMST.2015.2425958.

[10] C. C. Sun, A. Hahn, and C. C. Liu, “Cyber Security of a Power Grid: State-of-the-Art,” *Int. J. Electr. Power Energy Syst.*, vol. 99, no. November 2017, pp. 45–56, 2018, doi: 10.1016/j.ijepes.2017.12.020.

[11] F. M. Cleveland, “Cyber Security Issues for Advanced Metering Infrastructure (AMI),” *IEEE Power Energy Soc. 2008 Gen. Meet. Convers. Deliv. Electr. Energy 21st Century, PES*, 2008, doi: 10.1109/PES.2008.4596535.

[12] R. Vijayanand, D. Devaraj, and B. Kannapiran, “Intrusion Detection System for Wireless Mesh Network using Multiple Support Vector Machine Classifiers With Genetic-Algorithm-Based Feature Selection,” *Comput. Secur.*, vol. 77, pp. 304–314, 2018, doi: 10.1016/j.cose.2018.04.010.

[13] C. Zhang and Z. Fang, “A New Distributed Intrusion Detection System Model Based on SVM in Wireless Mesh Networks,” *J. Inf. Comput. Sci.*, vol. 12, no. 2, pp. 751–759, 2015, doi: 10.12733/jics20105231.

[14] S. Alanazi, K. Saleem, J. Al-Muhtadi, and A. Derhab, “Analysis of Denial of Service Impact on Data Routing in Mobile eHealth Wireless Mesh Network,” *Mob. Inf. Syst.*, vol. 2016, 2016, doi: 10.1155/2016/4853924.

[15] S. Khan, K. K. Loo, and Z. U. Din, “Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh Networks,” *Int. Arab J. Inf. Technol.*, vol. 7, no. 4, pp. 435–440, 2010.

[16] M. R. Hasan, Y. Zhao, Y. Luo, G. Wang, and R. M. Winter, "An Effective AODV-based Flooding Detection and Prevention for Smart Meter Network," *Procedia Comput. Sci.*, vol. 129, pp. 454–460, 2018, doi: 10.1016/j.procs.2018.03.024.

[17] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," *ACM Trans. Sens. Networks*, vol. 2, no. 4, pp. 500–528, 2006, doi: 10.1145/1218556.1218559.

[18] N. Beigi-Mohammadi, J. Misic, H. Khazaei, and V. B. Misic, "An Intrusion Detection System for Smart Grid Neighborhood Area Network," *2014 IEEE Int. Conf. Commun. ICC 2014*, pp. 4125–4130, 2014, doi: 10.1109/ICC.2014.6883967.

[19] Y. Park, D. M. Nicol, H. Zhu, and C. W. Lee, "Prevention of Malware Propagation in AMI," *2013 IEEE Int. Conf. Smart Grid Commun. SmartGridComm 2013*, pp. 474–479, 2013, doi: 10.1109/SmartGridComm.2013.6688003.

[20] Y. Guo, C. W. Ten, S. Hu, and W. W. Weaver, "Preventive Maintenance for Advanced Metering Infrastructure Against Malware Propagation," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1314–1328, 2016, doi: 10.1109/TSG.2015.2453342.

[21] Y. Guo, C. W. Ten, S. Hu, and W. W. Weaver, "Modeling Distributed Denial of Service Attack in Advanced Metering Infrastructure," *2015 IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. ISGT 2015*, pp. 1–5, 2015, doi: 10.1109/ISGT.2015.7131828.

[22] S. M. K. Quadri, "Information Availability: An Insight into the Most Important Attribute of Information Security," *J. Inf. Secur.*, vol. 7, pp. 185–194, 2016, doi: 10.4236/jis.2016.73014.

[23] T. Khalifa, K. Naik, and A. Nayak, “A Survey of Communication Protocols for Automatic Meter Reading Applications,” *IEEE Commun. Surv. Tutorials*, vol. 13, no. 2, pp. 168–182, 2011, doi: 10.1109/SURV.2011.041110.00058.

[24] Y. Jiang, C. C. Liu, M. Diedesch, E. Lee, and A. K. Srivastava, “Outage Management of Distribution Systems Incorporating Information from Smart Meters,” *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 4144–4154, 2016, doi: 10.1109/TPWRS.2015.2503341.

[25] “CENTRON® Meter Technical Reference Guide,” 2006. Accessed: Apr. 14, 2020. [Online]. Available: www.itron.com.

[26] R. A. Tell, R. Kavet, and G. Mezei, “Characterization of RadioFrequency Field eEmissions from Smart Meters,” *J. Expo. Sci. Environ. Epidemiol.*, vol. 23, pp. 549–553, 2013, doi: 10.1038/jes.2012.102.

[27] “802.15.4-2015 - IEEE Standard for Low-Rate Wireless Networks.” https://standards.ieee.org/standard/802_15_4-2015.html (accessed Apr. 14, 2020).

[28] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, “Cyber Security and Privacy Issues in Smart Grids,” *IEEE Commun. Surv. Tutorials*, vol. 14, no. 4, pp. 981–997, 2012, doi: 10.1109/SURV.2011.122111.00145.

[29] S. McLaughlin, D. Podkuiko, and P. McDaniel, “Energy Theft in the Advanced Metering Infrastructure,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2010, vol. 6027 LNCS, pp. 176–187, doi: 10.1007/978-3-642-14379-3_15.

[30] S. E. Anto, S. Seetha, and R. K. Kuriakose, “A Survey on DoS Attacks and

Detection Schemes in Wireless Mesh Networks," *Procedia Eng.*, vol. 38, pp. 2329–2336, 2012, doi: 10.1016/j.proeng.2012.06.278.

[31] M. Gandra, R. Seabra, and F. P. Lima, "A Low-Cost, Versatile Data Logging System for Ecological Applications," *Limnol. Oceanogr. Methods*, vol. 13, no. 3, pp. 115–126, 2015, doi: 10.1002/lom3.10012.

[32] "GPRS Smartmeter Centron Specifications." https://www.itron.com/-/media/feature/products/documents/spec-sheet/centron-gprs-smartmeter.pdf (accessed Apr. 15, 2020).

[33] "Digi XBee® 3 RF Module Hardware Reference Manual," 2020. Accessed: Apr. 15, 2020. [Online]. Available: www.digi.com/howtobuy/terms.

[34] "Digi Forum." https://www.digi.com/support/forum/ (accessed Apr. 15, 2020).

[35] "Raspberry Pi Downloads - Software for the Raspberry Pi." https://www.raspberrypi.org/downloads/ (accessed Apr. 15, 2020).

[36] N. Andreadou, E. Kotsakis, and M. Masera, "Smart Meter Traffic in a Real LV Distribution Network," *Energies*, vol. 11, no. 5, 2018, doi: 10.3390/en11051156.

[37] F. Melzi, A. Same, M. Zayani, and L. Oukhellou, "A Dedicated Mixture Model for Clustering Smart Meter Data: Identification and Analysis of Electricity Consumption Behaviors," *Energies*, vol. 10, no. 10, p. 1446, Sep. 2017, doi: 10.3390/en10101446.

[38] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and Evaluation of Security Threats on the Communication Networks in the Smart Grid," *Proc. - IEEE Mil. Commun. Conf. MILCOM*, pp. 1830–1835, 2010, doi: 10.1109/MILCOM.2010.5679551.

[39] S. Seth and A. Gankotiya, "Denial of Service Attacks and Detection Methods in

Wireless Mesh Networks," *ITC 2010 - 2010 Int. Conf. Recent Trends Information, Telecommun. Comput.*, pp. 238–240, 2010, doi: 10.1109/ITC.2010.51.

[40] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers," *IEEE Commun. Surv. Tutorials*, vol. 13, no. 2, pp. 245–257, 2011, doi: 10.1109/SURV.2011.041110.00022.

[41] A. D. Wood and J. A. Stankovic, "Denial of Service in Sensor Networks," *Computer (Long. Beach. Calif).*, vol. 35, no. 10, pp. 54–62, 2002, doi: 10.1109/MC.2002.1039518.