2022-12-01

Security Analysis And Implementation Of DNP3 Multilayer Protocol For Secure And Safe Communication In Scada Systems

Isaac Monroy
University of Texas at El Paso

SECURITY ANALYSIS AND IMPLEMENTATION OF DNP3 MULTILAYER PROTOCOL FOR SECURE AND SAFE COMMUNICATION IN SCADA SYSTEMS

ISAAC MONROY

Master's Program in Computer Engineering

APPROVED:

_____

Sai Mounika Errapotu, Ph.D., Chair

_____

Jaesung Lee, Ph.D.

_____

Virgilio Gonzalez, Ph.D.

_____

Palvi Aggarwal, Ph.D.

_____

Stephen L. Crites, Jr., Ph.D.
Dean of the Graduate School

DEDICATION

I dedicate this work to my brother, who's been my inspiration and role model, my parents and friends who have been there to help through my academic career.

SECURITY ANALYSIS AND IMPLEMENTATION OF DNP3 MULTILAYER PROTOCOL FOR SECURE AND SAFE COMMUNICATION IN SCADA SYSTEMS

By

ISAAC MONROY, B.S.E.E.

THESIS

Presented to the Faculty of the Graduate School of
The University of Texas at El Paso
in Partial Fulfillment
of the Requirements
for the Degree of

MASTER OF SCIENCE

Department of Electrical and Computer Engineering
THE UNIVERSITY OF TEXAS AT EL PASO
December 2022

ACKNOWLEDGEMENTS

I would like to acknowledge Dr. Sai Mounika Errapotu. She has been my teacher and my mentor for the last two years. When I began my journey within cybersecurity, an error with my degree plan occurred during my first year as a graduate student, where I was transitioned into the introductory class of cyber security. As a result, I immersed myself into another branch of computer engineering where I didn't think I would be so fond and interested in learning. As a result, I decided to make the decision and research a topic within cybersecurity under Dr. Errapotu's supervision. While experiencing bumps in the road, she gave me advice toward the direction that my research was taking, and I am grateful for all of that she has taught me both inside and outside of the classroom.

At last, I would also like to acknowledge the department of Electrical and Computer Engineering for always being able to help me and support me.

ABSTRACT

When SCADA systems were first introduced into society, a lot of manpower was required for monitoring and controlling devices within critical infrastructures. With the increasing demand for services and growing systems, a need arose to automate the monitoring and controlling tasks. This led to introduction of networks into SCADA systems to enhance monitoring and control capabilities, that can scale with system size and requirements. But this introduction of network layer along with its advantages, also introduced a new threat surface which exposed multiple vulnerabilities within the system that can exploited to launch attacks, that led to the integration of security features in existing protocols or creation of new security-based protocols. When communication protocols such as IEC 60870, IEC 61850, Modbus, and DNP3 were initially designed for SCADA systems, these were developed without security features since their objective was to be an open standard that provided interoperability among all the devices that are available in the market. Eventually, when cyber-attacks began to emerge within SCADA systems, this pushed developers to release newer and secure versions of their protocols. The purpose of this thesis is to specifically analyze the security challenges and constraints within critical infrastructures in terms of implementation, and why Distributed Network Protocol Version 3 (DNP3) communication protocol for SCADA systems, and how its security features could be improved. The advantages of DNP3 over other SCADA protocols include its reliability, efficiency, and real-time transference of data, along with capabilities to support implementation of several standard data formats and data synchronization. It advanced through multiple versions since its launch, and currently in its sixth version provides devices with advanced capabilities to collect and acquire information during operation. Despite its advantages, security and cryptographic features were not integrated till fifth and sixth versions. With recent security additions, the protocol provides integrity, encryption options to protect the messages being transmitted and received within a communication link, and secure authentication to verify the authenticity of control messages sent to destination devices. Vulnerability and attack resistance analysis in DNP3 is in developmental stages. In this work, we conducted an extensive security analysis on the modes of operation of DNP3, its topologies, along with additional features that could be incorporated into its security to make SCADA communications more secure.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

When industries first began to build power grids, a method to monitor and control the components of the system was implemented by the Supervisory Control and Data Acquisition (SCADA), which consists of a group effort from the outstations, master stations, and the human machine interface, controlled by operator. This system gave the companies an ability to interact with sensors and actuators to both collect data and control the devices of the grids. However, as power grids continued to expand and scale, requiring a greater number of components from which to gather information, a need to manage power grids more effectively arose, leading to the implementation of the Smart Grid, that allows devices of the grid to be connected to the network. Through specialized communication protocols, SCADA systems now are capable of faster collection of data as well as facilitate interaction between devices of the power grid.

Even though the implementation of this new technology brought forward many advancements to the power grids, it has also exposed them to the dangers of the networks, and this becomes highly important as compromised devices being can critically affect or, ultimately, compromise the SCADA system. There are two categories of attacks in SCADA systems; first are the passive attacks which are just listening on the network without making any changes or attacking systems, and the second are active attacks which are the type of attacks that hinder the communication and damage the systems. Recent attacks in SCADA communication include the Denial of Service (DoS), eavesdropping, Man-In-The-Middle, and system break-in, which should be avoided. As a result, security implementation in communication protocols is becoming a priority to ensure power grids have protection and can keep offering the services to customers.

Even though SCADA security is in developing stage and systems are vulnerable to attacks, there are some defense mechanisms developed against some cyber-attacks, depending on the communication protocol utilized for the system. In this thesis, SCADA system security when implemented with the Distributed Network Protocol version 3 (DNP3) communication protocol will be analyzed for each of its protocol stack layers and its interactions, respectively. Moreover, the possibilities of having attacks on a system will never be zero so, the implementation of this protocol shall deeply study the security interactions to build SCADA systems that self-heal from active attacks and have resiliency to continue operation even in case of attacks.

Currently, DNP3 is the leading communication protocol being utilized in North America for implementation. However, since the release of the DNP3 protocol, which came with a weak

protection against attacks, many versions of the protocol have been released. In addition, not all of the devices being sold in the market are provided by the same vendor. So, security implementation and testing of the DNP3 protocol that offers interoperability in power grids to add devices from different manufacturers while still maintaining the intended performance, will provide insight on how communication interactions should be made resilient without compromising the flexibility of the protocol to enhance grid security.

1.2 Trends in SCADA Communication

The automation of SCADA systems brought new trends in communication technology of the grids, below we will discuss the communication protocol updates in SCADA systems over time:

- Before SCADA systems' automation, manpower was utilized to perform these tasks.
- Proprietary communication protocols were used, which were designed for short distance point to point communications
- **Automation and Networking:** With a growing demand in services, automation and networking was starting to be introduced in SCADA systems in mid-90s.
- **Complex Architectures:** This shift has evolved into complex mazes of interconnected systems, intelligent electronic devices, and other equipment, running and talking on proprietary communication media and protocols.
- **Introduction of SCADA specific Communication Protocols:** Eventually with a growing system so large, short distance communication wasn't the most efficient, and a new set of SCADA Communication Protocols such as Inter-Control Center Communications Protocol (ICCP), Modbus and Distributed Network Protocol (DNP) were introduced.
- **Interoperability:** One key challenge in facilitating seamless SCADA communication was divergence in protocols and methods different device manufacturers and vendors used in Industrial Control Systems (ICS) and Energy Markets. This led to update of communication protocols to interoperable protocols, such as DNP3 and Modbus over IP, where device manufacturers, vendors and users can agree on a common language and medium through use of ethernet (TCP/IP).

1.3 Trends in SCADA Communication Security

Along with trends in communication, there have been changes over the communication protocol security in SCADA systems. Below we will discuss the trends in SCADA communication protocols' security:

- Proprietary communication protocols are inherently insecure since they were designed point to point communications with single wiring.
- SCADA communication protocols were designed only for seamless communication but haven't considered any security measures.
- It is evident that "Almost all traditional communication protocols lacked security measures such as authentication, authorization, or encryption"
- Even though the traffic between all these devices was wide open, plain-text and easy for manipulation and attack, there were very few attackers that could make it onto those communication networks. It had to be someone inside the ICS facility with the equipment and the knowledge to be able to manipulate the system.
- But the integration of ethernet/internet in interoperable SCADA communication protocols expanded threat surface to an extent unimaginable, creating vulnerabilities that attackers anywhere in the world could exploit by connecting remotely.

Security was not an eminent part of SCADA communication protocol design. "Security is an afterthought in all existing SCADA communication protocols, that started becoming priority after numerable cyber threats emerged."

1.4 Motivation & Purpose of this Work

SCADA communication, the protocols that facilitate interactions and their security plays a major role in overall SCADA system security. Despite communication being the strongest pillar that facilitates automation in SCADA systems, security and cryptographic mechanisms were not added to these protocols till 2010s. SCADA communication protocols were not initially designed with security and were primarily designed to offer seamless communication, but with increasing attacks

on SCADA systems security inevitably became a part of SCADA communication. “This shift has not aided for new design of communication protocols that had in-built security, but only focused on the integration of existing security mechanisms with communication protocols that are in use in SCADA systems.” This is because SCADA systems already had communication protocols that provided interoperability and adding security to those without disturbing the operation has become a wise choice, since updating the systems with needed computational hardware to facilitate such interactions in large scale systems is significantly expensive. As a result of such choices, security mechanisms are being tested in plug and play mode to check which works well/ which doesn’t work well for SCADA communication. One such major communication protocol being tested and used in ICS and energy grids is Distributed Network Protocol 3 (DNP3) which is not only interoperable but also has some integrated security mechanisms. The integration of security in DNP3 protocol has brought protection features against some attacks in SCADA systems but also brings new communication surfaces and vulnerabilities at IT-OT (Information Technology - Operational Technology) space to light, which should be studied in-depth and addressed to have a safe and secure operational environment. Among all the existing SCADA communication protocols DNP3 is good choice for enhancing SCADA system security, because DNP3:

- Provides time-stamped messages that indicate changes
- Is an Open-source protocol between manufacturers, vendors and users
- Is built with architectural stack and doesn’t need protocol translators or add-ins for communicating over the internet
- Supports multiple topologies for implementation
- Supports different communication modes such as Polled and Quiescent

This work primarily focuses on in-depth analysis and key aspects of security implementation such as operational security modes, session set up and connections; in existing security versions of DNP3 protocol. Despite being released in 1993, cryptographic mechanisms were not added to DNP3 protocol till 2012, and the added security mechanisms are undergoing operational testing to see if they are suitable for resilient operation. This work will provide a formal security analysis and features of DNP3 protocol’s security, that will help in understanding operational elements and communication exchanges required for enhancing resilient and self-healing nature of SCADA

systems. Since Industrial Control Systems and Energy grids are important critical infrastructures, where system disruption due to cyber-attacks not only affects machines in the network but has potential to control and disrupt physical systems connected to compromised machines. Analysis of issues at communication interface and their impact on cyber physical systems security is very important not only to protect the system from intruders and ensure system stability & availability, but also to ensure safe operation of system in order to protect people working on such premises.

1.5 Document Organization

The organization of this thesis document will first begin with Chapter 2, which gives an introduction of what SCADA systems entail. First it shall describe the different devices utilized and implemented within SCADA systems, and how these devices exchange information when communicating. Next, the chapter shall discuss how the SCADA systems transitioned to the internet and, moreover, mention the benefits and risks for transitioning, and the explanation of the most common SCADA protocols being utilized.

Next, Chapter 3 discusses the different types of security objectives found within the SCADA systems to ensure the success of the system. Next, the chapter discusses the categories of attacks and the different types of attacks targeting the SCADA systems, and the explanation on how each attack have a specific target within the system.

Chapter 4 talks about the DNP3 communication protocol. The chapter begins by illustrating what is the architecture of the protocol and how a message is created by a device to later be transmitted to its intended destination. Next, it is discussed what are the benefits and advantages of utilizing this communication protocol for a SCADA system.

Chapter 5 discusses the problems found within legacy systems, and their lack of hardware for computationally intensive security algorithms. In addition, how having very complex systems being implemented can have advantages and risks from the implementation. Now, the chapter also discusses the scalability issues found within the system. Finally, it is mentioned how all these issues can be resolved by having a different approach towards the solution.

Chapter 6 talks about how the DNP3 Secure Authentication Version 5 (DNP3 SAv5) implements a mechanism utilized by the protocol to secure the messages being transmitted between the devices and how a session is initially established among the devices.

Chapter 7 talks about the changes made to the 5th version, and now DNP3 SAv6 implements a new solution while still addressing all the security challenges from DNP3 SAv5. Now, within this chapter, we also discuss about the implementation details and explain how two devices interact and demonstrate a successful communication between them. At last, chapter 7 talks about the differences between 5th and the 6th versions of the protocols and why the new changes mentioned are made.

Chapter 8 concludes the thesis and talks about future additions to DNP3 protocol security.

CHAPTER 2: SCADA SYSTEMS

When industries were operating in the mid-20th century, men worked on controlling and monitoring the devices that were utilized by infrastructures. Eventually, due to the fact that these infrastructures needed to expand and scale to a wider area, a problem arose where relying solely on manpower to continue the control and monitoring tasks wasn't enough. Multiple attempts were implemented to create a solution to keep men on these stations yet, eventually managers realized that expanding infrastructures needed a new and optimal solution to keep working at the same pace therefore, an implementation to fully automate the tasks came about; and this is when Supervisory Control and Data Acquisition systems were introduced.

With passing years, heading to the 21st century, the introduction of microcontrollers and new technology began to make SCADA systems more relevant for the automation of critical infrastructures. Now, within the industries there are facilities and services which are classified as crucial for the security, safety, and economic well-being of companies and, most importantly, the people; as a result, they have been starting to get entitled as critical infrastructures. Some examples of these are telecommunications, the transmission of information between two endpoints by cable or other technologies, transportation, such as subways, tramways and buses, power infrastructures, distribution of power from chemical, water, wind, and solar power generators. All these critical infrastructures need to be monitored constantly in order to provide the best service for the people. Moreover, where repetitive tasks were found within the infrastructures, where not even getting the biggest number of men for the job was feasible, this is where the implementation and the growth of the system became critical, and automating it was the only option. As a result, SCADA systems began to be implemented among all the critical infrastructures to keep up with scaling and expansion of systems.

2.1 Devices in SCADA Systems

SCADA system is composed of an operator, human machine interface (HMI), master terminal units (MTU), remote terminal units (RTU), and the field devices. As a result, it can be depicted as a hierarchy on how the SCADA systems functions and how it collects the information, as shown in figure 1. Now, to commence on the explanation on the components of the SCADA system, first the operator and the human machine interface; the operator is the person assigned to

manually see how the whole operation within the SCADA system is. In addition, the operator sees how the collection of information is happening and if any changes need to be made within the system; and if the operator sees fit, any changes can be made with the help of the human machine interface. Now, the human machine interface, as the name implies, it is a computer that has access to all the information that is being collected from all the devices and depicts a representation to the operator, and this information gets updated in real-time. So, both of these parts of the SCADA architecture stand at the top of the hierarchy, since any decision being made, and the power to make those changes resides within this pair.

Moving on, another important part of the architecture are the master terminal units or master stations. These devices must have at least two connections; one for the human machine interface or to another master terminal unit, and to a remote terminal unit. The reason for the type of connection is because of the tasks that it has at hand, but the main task of the master station is to collect the information of the remote terminal units and report this information back to whoever it is reporting to, respectively. Now, as mentioned before, these devices can have multiple connections because, first, the master terminal unit can be connected to multiple remote terminal units, and they are all reporting back to it all the information that they are collecting. On the other hand, if the SCADA system has expanded greatly, then a hierarchy can be that this master station is now reporting to another master station above in the hierarchy. So, as the SCADA system grows, the hierarchy grows with it.

The next component of the architecture are the remote terminal units or outstations. For the remote terminal units, one of their main tasks will be to collect the readings and the information from the field devices themselves. And the field devices are the sensors or the actuators that are out in the field and they are measuring the information that they are being exposed to. Now, the remote terminal units will be the ones to collect this information and report it back to the master terminal unit which they are connected to. One thing to note is that these can be compared to the master terminal units only in the case that the remote terminal units are also designed to be connected to multiple field devices and collect their data simultaneously, because it would be cost-ineffective to have one remote terminal unit to a single field device, if that were the case, then the field devices would be connected instead directly to the master terminal unit. In addition, the ability of both the master terminal unit and the remote terminal unit to adapt for scalability is what brings the full potential of the SCADA systems when they are implemented to critical infrastructures and

that is why they are relied upon as the solution to collect and interact with the information from the field devices.

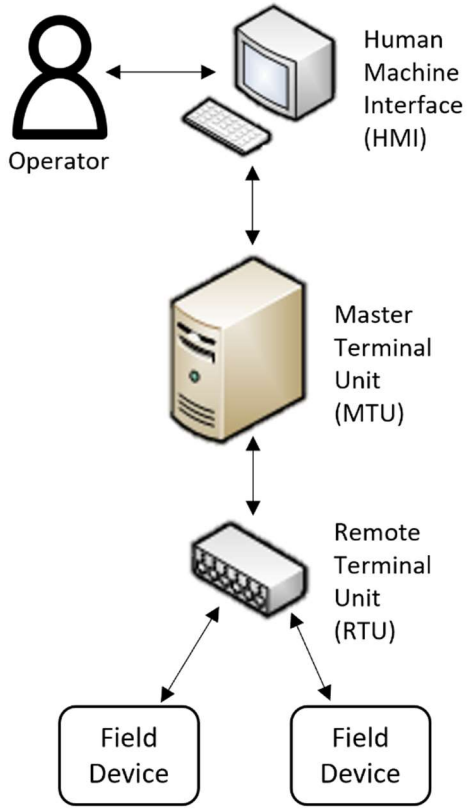

Figure 2.1 – Supervisory Control and Data Acquisition Architecture

In brief, with all the components of the SCADA architecture together, an example can be when a sensor from a field device is working as intended but, all the sudden, it begins reporting to the outstation the same measured value as it reported in the last 10 readings. This will immediately be reported back to its master station, respectively, and go up the hierarchy all the way to human machine interface to notify the operator that there is a sensor that isn't working properly and then is when action can be taken from part of the operator to make changes as seen fit. In addition, any other failures that happen within the network can be attended to and be dealt with to an extent, because maybe that one sensor just sent 10 same readings by error and then it continued working as intended, or the case can also be that multiple sensors also send the same readings, and this is where a major failure must be dealt with. Moreover, the damage can range from a single sensor or actuator to a whole outstation or major area of the SCADA system.

2.2 Transitioning to the Internet

With the continued expansion of SCADA systems being greater, to cover a wider area of systems and devices, a new problem arose for SCADA systems where now they needed to have communication in a wider rang. So, with the technology of the internet and implementing this medium for information to flow through the network and reach from one destination to another in a matter of seconds became a viable solution to upgrade the systems. However, now with the systems being connected to the network, it exposes them to the dangers of the cyber world and security issues within the systems. As mentioned before, there can be physical failures from sensors and actuators themselves, but there can also be now software failures within the SCADA systems normally or can also be through cyber-attacks, which can have a broader range of targets, including the master and remote terminal units. If it is a cyber-attack against the system, it can have serious consequences on the critical infrastructures and as a result, can affect the safety of the people and the services utilized by the public. For example, an attack on the systems can be where an adversary can completely shut down a power grid therefore, leaving the public with no electricity until the issue is resolved, and depending on how big the attack was, the system can be rebooted in a time span of 5 minutes to 5 weeks or even more. So, having the correct security implementation for these crucial systems is essential for well-being of everyone who uses its services and any individual who is affected by these services.

Now, with the transition of SCADA systems now being connected through internet, every system needs a communication protocol depending on the type of application that the system is part of, nevertheless, every communication protocol should come with security implementation for secure and safe transfer of the messages between each of the devices mentioned in the architecture i.e., from the field devices all the way back to the human machine interface, and vice versa. In this thesis, Distributed Network Protocol Version 3 (DNP3), and further details of its communication features will be discussed in the following chapters.

2.3 Different Compliant Protocols for SCADA Systems

Aside from the DNP3 protocol capable of being implemented in SCADA systems, other compliant protocols are IEC 60870, IEC 61850 and Modbus. The mentioned protocols are similar

to DNP3 based on the physical medium that they utilize to communicate, which is with ethernet. Now, ethernet is a connection-based method of communication among devices and the major benefit that it provides is that it ensures stable transmission among the devices and since only the required devices must be connected to the SCADA systems, having multiple ports isn't a problem in this case. So, the first protocol IEC 60870 is mainly utilized in within the power industry for automating the system by performing remote controlling and monitoring of each of the devices. Next, the protocol IEC 61850 is also utilized within the power industry and one of its features is that for its topology, it connects the human machine interface directly to the connected field devices that make up the system. Compared to the architecture shown in figure 1, since IEC 61850 doesn't utilize master terminal units or remote terminal units, then this is where the human machine interface must be implemented with bigger capabilities to keep up with all the reporting information that the field devices are picking up from the surroundings. Finally, the other compliant protocol is Modbus and one of its biggest features is the different types of communication that it offers, more specifically, meaning that Modbus doesn't require devices to connect on a proprietary network to communicate and send information; devices just need to connect to one of the multiple Modbus variants and they'll be connected to the network. Moreover, because of this feature is what allows Modbus to be easily deployable and eases the interconnection for the industrial devices.

CHAPTER 3: TYPES OF ATTACKS

As mentioned previously in chapter 2, since the SCADA transitioned to automating the system with internet connectivity has surrendered the system itself to potential cyber-attacks from adversaries. For this chapter, attacks that can cause harm to the SCADA systems will be listed between two subchapters, active attacks, and passive attacks, respectively.

Now, a cyber-attack is identified as an attack from adversary utilizing either a computer or a physical media (i.e., USB stick), and this attack can be towards a single computer, or it can range to group of computers. Moreover, cyber-attacks can have targets, and these can be the ones that cause the most harm since, for example, adversaries can deny the service to someone trying to access information; they can see information that wasn't directed to them; or, ultimately, compromise an entire system. Now, the last example would be the worst-case scenario for a kind of attack because, as mentioned before, SCADA systems are implemented in critical infrastructures, and these directly affect the public safety so, having resiliency in the system should be a minimum to prevent anything close from happening.

3.1 Security Objectives

As mentioned previously, since SCADA systems are implemented within critical infrastructures, then any changes being made directly impact the public safety so ensuring that the systems are meeting the required security objectives is important to both keep important information and access to the infrastructures out of hands reach from anyone who isn't authorized to use it.

3.1.1 Availability

The first security objective that SCADA systems should ensure is availability. Availability refers to the system itself, since the system should have the ability of communicating the transmitted messages and receiving the messages as well, from the operator to field devices and vice versa. Moreover, the operator is one of the main parts of the system for which availability shouldn't be an issue because having access to late readings from the system could delay making important decisions which could overall make an impact on the system.

3.1.2 Authorization

Moving forward, the second security objective is having authorization. This objective refers to who can access the system and who can't. Now, the main concept for this objective can be towards the operator, for which they should have their login information to access the human machine interface and interact with the system, but this also applies to all the other devices as well, such as the master terminal units and the remote terminal units. For example, when the operators are functioning within their role, they don't have to necessarily be monitoring each of the master stations or outstations within the system, each master station can take decisions based on what it's appropriate for its linked devices. So, authorization also applies to all of the devices that are communicating important information through the network.

3.1.3 Integrity

The third security objective is the integrity within the system. Ensuring that the communication between the devices remains intact and that no messages are being modified is of great importance because if messages were to be modified and implemented by the receiver, then unintended damage could be caused to the system.

3.1.4 Replay Protection

Another important security objective is having replay protection. Now, there are replay-attacks which are when a message that was already sent is sent a second time by an adversary. As a result, this can greatly exhaust the receiver's computational resources by having to execute the same task more than once when it could focus on another message. So, having protection against these messages is important to avoid the waste of the device's resources.

3.1.5 Non-Reputability

Finally, the last security objective is non-reputability. This last objective refers to the fact that any message or action being sent by either the operator, master terminal unit, or remote

terminal unit should be able to be identified without question. If the case arises where a message's source device can't be identified, then this is when the receiver should be immediately aware that the device that made the message is most likely not part of the system, and the message should be discarded. Now, each of these security objectives have their own vulnerabilities that can be exploited and can potentially harm the system and cause damage, however, by ensuring that these are protected to a certain extent, since every attack can't be predicted, then in this way the system can become resilient to cyber-attacks and protect the safety of the public.

3.2 Category of Attacks

Now, there are two categories for the attacks that target SCADA systems, there are passive and active attacks. First, a passive attack is the attack that targets the information that is being transmitted among the devices however, this information is not tampered with or modified, instead an adversary that got access to this link is instead listening or reading the information. So, this attack creates no harm to the system but, in any case, it must still be prevented because if the case happens where the adversary gets a hold of important information, then more sophisticated attacks can be prepared, launched, and cause bigger damage to the system. On the other hand, active attacks target either a specific device or the ongoing communication that is happening among two devices. The main objective from this category of attacks is to make the overall system unusable where communication takes longer, or messages are modified, and the receiver performs an unintended action compared to what the source had generated. So, these types of attacks can become dangerous if they are not detected within the system, because if left unchecked, then the attack can keep growing and, ultimately, compromise the system.

3.3 Passive Attacks

As mentioned before, passive attacks are the ones who don't cause any harm to the systems or the communication because no modification or infiltration is happening, yet there are unauthorized users who are accessing a type of information which they shouldn't be able to.

3.3.1 Eavesdropping

Now, a kind of attack that falls under the passive attacks category is eavesdropping, shown in figure 2. Eavesdropping is when an adversary infiltrates itself into the system without being detected and can listen in to the conversation that is happening within the network with no authorization. Moreover, eavesdropping doesn't necessarily cause any damages to the SCADA systems; if the adversary doesn't find any useful information, then this information can be discarded, and no damage is created. However, if the adversary gets a hold of important information within the communication of the devices, then this is where it can become hazardous because the classified information can now be used to cause harm into the system. In the case of the SCADA system, for example, the eavesdropper can potentially be listening the communication between a master terminal unit and a remote terminal unit, and for the most part they can be sharing information about what the outstation is reporting, but the adversary can also listen on, perhaps, the sharing of an authentication key that only the master and outstation should know, and this can cascade to bigger attacks from the adversary.

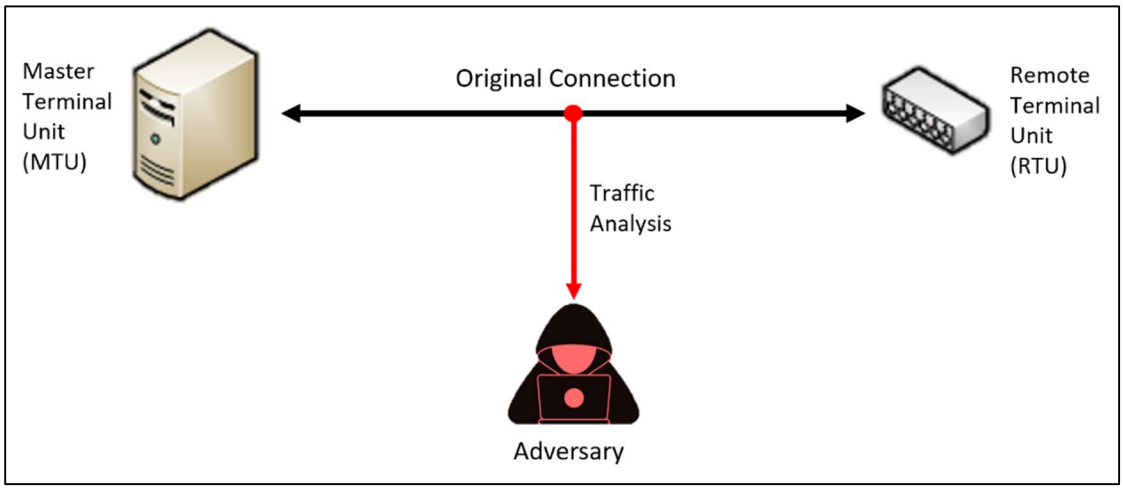

Figure 3.1 – Eavesdropping Attack

3.4 Active Attacks

Passive attacks can have or not a specific target, but for the most part they just listen on the traffic on the network however, active attacks are different since these types of attacks do intend

harm on the communication or the system itself by overwhelming a receiver; tampering with the communication of two devices that are communicating; or intercept messages and modify them entirely from the original intention behind the action. So, the following set of attacks will illustrate the category.

3.4.1 Denial-of-Service

Now, the first type of attack shall be the Denial-of-Service ash shown in figure 3. This attack's primary objective is to cause limitations on the system, and the limitations can range from having delayed messages to having a complete denial of service to the feature that the device or operator are trying to use. Moreover, this attack works by overwhelming the receiver with unwanted messages, and due to the fact that the receiver must check first if they are legitimate or not, then this consumes a portion of its resources. Now, when many more messages keep arriving to the receiver, then this is when all of its resources are working at full capacity to see every message and, ultimately, creates a denial of service for other devices that are trying to reach and communicate with the device that is being attacked. Furthermore, since this attack is targeting the communication between devices, then the security objective that is being compromised is availability.

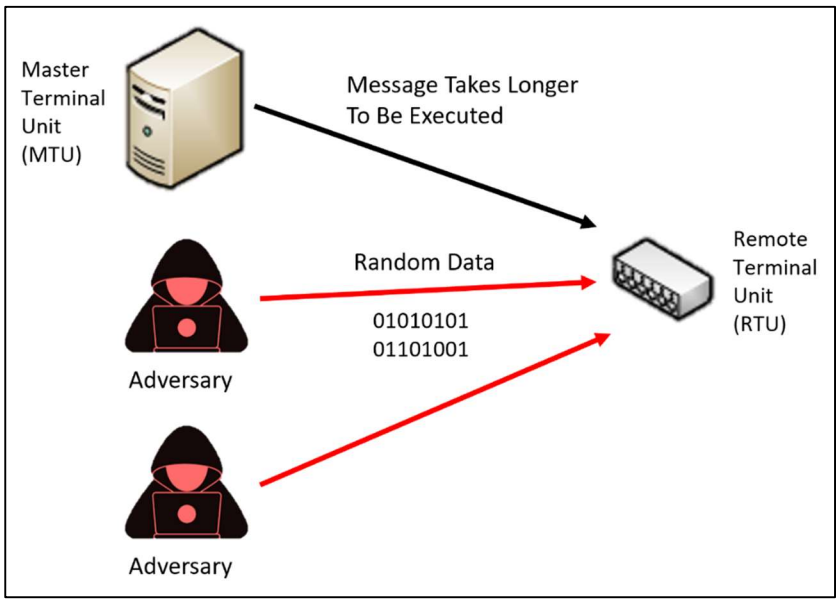

Figure 3.2 – Denial-of-Service Attack

3.4.2 Spoofing

Another kind of active attack that targets SCADA systems is spoofing, ash show in figure 4. This attack hinders both the authentication and the authorization security objectives by an adversary successfully infiltrating within the system and having the authorization to give commands to the devices. Moreover, this attack can be disastrous because the fact that the adversary can now communicate successfully with the devices that it is linked to, and it can be authorized to also send harmful messages to each of the devices and implement what the adversary sends depending on the commands sent, and unless the linked devices have an intrusion detection system implemented into it, then this is when the SCADA system must be resilient to the attacks that are being sent by the adversary until a new set of keys are distributed to the devices to re-authorize them. So, overall, this active attack can have a big impact on a portion of the system, and spoofing doesn't necessarily need to be strictly targeting the important devices that are high in the hierarchy, they can also target and infiltrate themselves as an outstation, but the most that they'd be able to do is to stop collecting the reported information from the field devices.

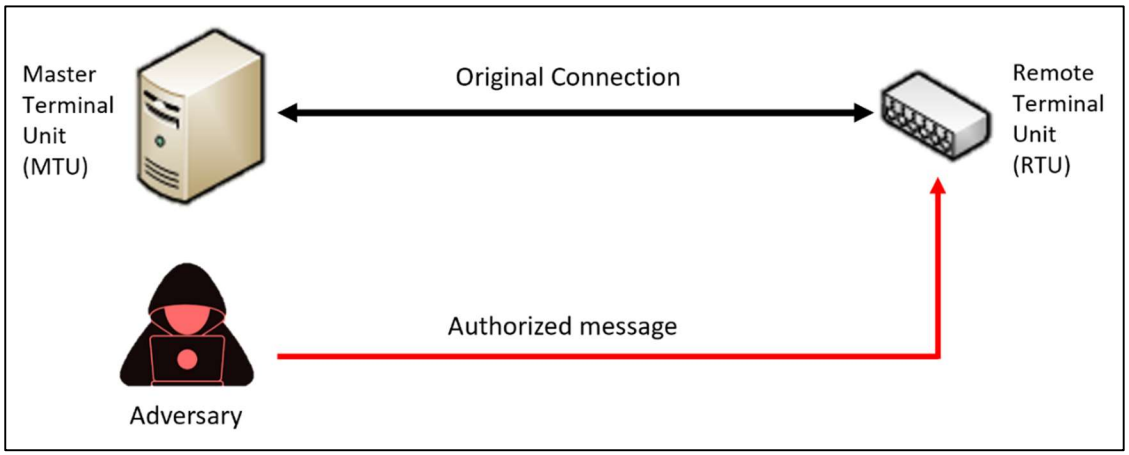

Figure 3.3 – Spoofing Attack

3.4.3 Man-In-The-Middle

The third kind of attack that targets SCADA systems is the man-in-the-middle, as shown in figure 5. Now, this attack targets both the authentication and integrity security objectives. First

the authentication security objective is being infringed because the man-in-the-middle attack is similar to spoofing in regard to an adversary successfully infiltrating itself within the system but now in this case, the adversary, as the name of the attack implies, the adversary is in the middle between the communication of two devices. Now, for example, if the two devices that are talking is a master station and an outstation, the master station is responsible for sending messages check-in messages for when the outstation doesn't send its reporting messages every so often, but if a successful man-in-the-middle attack was made, then that means that the adversary was authenticated. Moreover, the messages that are being sent by the master station can be modified by the adversary and an intended message to provide an update on the information being captured by the field devices can change entirely to make the outstation reboot entirely, and this is the reason why the second security objective of integrity is compromised by this attack. So, just like spoofing, having man-in-the-middle attacks within the SCADA systems can have big impacts on it and they can scale from small attacks, such as reboots, to bigger attacks that can damage the overall working of the system.

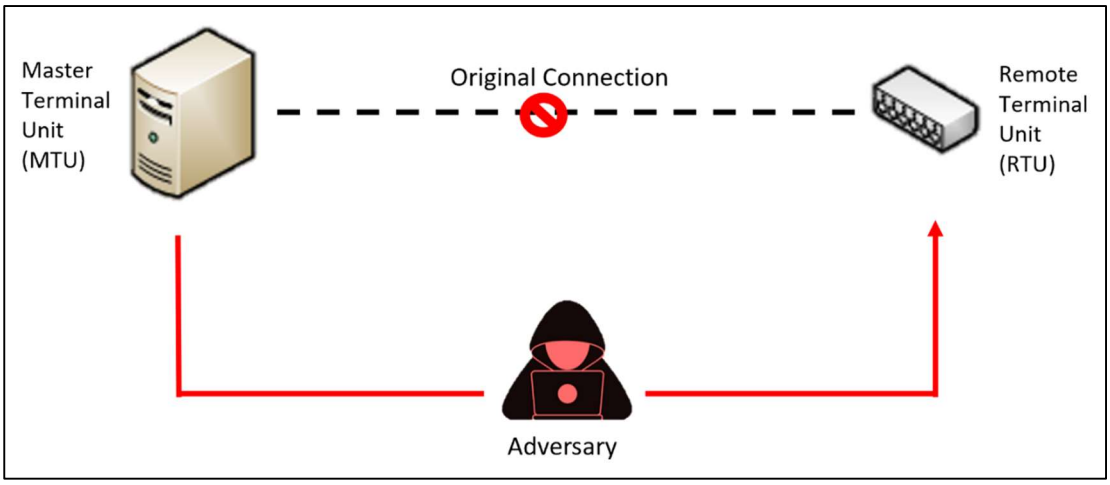

Figure 3.4 – Man-In-The-Middle Attack

3.4.4 Replay-Attack

The last kind of attack that targets SCADA systems are the replay-attacks, shown in figure 6, and, as mentioned before in the security objective subsection, the security objective that it compromises is replay protection. Now, this attack is similar to Denial-of-Service in which both attacks aim to

overwhelm the target device by leading it to waste its computational resources. Moreover, replay-attacks take a legit message that was fabricated by an authenticated device within the SCADA systems, and then it replays the message by sending it once again to the receiver therefore, since the message was authentic, the receiver will execute the instruction of the new message, even though it had already executed the same instructions with the previous received message. So, in the same case as Denial-of-Service attacks, the SCADA system should be able to identify when the received messages are duplicates from previous messages sent and shall be discarded to protect the devices. Now, with both types of attacks described and mentioned the attacks that fall under each category, respectively, an optimal SCADA system should, at the least, be able to stay resilient to the attacks from adversaries because, the fact is that all cyber-attacks are unpredictable and some attacks won't be able to be discarded or be dealt with on the spot; so a system that is resilient and keeps operating under these circumstances is the optimal system to keep critical infrastructures as safe as possible.

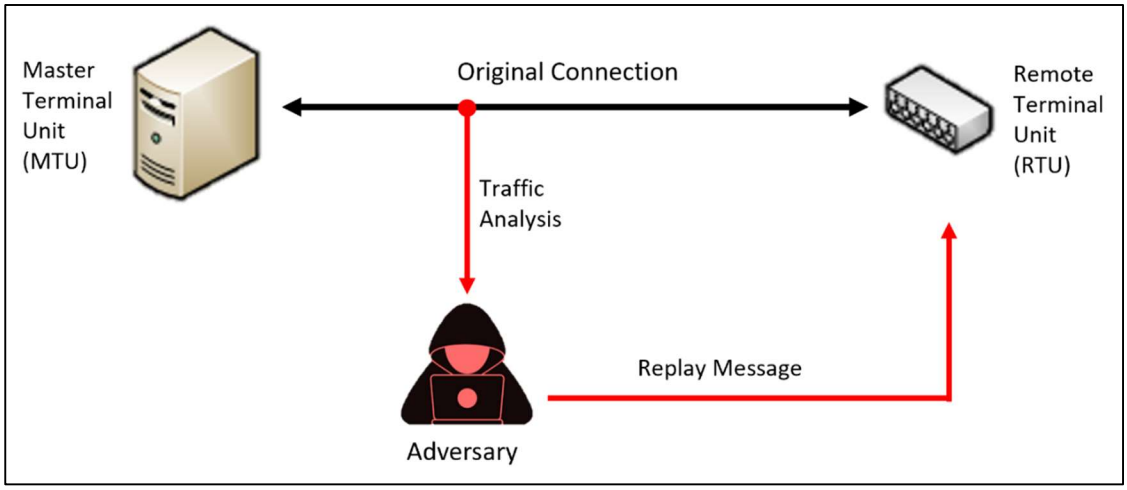

Figure 3.5 – Replay-Attack

CHAPTER 4: DISTRIBUTED NETWORK PROTOCOL VERSION 3

When SCADA systems continued growing and expanding, a demand for a communication protocol was growing as well. This was because either the protocols available wouldn't meet the system's requirements or the protocols weren't interoperable, meaning that only devices from the same manufacturer were to be utilized for the system since the manufacturer would implement a specific protocol for their products.

4.1 DNP3 Architecture

Now, in the late 20th century, a modification of the Open Systems Interconnection (OSI), developed by the International Organization for Standardization (ISO), from its 7-layer model, a three-layer model was proposed by the International Electrotechnical Commission (IEC) tailored specifically for the communications within the SCADA systems, and it became to be known as the Enhanced Performance Architecture (EPA) model. Moreover, based on the model two communication protocols were developed with the function to work for the benefit of the SCADA systems, and these were the Distributed Network Protocol 3 and the IEC 60870-5-101.

4.1.1 Physical Layer

As shown in figure 7, the architecture of the DNP3 communication protocol is shown. Starting from bottom to top, the first layer is the physical layer. Now, the physical layer is responsible for being the medium between the receiver and the transmitter because this layer will be the one that transmits when the device wants to communicate with another device and vice versa. Moreover, the methods of communication that the DNP3 protocol utilizes are half-duplex and full-duplex. Now, half-duplex is when the communication between two devices is both ways, so either device can transmit and receive messages however, half-duplex only allows the communication to happen at once, so one device gets the opportunity to transmit and the other to receive, then the second device now gets the opportunity to transmit afterwards. On the other hand, full-duplex is when both devices are communicating at the same time, so they can both be transmitting and receiving simultaneously. Furthermore, since DNP3 supports different types of topologies for communication, another important task of the physical layer is to keep all of the

incoming message in order to not mix up all of the data being received and depending on the communication method implemented, the device can attend to the replies for each of the devices, respectively.

4.1.2 Data Link Layer

The next layer within the DNP3 architecture is the data link layer. Now, this layer has an important task at hand since it maintains the transmission between two devices that are communicating. So, the data link layer ensures that the communication between the two devices is still going because during the transmission errors can be occurring, and while these are avoided, the data link layer can still correct these and keep the transmission. The data link layer is also responsible for converting the link service data units (LSDU) – which is the output from the transport layer, the transport data units (TPDU) – to link protocol data unit (LPDU), and the result of the LPDU will go to the physical layer with the source and destination addresses, a control byte, and the cyclic redundancy cycle (CRC) generated codes, and all of the appended bytes to each of the fragments will result in an LPDU frame of 292 bytes.

4.1.3 Pseudo-Transport Layer

The following layer in the architecture is the transport layer. Now, as mentioned earlier, the EPA model is only a three-layer model however, the transport layer is not the final and third layer for the DNP3. The transport layer is added to the architecture and counted as a layer because it is limited contribution to the DNP3. Moreover, the transport layer is called pseudo-transport and it is made of two layers, the limited transport layer, and the limited network layer. So, the job of the transport layer is to receive the data that is being sent from the above layer, the application layer, and since this data is big, transport service data units (TSDU), and has a total size of 2048 bytes, these get shrunk down into chunks of data, TPDU, with a maximum size of 249 bytes so the data link layer can fit each of the TPDU's into the frames for the message transmission. Moreover, the transport layer is also responsible for doing the same job but the other way around when there is incoming data to the device. The incoming messages come in the format of TSDU's, and the transport layer converts them to TPDU, 2048 bytes message, for the application layer.

4.1.4 Application Layer

Now, the last layer of the architecture is the application layer. The main tasks of the application layer are to collect data from the user, which is turned into the application service data units (ASDU), so it can be sent either to a connected master station or to an outstation. In addition, requests can be created which are meant to be sent to the outstations and these include commands to be executed, or simply send data to the outstation or request any data from it. In any case, the ASDU's are turned into application protocol data units (APDU), with a total size of 2048 bytes, which is utilized as input for the transport layer.

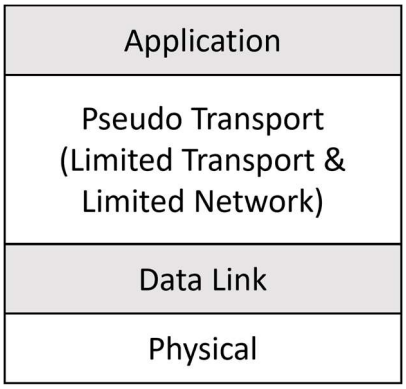

Figure 4.1 – Distributed Network Protocol Version 3 Architecture

4.2 DNP3 Message Build-up

Moving forward when all the layers are working together, then this is when the DNP3 protocol shines and creates a message to be transmitted to another device and the receiving device can decipher what was sent in the message. Now, to reiterate the mentioned architecture, for example, the user requests are collected by the application layer, which is turned into data fragments, then this information is passed on to the transport layer which then breaks each of the blocks of information into smaller fragments of data to be sent as input for the data link layer. Next, after the data link layer has established the transmission, then to the received fragments of data, the addresses and security is added to the information so it can't be deciphered – only by the receiver – and, at last, it is transmitted by the last layer of the architecture, physical layer, as shown in figure 8 with the building of a message.

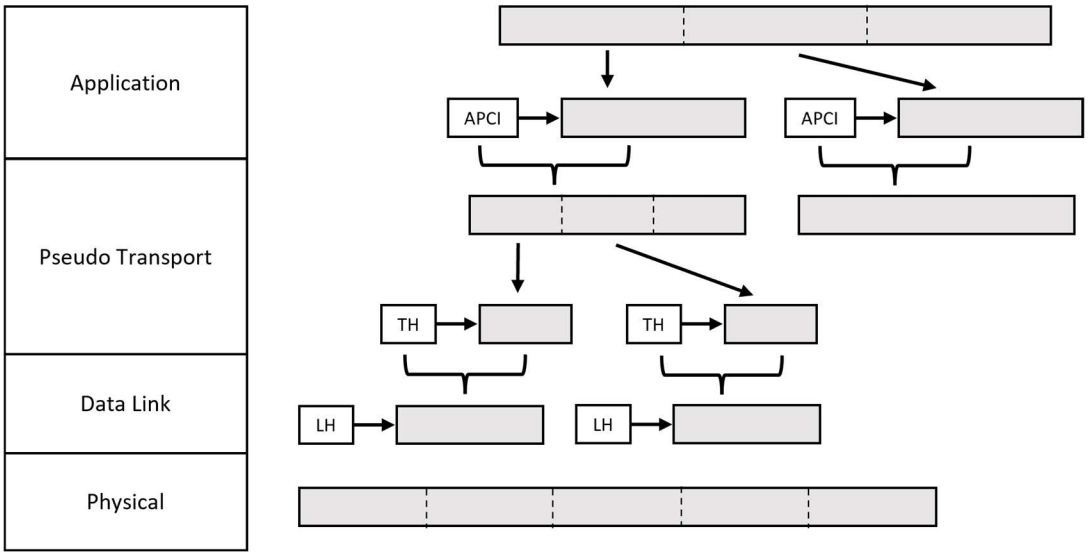

Figure 4.2 – Distributed Network Protocol Version 3 Message Structure

4.3 Importance of DNP3

Currently, DNP3 is the leading protocol, within North America, that it is being utilized and this is because of the benefits that it offers. As shown earlier in figure 4.2, DNP3 has the ability of breaking down the collected data from a user's request, and this data goes through a transformation, and this is important because it allows the system to pick up on any errors being produced, so they can be fixed. Moreover, the fact that the messages get broken down into multiple fragments, it allows for faster transmission and enables for faster communication between the link on the devices. Another important feature for DNP3 is being able to time stamp, which is the ability to add the time and date from when a message was manufactured and add this information to the message that is being sent out to a receiver. Knowing this information of when a message was sent is crucial because in the case that there was a fail in the system, the root of the cause can be tracked down by pinpointing the exact time that the failure happened and, most of the time, the cause could have been due to an attack on the system, therefore tracking down which message was sent at what time can save the operators time to resume the operation within the system.

In addition to the features provided by DNP3, there are also immediate and long-term benefits from utilizing the communication protocol. Now, the biggest benefit from the protocol is the ability to offer interoperability within the SCADA systems utilizing different manufacturer's

products. This provides a big opportunity for a company to not rely on a single manufacturer, because if the company only relied on a single manufacturer, then prices for maintainability and services would be very high. Now, acquiring products from different manufacturers might provide higher quality and performance and among all the competitors that are selling on this market, demand would remain the same among them. Touching back on interoperability, on the long run, while the system keeps growing and scaling, when new devices are being implemented into the network, since DNP3 is interoperable with other devices with the same protocol, no protocol translator would be required to initialize the device into network while still being able to provide a reliable and efficient transmission during the communication with the SCADA systems.

4.4 DNP3 Topologies

Another major and important feature from DNP3 is its ability to support a versatile topology implementation for SCADA systems. As shown in figure 4.3, the different topologies that are being demonstrated are direct connection, multidrop, hierarchical, and multiple master topologies. The most common type of topology is the direct communication, which is the connection of a remote terminal unit to a master terminal unit, or if the master terminal unit is serving as a slave, a direct connection between it and another master terminal unit higher in the hierarchy. In addition, the multi connection topologies are both multidrop and hierarchical, which for multidrop it entails the connection of multiple remote terminal units to a single master terminal unit to collect information from multiple sources and hierarchical is when a high rank master terminal unit can be connected to a remote terminal unit and another master terminal unit that is serving as a slave. At last, there is the multiple master topology, which is when two master terminal units are sharing the information that is being gathered by either a remote terminal unit or, perhaps, another master terminal unit.

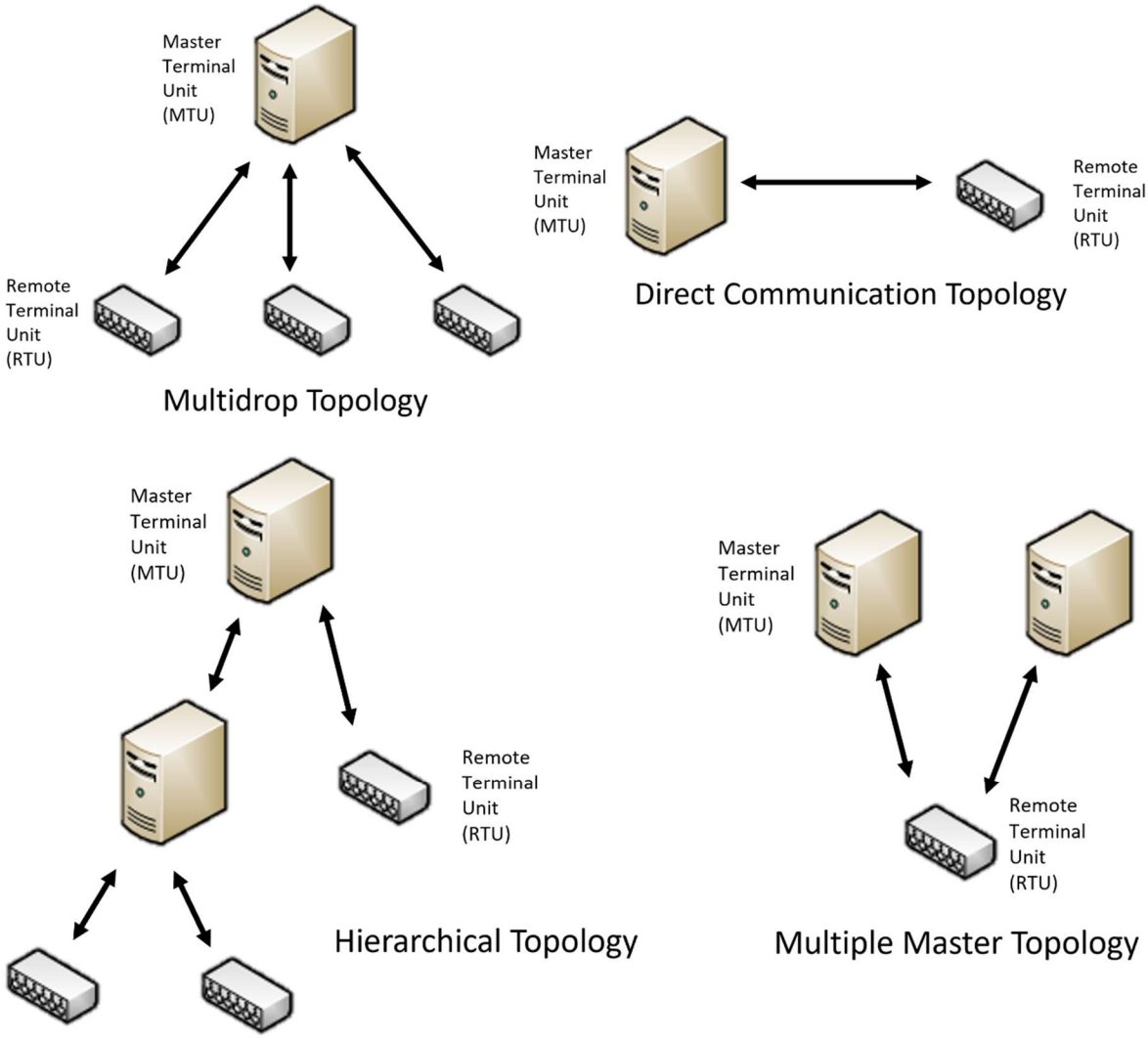

Figure 4.3 – Distributed Network Protocol Version 3 Topologies

Now, depending on the application from the company that is implementing a SCADA system, all these topologies are relevant and can be utilized to towards the success of the system. For example, there can be outstations that are acquiring important information from different field devices and letting multiple master stations have access to the information is essential for the system. Furthermore, a combination of hierarchical and multidrop topologies can be the most optimal to allow the system for scalability and growth. When a master station is allowed to communicate to multiple outstations at the same time, it allows for the company to use the full resources of a single master station to control and monitor the outstations. On the other hand, a balance should be considered with how many outstations are connected to a single master station,

because overwhelming a single device can cause a small lifespan for the device and slow communication on the overall system. Now, when one master station is collecting all of the information of multiple outstations and it is acting as a slave device to another master station, the next master can be also monitoring multiple master and outstations as well, so the system's devices work in compliance with each other so no device within the system experiences overhead from all of the communication that is happening within its node.

4.5 Operational Modes in SCADA Systems

Regardless of the topology being utilized, whether there is a master terminal unit connected to another or if a master terminal unit is connected to a remote terminal unit, there are two ways that devices can communicate in a master and slave procedure, either through polled or by quiescent operation.

4.5.1 Polled Operational Mode

For polled communication it's when the master specifically requests the slave to report back the information that it has been gathering, and the slave shall respond with the requested information in a reply to the master. This method is efficient for when the master station needs a specific type of information in a certain time limit and it needs to keep asking for it however, at the same time it is inefficient because it takes time from the master to put together a message and send it to the slave. Moreover, the slave gets interrupted from its course of action to reply to the master station first, since it has higher priority than what it is currently doing.

4.5.2 Quiescent Operational Mode

Now, the second method for communicating is quiescent operation. For this method, the slave can send unsolicited messages back to the master without the request of the master and it only sends messages back to master when there are changes in the operation. Compared to the polled method, quiescent is more efficient because the master doesn't have to create a request message and wait for a reply, instead the outstation is responsible for notifying the master station

of the changes. On the other hand, it is also inefficient because if the master station needs specific information, then the master station wouldn't have access to that information. So, by implementing both communication schemes, the best of both worlds creates an optimal communication for the benefit of the SCADA systems.

CHAPTER 5: DNP3 SECURITY

DNP3 capabilities have already been mentioned, but there are still issues within the smart grids infrastructures implementing SCADA systems. The complexities fall on having legacy systems, how expensive it is to upgrade them, and how complex the systems are. Moreover, when implementing the public key infrastructure (PKI) into the systems, this ties directly to the scalability issues within the infrastructure.

5.1 Legacy Systems

Legacy systems are defined as the systems that were utilized when critical infrastructures were first implemented into the system. In addition, minor changes are included in the legacy systems such as the replacement for a portion of the components for newer versions, however for the main parts of the infrastructure, these remain and operate in the same way since it was first implemented. As mentioned, leaving the legacy systems as they are, these brings big complexities for the overall performance of the system. Now, because of the new technologies that are being developed, new attacks are being created and implemented which can ultimately surrender the system. So, the solution that companies are geared towards is trying to implement new technology to the legacy systems. While this is a viable solution which can include a lot of new capabilities to the legacy systems, at the same time, replacing all of the technology from all of the components scattered throughout the infrastructure, then this is when the company suffers from a big expense. Now, if the case was that the company was able to afford a big expense such as this, where they are able to replace all of the current technology with new; during those years, they'll meet with all of the demand and, potentially, almost all cyber attacks that target the SCADA systems however, eventually they'll face the same situation where the same technology isn't enough to provide for the infrastructure and another big expense must be made to resolve the same issue. So, acquiring new technology is just a temporary, ineffective, and expensive solution for the current system.

Another important issue with legacy systems is knowing how complex a system is. Now, when companies are designing and implementing a system, the mentality is usually to make the system as complex as possible to prevent any attacks into the system. However, having a very complex system also makes it difficult for the devices to communicate among themselves, due to complicated routing methods, and due to the complexity, it increases the possibility of the system

having vulnerabilities. Moreover, since the system might have a longer time trying to pin down where a message originated, then this is an opportunity for an adversary to get in and perform a cyber-attack. So, having a very complex implementation for a system wouldn't be a viable solution.

5.2 Scalability Issues

As mentioned in the previous chapter, one of the benefits of DNP3 is its ability to offer interoperability by setting a standard for all manufacturers, so their products are able to communicate with the devices of other vendors. As a result, this enables for companies to grow and scale the system. So, to achieve a secure communication among all of the devices, a security implementation such as the public key infrastructure would aid the system. Now, the public key infrastructure consists of implementing a public key cryptography. This method consists of having a total of two keys, both generated by a device that wants other devices within the system to communicate with it securely. The first generated key is a private key for the devices to keep and the second generated key is a public key. An external device with the key is able to encrypt the information with its public key and the device with the private key is able to decrypt the information with its key. Now, to issue a public key, the device must first be authorized before hand by acquiring a digital certificate, and this certificate is distributed by the certificate authority. Once, the device has been confirmed and cleared that it is in fact legitimate, then now it can utilize its public key for communication. Now, after the implementation of the public key infrastructure, this is when scalability becomes an issue. Even though the public key infrastructure provides optimal security and traceability – to see who is sending the messages to the device – it is preferred to be utilized within a small scale to provide the best security, and the reason is because of the key management. When the cryptographic method is distributing the keys among the devices on the system, the bigger the system the more digital certificates the certificate authority must create for all the authentic devices. In addition, the update for new digital certificates, due to new key generation and certificate distribution creates overhead, when devices are utilizing their computational resources either close or to the limit causing the device to reach the end of its life faster, for the system.

5.3 Lightweight Protocols

In brief, problems that target SCADA systems are majorly during scaling i.e., when system is growing and expanding. There are issues that surface when the company has to replace the components in place for newer ones, as always this is a temporary fix and will rise once again in the future. There are issues when creating a new or reconfiguring the connections within the SCADA systems, which also creates vulnerabilities within the system that can be exploited. Other challenges due to scaling is the implementation of very secure protocols such as the public key infrastructure, which becomes difficult with system size.

One way to approach this problem is by the implementation of lightweight protocols into the system. Lightweight protocols refer to the capability of the protocol to not create a lot of strain on the devices which, ultimately, leads to overhead. Instead, these lightweight protocols are manufactured to provide high security while considering the capability of each device. Some of these new protocols include BLAKE2, SHA-3, and elliptic curve cryptography. In chapter 7, these will be discussed in further detail for their application, but both BLAKE2 and SHA-3 provide authentication, and elliptic curve that can provide combination of both symmetric and asymmetric cryptography features. Now, lightweight protocols can be very beneficial for legacy systems, because either by doing an update to the system software or adding the minimum amount of hardware to have these protocols running for the protection of the device and system, security could be added. Moreover, the protocols can add a strong authentication or encryption. Therefore, designers responsible for the implementation of the SCADA systems won't have to rely on making the system complex and keeping the system simple to avoid any vulnerabilities in the system. Finally, since complex cryptographic methods of public key infrastructure with larger bit sizes, would be replaced by lightweight protocols such as the elliptic curve, then scalability problems could be addressed to a larger extent.

CHAPTER 6: DNP3 SECURE AUTHENTICATION VERSION 5

One of the features that sets DNP3 apart from the other compliant SCADA systems protocols is its secure authentication feature, which only allows authenticated devices to transmit within the infrastructure. Now, the purpose of having this feature is for master stations to authenticate the outstation that they are talking to or if the master station is serving as a slave to another master station, it would be same instance, and, moreover, it's to ensure that the communication is intended to the intended receiver and no other device. On the other hand, when the outstation is communicating to a master station, with secure authentication, the outstation can ensure that only an authenticated device higher in the hierarchy can utilize its resources.

6.1 Action Principle

Even though the secure authentication feature from DNP3 only implements authentication as its security measure, it can still address and target spoofing, modification, replay, and eavesdropping attacks coming from adversaries. [4] This can protect the system from attacks that either intend to change the integrity of the communication or any action messages intended to make unintended actions upon an outstation. In addition, keeping the devices safe from being overwhelmed of doing a task more than once. Now, the threat of eavesdropping, with this security measure, it only addresses the keys that are being exchanged between the devices, so no adversary is able to get a hold of these.

Since the secure authentication feature is part of the application layer within the DNP3 architecture, then for authentication, both the master stations and outstations utilize the application service data units, being generated from the application layer message, to authenticate the messages that are being transmitted. However, not every single message that is being transmitted is going to be authenticated and the difference between which is and which isn't authenticated resides on whether the message is a critical ASDU or not. If the message is a critical ASDU, then the action will be challenged. In brief, the mechanism that secure authentication utilizes is challenge and response and it means that for every critical ASDU that is being received by the outstation, then the outstation is assuming that its resources are trying to be utilized by a master station, respectively, and instead of replying directly to the command or before executing the actions that are being requested, the outstation will solicit the device to authenticate, challenge

message to the master station, itself before the outstations moves on further and process the received message. Afterwards the master station will reply with an authentication and if it is verified, then it will be executed.

6.2 Non-Aggressive Mode

Furthermore, the mechanism that secure authentication utilizes can be utilized in two ways, and the first is the non-aggressive mode. [7] Now, within this mode, as shown in figure 6.1 and figure 6.2, the master station can communicate regularly with an intended outstation with non-critical ASDU's. Subsequently, the master station now asks for a specific action within its message and sends a critical ASDU to the outstation. Then, the outstation needs to respond with an authentication challenge as a message to the master station and, the master station shall reply with an authentication response, which includes a message authentication code (MAC). Now, the MAC is generated by utilizing a session key, which both parties share. The outstation then takes the message and processes the authentication response and if it is verified, then and only then, will the outstation process the critical ASDU that was sent at the beginning. Next, the outstation will only reply to what was being requested through the critical ASDU.

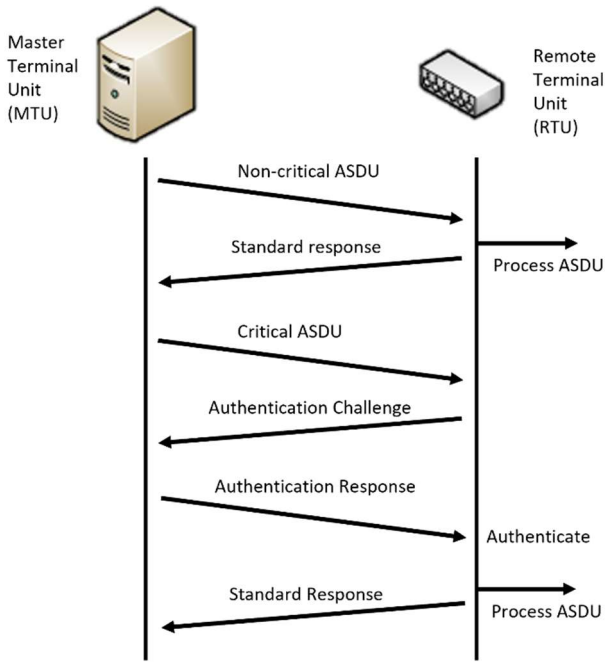

Figure 6.1 – Non-Aggressive Successful Challenge Between Master Station and Outstation

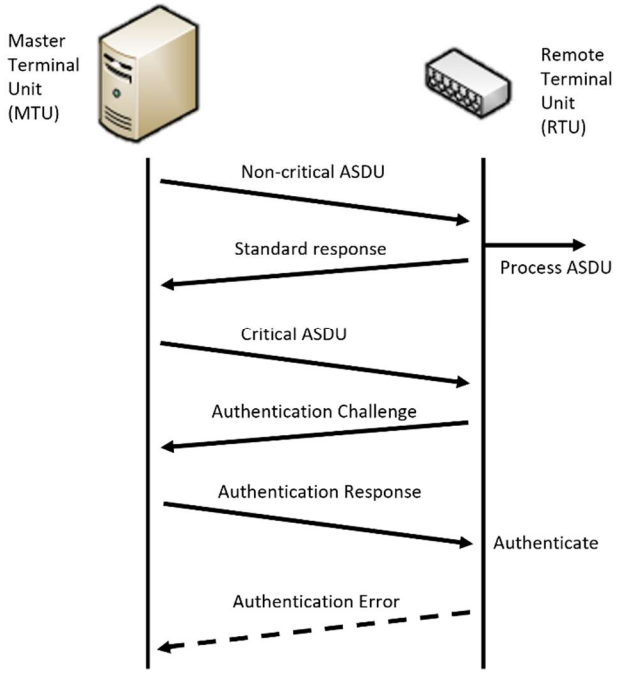

Figure 6.2 – Non-Aggressive Unsuccessful Challenge Between Master Station and Outstation

6.3 Aggressive Mode

The second way for the challenge and reply mechanism for secure authentication is the aggressive mode, as shown in figure 6.3 and figure 6.4. [7] The aggressive mode is very similar to the non-aggressive mode. If the master station decides to send a non-critical ASDU, then the outstation will reply to the master station without taking further action either. Now, when the master station asks to execute something important, once again, the critical ASDU will be sent but now, since it will be sent in aggressive mode, the message authentication code will be sent along with the critical ASDU. Next, the outstation will receive the critical ASDU request from the master station, but since the authentication response was delivered as well, then there is not a need to send an authentication challenge. Afterwards, the outstation will process first the MAC and once being authenticated, then it will process the critical ASDU, and reply to the master station that its request had been processed.

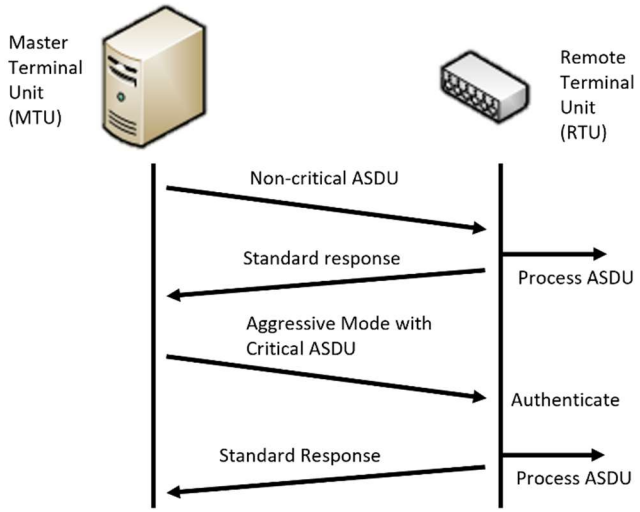

Figure 6.3 – Aggressive Successful Between Master Station and Outstation

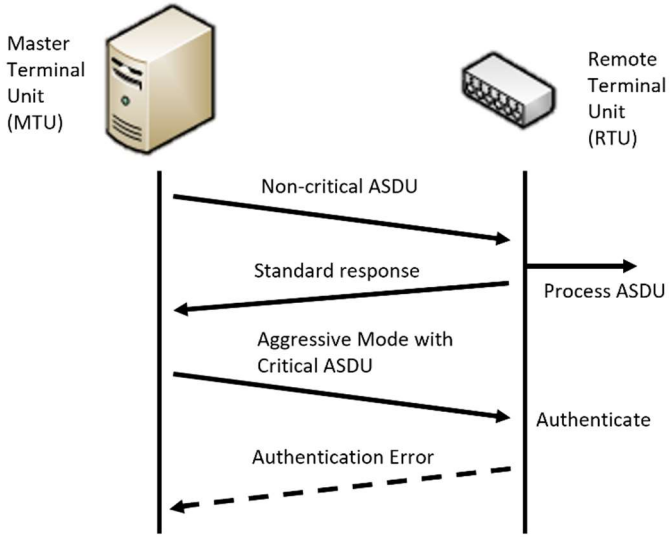

Figure 6.4 – Aggressive Unsuccessful Between Master Station and Outstation

6.4 Application & Role of Keys

In DNP3 secure authentication, as mentioned before, the message authentication code is generated by utilizing the session keys, and the MAC is utilized to authenticate that the sender device is part of the SCADA systems, so keeping the keys a secret is very important. Now, each of the devices within the systems will have their own session keys. In the case of the master station,

when he is going to either reply to an authentication challenge with an authentication response, or if he is going to send a critical ASDU with the MAC, in either case, the master station utilizes its session key to generate the MAC and send it as a message to the intended outstation. Next, the outstation with its own session key, respectively, it will authenticate that the generated MAC message was sent by an authentic master station within the network. However, even though these keys have a great task for authentication, they must keep being changed after a certain period of time so there is no chance of them being compromised by an adversary for staying within a device too long, and they can be changed with symmetric or asymmetric methods.

6.4.1 Symmetric Keys

If the devices that are communicating are configured to use symmetric cryptography, then the devices shall utilize symmetric keys for communication, and there will be a total of four important set of keys that are utilized for the success of the communication. [7] Now, symmetric cryptography entails that when two devices are communicating, the same key and algorithms are used by both communicating devices for the sender to encrypt the information and the receiver can decrypt the sent message. For this example, since there are three entities, the authority, master station and outstation, there are only four keys but upon having a bigger system, then more keys shall be generated for each device, respectively. The first two set of keys are the session keys, and these are shared between the master station and the outstation. The master station has the control direction session key, and the outstation has the monitoring direction session key, and the purpose of both keys are to authenticate the data that is being transmitted their way. Now, both the master station and the outstation share the third key named the update key however, only the master station is authorized to utilize the update key. The purpose of the update key is for when the range of time comes to an end for the use of the current session keys in both devices; so, the master station utilizes the update key to encrypt the session keys and distributes the control direction session key to itself and the monitoring direction session key to the outstation. Afterwards, it will result in both devices having updated keys to resume the operation within the SCADA systems. Finally, the last key is the authority certification key. This key is only utilized by both the operator and the human machine interface, the authority, and only the outstation also has the authority certification key. In the case that an update key reaches the end of its use and needs to be updated, or if it becomes

compromised, the authority utilizes the authority certification key to encrypt the update key which is sent to the outstation, by the master station, to be decrypted and if it is valid. Then, the outstation can now utilize the update key and it will send a confirmation to the master station notifying it that it is valid. Once the master station confirms the response too, then it will also start utilizing the update key too. On figure 6.5 and figure 6.6 it depicts the update of both the session keys and the update keys too.

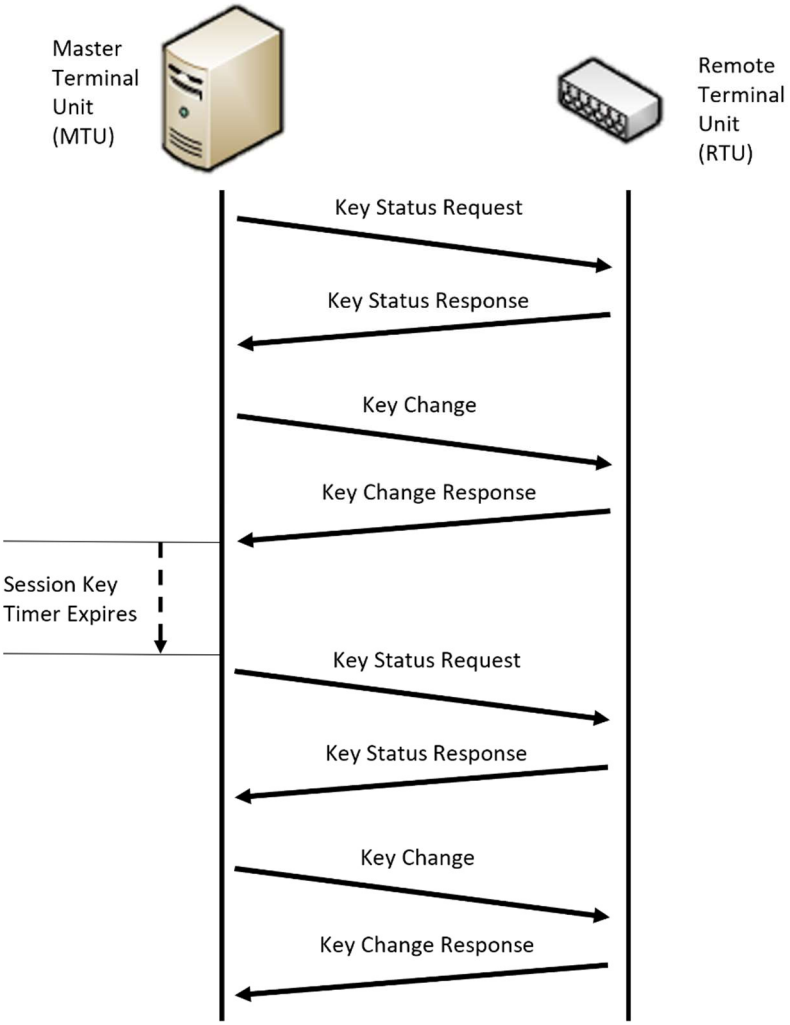

Figure 6.5 – Change of Session Keys

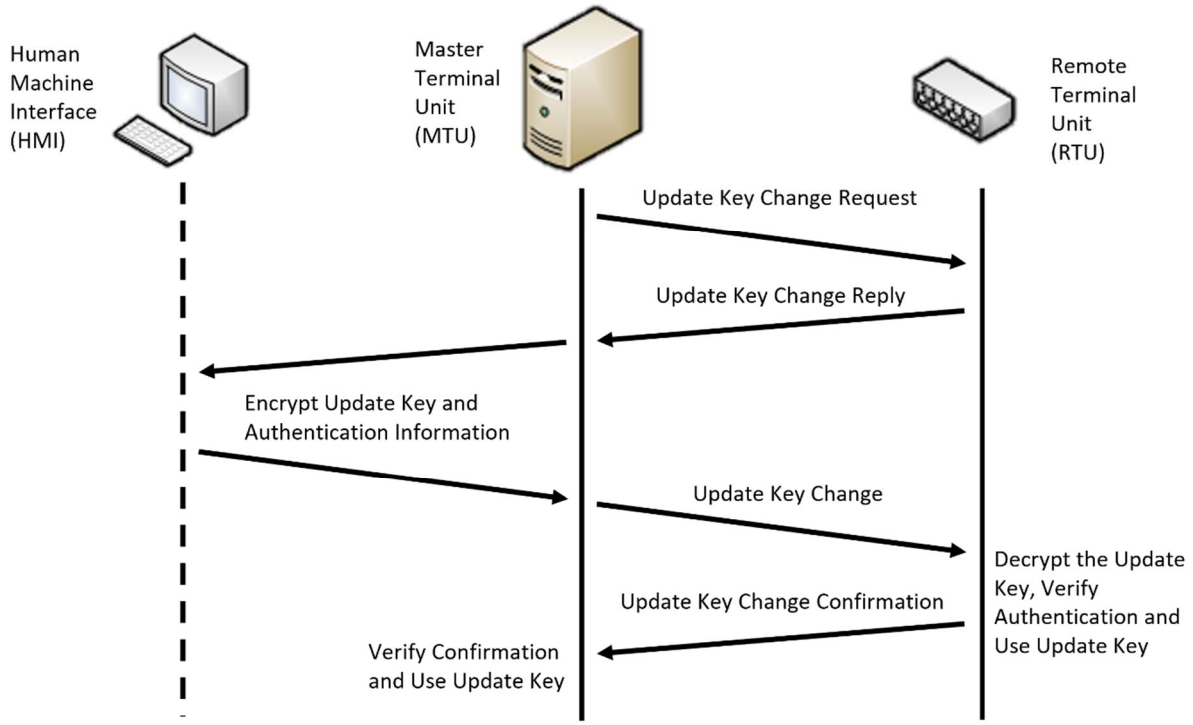

Figure 6.6 – Change of Update Keys

6.4.2 Asymmetric Keys

Now, if the devices are configured to utilize asymmetric cryptography, then the asymmetric keys will be utilized for the encryption of the information. [7] For asymmetric cryptography, the main idea of this method is that there is a total of two keys available for communication, the private key, and the public key. If a device wants to communicate with other several devices, the original device will generate the two keys, one private key for itself and a public key that devices can use to communicate. Furthermore, when a message is sent by the outside device, the message gets encrypted with the public key and the receiving device can decrypt it with the private key and read the message. Now in secure authentication, compared to the symmetric keys, in asymmetric there is a total of 6 keys. The authority, the master station, and the outstation each have their private key, and each of the private keys are generated within the devices except for the authority, which uses external help to generate its private key. Afterwards, public keys are safely distributed along the devices securely by trusted employees of the company. In addition, when public keys need to be updated, the same procedure would occur for the distribution of the keys after the new private keys

are generated. Now, even though it is mentioned that there are only three entities on these examples, but depending on the size of the system, each authority, master station, and outstation shall have one private key that the device utilizes to decrypt incoming messages from devices that have their public keys to encrypt the messages and transmit it to them.

CHAPTER 7: DNP3 SECURE AUTHENTICATTION VERSION 6

A new version of the secure authentication protocol has been released, and it is the DNP3 secure authentication version 6th, and just like its predecessor, it targets the same security issues with new features. The main changes that were implemented into this version are the changes made from the previous secure authentication version, the addition of the authorization management protocol (AMP), and how both protocols are working together to keep the critical infrastructures safe and ensure a safe communication among all the devices. Moreover, these protocols can utilize lightweight protocols such as BLAKE2, SHA-3, and elliptic curve cryptography for authentication and the distribution of the keys among the devices. Now, the implementation in this thesis will be discussed by explaining how a direct link communication was tested between a master station and an outstation and the information that was exchanged.

7.1 DNP3 Implementation

The implementation that was performed for this thesis was to initialize a communication link between two devices, a master station, and an outstation, and it was deployed on a virtual environment utilizing the Linux operating system Ubuntu 20.04. Within the virtual environment, a Linux terminal was opened, and the master station code was executed to and, as shown in figure 7.6, the master station is being initialized, then right after a menu is shown from the capabilities that the master station has access to, and all of these are commands that can be sent to the outstation for it to execute them, shown in figure 7.7. Now, while the master station is waiting for a link to connect to, another Linux terminal was opened, and the outstation code was executed here to create it. In addition, the same scenario happened as with the master station, where both the initialization and the action menu, capabilities of the outstation, were shown on the terminal, as shown in figures 7.8 and 7.9.

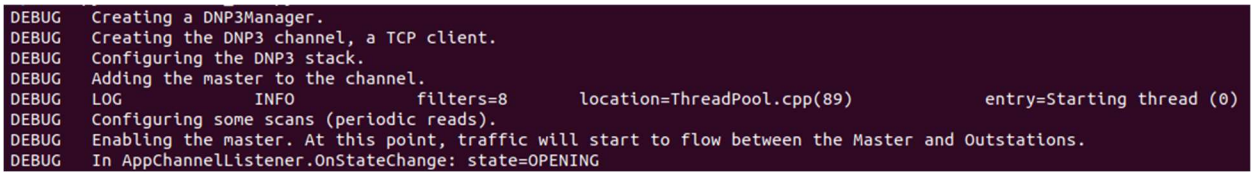

Figure 7.1 – Master Station Initialization Screenshot

```
Welcome to the DNP3 master request command line. Supported commands include:
       chan_log_all    Set the channel log level to ALL_COMMS.
       chan_log_normal Set the channel log level to NORMAL.
       disable_unsol   Perform the function DISABLE_UNSOLICITED.
       help            Display command-line help.
       mast_log_all    Set the master log level to ALL_COMMS.
       mast_log_normal Set the master log level to NORMAL.
       menu            Display this menu.
       o1              Send a DirectOperate LATCH_ON command.
       o2              Send a DirectOperate analog value.
       o3              Send a DirectOperate CommandSet.
       quit
       restart         Request an outstation cold restart.
       s1              Send a SelectAndOperate LATCH_ON command.
       s2              Send a SelectAndOperate CommandSet.
       scan_all        Read data from the outstation (ScanAllObjects).
       scan_fast       Demand immediate execution of the fast (every 1 mins) Class 1 scan.
       scan_range      Perform an ad-hoc scan (ScanRange) of GroupVariation 1.2, range 0..3.
       scan_slow       Demand immediate execution of the slow (every 30 mins) All-Classes scan.
       write_time      Write a TimeAndInterval to the outstation.
Please enter a command.
master>
```

Figure 7.2 – Master Station Action Menu Screenshot

```
    DEBUG   Configuring the DNP3 stack.
    DEBUG   Configuring the outstation database.
    DEBUG   Creating a DNP3Manager.
    DEBUG   Creating the DNP3 channel, a TCP server.
Starting thread (0)
    DEBUG   Adding the outstation to the channel.
    DEBUG   Enabling the outstation. Traffic will now start to flow.
    DEBUG   In AppChannelListener.OnStateChange: state=ChannelState.OPENING
```

Figure 7.3 – Outstation Initialization Screenshot

```
Welcome to the outstation request command line. Supported commands include:
       a               Analog measurement.     Enter index and value as arguments.
       a2              Analog 2 for MMDC.Vol (index 4).
       b               Binary measurement.     Enter index and value as arguments.
       b0              Binary False for MMDC1.Amp.range (index 6).
       c               Counter measurement.    Enter index and value as arguments.
       d               DoubleBit DETERMINED_ON.        Enter index as an argument.
       help            Display command-line help.
       menu            Display this menu.
       quit
Please enter a command.
outstation>
```

Figure 7.4 – Outstation Action Menu Screenshot

After the link has been established and the outstation is listening on the master station, then a communication between the two devices has commenced. As shown on figures 7.10 and 7.11, a message was exchanged between both the master station and the outstation. Now, there are bits found within each of the messages that are sent by the outstation these are the first fragment of a

multi-fragment message (FIR), the final fragment of a multi-fragment message (FIN), if confirmation is required (CON), if the message was unsolicited (UNS) and the fragment sequence number (SEQ). [6] All these bits determine how the master station will react towards the responses that it will be receiving from the outstation since, for example, if the outstation sends a 1 in the bit number for FIR and a 0 in the bit of FIN, then the outstation is notifying the master station that this is one part of the message and there is still more left to transmit. In addition, the delivery of these message would continue with the FIR bit being zero and until the outstation sends a message with the FIN bit being 1, then that would be the end of the transmission. Now, for the multiple bit SEQ part, either the master station edits this portion or the outstation. If the master station is requesting, polled action, the outstation to send the gathered information back to the master station, then the SEQ number would be from 0 to 15. Moreover, if the outstation sends an unsolicited message, quiescent operation, then the SEQ number would be from 0 to 31. Next, the functions that are being executed is a response request sent by the master station to the outstation. Afterwards, the outstation shall execute the read function to read from the collected data and transmit it back to the master station.

```
master  DEBUG   LOG  --AL->   entry=CA 01 3C 02 06
master  DEBUG   LOG  --AL->   entry=FIR: 1 FIN: 1 CON: 0 UNS: 0 SEQ: 10 FUNC: READ
master  DEBUG   LOG  --AL->   entry=060,002 - Class Data - Class 1 - all objects
master  DEBUG   LOG  --TL->   entry=FIR: 1 FIN: 1 SEQ: 11 LEN: 5
master  DEBUG   LOG  --LL->   entry=Function: PRI_UNCONFIRMED_USER_DATA Dest: 10 Source: 1 Length: 6
master  DEBUG   LOG  <-LL--   entry=Function: PRI_UNCONFIRMED_USER_DATA Dest: 1 Source: 10 Length: 10
master  DEBUG   LOG  <-TL--   entry=FIR: 1 FIN: 1 SEQ: 13 LEN: 4
master  DEBUG   LOG  <-AL--   entry=FIR: 1 FIN: 1 CON: 0 UNS: 0 SEQ: 10 FUNC: RESPONSE IIN: [0x00, 0x00]
```

Figure 7.5 – Master Station Request Message Screenshot

```
ms(1669685771540) --AL->  outstation - FIR: 1 FIN: 1 CON: 0 UNS: 0 SEQ: 9 FUNC: RESPONSE IIN: [0x00, 0x00]
ms(1669685771540) --TL->  outstation - FIR: 1 FIN: 1 SEQ: 12 LEN: 4
ms(1669685771540) --LL->  outstation - Function: PRI_UNCONFIRMED_USER_DATA Dest: 1 Source: 10 Length: 5
ms(1669685831545) <-LL--  server - Function: PRI_UNCONFIRMED_USER_DATA Dest: 10 Source: 1 Length: 11
ms(1669685831545) <-TL--  outstation - FIR: 1 FIN: 1 SEQ: 11 LEN: 5
ms(1669685831545) <-AL--  outstation - CA 01 3C 02 06
ms(1669685831545) <-AL--  outstation - FIR: 1 FIN: 1 CON: 0 UNS: 0 SEQ: 10 FUNC: READ
ms(1669685831545) <-AL--  outstation - 060,002 - Class Data - Class 1 - all objects
```

Figure 7.6 – Outstation Response Message Screenshot

For this implementation, DNP3 SAv6 wasn't integrated into the communication between the master station and the outstation, however from the features that the 6th version of secure authentication offers a strong and secure communication can be implemented. First, with the

implementation of the authorization management protocol, the master station and the outstation would be able to communicate as they currently are where they can both get linked based on authorization. In addition, with reply confirming that a certificate was granted from the security managers from each of the devices that are linked. In this way, if an adversary were to enter, then it would be recognized by the AMP protocol that an unauthorized device is attempting to communicate. Now that SAv6 offers encryption to messages, in the case that an adversary successfully infiltrated the network and it is eavesdropping; then, when the master station wants to share important messages, or vice versa, they can be encrypted to avoid important information falling on the wrong hands. Now, since DNP3 SAv6 supports the use of lightweight protocols such as BLAKE2, and ECC, both can be implemented into the communication. With BLAKE2, it can be utilized for authentication such as when an authority wants to make impactful changes to one of the devices, then these must be secured with additional security to avoid any unintended results, so following this process, only authorized devices are capable of making these changes. Moreover, with ECC being implemented to the devices when they are both generating the authentication update key and the encryption update key. At the moment of creating an association between devices and the session key initialization, ECC can be utilized to reduce the overhead on both devices, yet still offering security and ensuring that the keys won't be stolen or misplaced.

7.2 Secure Authentication Version 6 Details

The secure authentication implementation in the previous version was a success for the cyber-attacks that it addressed, but with new tactics and new technologies emerging, new cyber-attacks are being released, so a new version, DNP3 secure authentication version 6 (DNP3 SAv6), was manufactured and implemented. [11] For the 6th version of this protocol, just like with the 5th version, it is still implementing the message authentication codes however, this version now utilizes hash-based message authentication code (HMAC). The purpose of both technologies is to enforce the authentication of the sender and the integrity of the message. On the other hand, the difference is that HMAC utilizes a cryptographic hash function – which is a process to create a unique hash value based on the input and if any part of the message changes, then a whole new value is generated, therefore making this a very precise and secure authentication process – for

authentication and, in addition, HMAC is a pseudo-random function, so only random bits will be shown if verified with the proper key.

Now, the encryption method that secure authentication utilizes to encrypt that sender devices are transmitting is the AEAD-AES-256-GCM. [11] The mechanism that the encryption method uses is for when a message is being encrypted, a key is utilized and a nonce is produced. Since AES is a symmetric standard, then there is only one key available to both encrypt and decrypt the information, so the receiver must also have access to the key to be able to decrypt it and use the information within the message. One big feature that is implemented by AEAD is that the message won't be decrypted by the private key until this message is verified by the received nonce too, so this adds another layer of protection to ensure that the sender is legit and part of the system and, in addition, that the sender intended to send the message to this device.

7.3 Authorization Management Protocol Details

As mentioned before, one of the new additions in this version of secure authentication is the addition of the authorization management protocol. The purpose of this protocol is to manage which devices within the critical infrastructure are authorized to communicate with the rest of the devices. [13] This protocol is centrally managed by the DNP3 authority, and this can be either one interface or multiple ones. In addition, the security managers that have access to the authority can revoke the authorization privileges of the devices that are currently part of the system or when enabling devices to be authorized to send messages within the system, then the authority will provide them with an authority-signed certificate to finalize their authenticity. Now, this feature can greatly benefit the system because in the case of a cyber-attack to the SCADA system, the security managers can quickly mitigate the attack by locating the source of where the attack is originating and cutoff the link by removing any authorization the adversaries might've obtained. Now, since the AMP is centrally managed, it creates its own routing tables – the routing tables are utilized to route messages, that are being transmitted, among multiple nodes in the network by having access to the topology of network – to route the messages from the authority to master stations and outstations. Moreover, to increase the security within the system, the authority utilizes role-based access control (RBAC) and let the outstations know what master stations have certain authorizations. So, in the case where a master station sends a message requesting the outstation

out of the range of its capabilities, most likely it is an infiltrated adversary launching a cyber-attack.

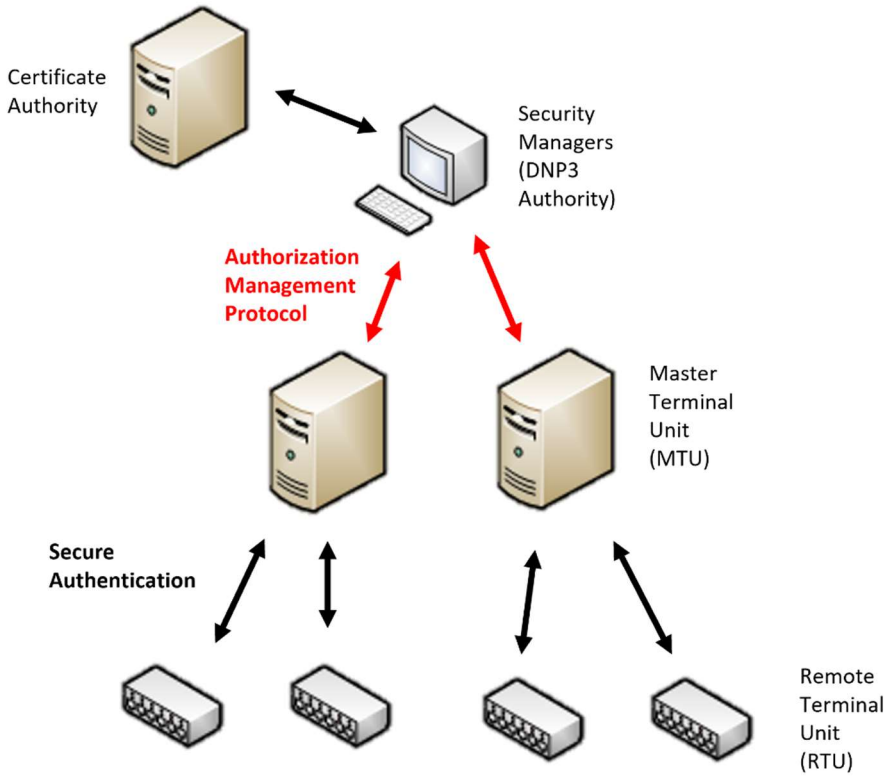

Figure 7.7 – DNP3 SAv6 and AMP Interaction on Network

7.4 Compatible Lightweight Protocols

Mentioned in the previous chapters, a solution to the limited computational hardware that legacy systems have access to makes them vulnerable to new attacks that are being deployed, so having a strong cryptographic protocol is essential for the success of the SCADA systems however, having a strong protocol doesn't necessarily mean to rely on heavily computational protocols; new protocols are being released, which are both strong and lightweight, to avoid overhead. The following protocols are BLAKE2, SHA-3 and elliptic curve.

7.4.1 BLAKE2

BLAKE2 is an authentication protocol that utilizes a hashing function to hide the true value of the message that is going to be utilized. To emphasize, as mentioned in previous chapters, each protocol that uses hashing they utilize their own hashing function, respectively, for authentication purposes for when the information is trying to be accessed by a legitimate device or user. [8] Now, for BLAKE2, there is a total of 2 variations to this protocol. The first is BLAKE2b and this protocol is geared towards machines that can operate with 64-bit processors and for the hashing process it has a total of 12 rounds. The second protocol is BLAKE2s, and this protocol is geared towards lower-end processors from 8 to 32-bits with a hashing process of 10 rounds. Now, the BLAKE2 protocol's mechanism works by two main parts. First, the generate block is the one in charge of adding the pads to the message, and, depending on how big the message is, it notifies the second part of the protocol, the digest block, and lets it know how many message words will go through the function. The digest block is responsible for adding the hashing part of the algorithm to the message word that both blocks are working on. In brief, the difference between the two versions of the protocol is in the word size, for BLAKE2b it's a word size of 64 bits and for BLAKE2s it's a word size of 32 bits. Now, as shown in figure 7.2, BLAKE2 is being compared to other renowned hashing algorithms such as the different kinds of secure hashing algorithms (SHA) and the MD5, and in this comparison BLAKE2b has a higher throughout to most of the algorithms, except for SHA-1, where they were very close in the score. Moreover, BLAKE2s, even though it is topped at 32-bits and why it stayed behind, it still placed third highest compared to the rest of the algorithms.

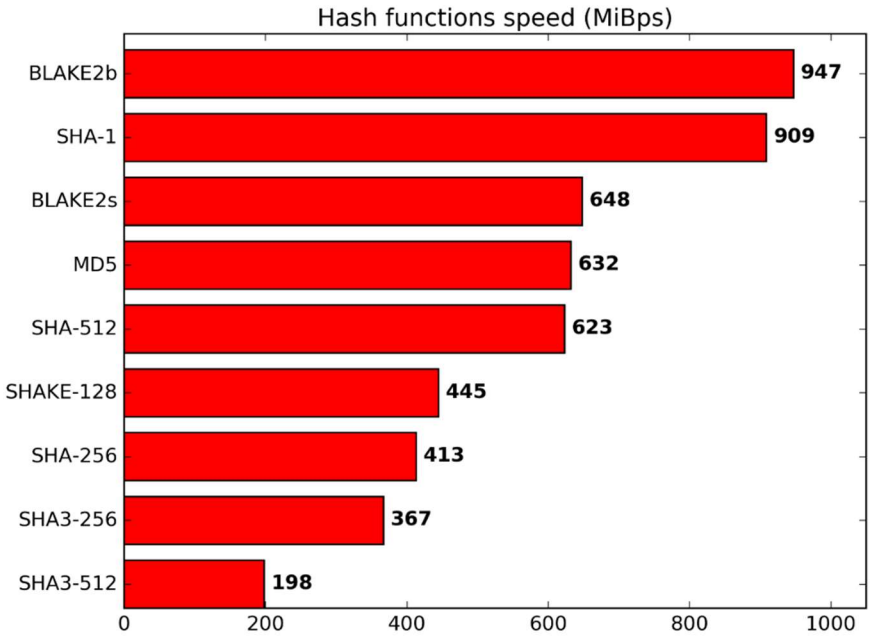

Figure 7.8 – Comparison Among Hashing Protocols [8]

7.4.2 SHA-3

Another protocol that is supported by the secure authentication version 6 is SHA-3, and just like BLAKE2, this algorithm also implements hashing to a message and transforms it to a hashing value. There are a total four different types of SHA-3 hashing algorithms because they depend on the output length, which is 224, 256, 384 and 512, and they also vary with the rate and the capacity that they can hold to calculate with the hash value. [9] Now, the first step of the mechanism in this protocol is the padding portion, and this process is when bits are appended to a portion of the message. Moreover, this step is important because if the padding part wasn't implemented, then when the size of the message goes into the hashing function, then the message size wouldn't compliment the hash length needed to compute the hash function. So, after padding the message that is going to be hashed the second step is the state size, which is the sum of the rate and the capacity based on the chosen SHA-3 size. For the third portion of the algorithm, the absorb function is utilized by taking in the output from the state size and performing a set of 5 different functions to obtain the hash value. Finally, the squeeze function is the last step of the process where the final hash value is extracted. Furthermore, both the rate and the capacity are segregated from each other and depending on the size of the output length that was selected based on the SHA-3

that was utilized to acquire the hash value, then this will be the final output of the hashing algorithm. Compared to BLAKE2, SHA-3 performs less efficiently compared to the other hashing algorithm but depending on the situation of the available computational hardware on the devices, then utilizing SHA-3 can be more beneficial to the success of hashing the messages being transmitted.

7.4.3 Elliptic Curve Cryptography

Compared to the mentioned protocols, the last protocol that is now compatible for use with secure authentication is the elliptic curve cryptography (ECC). This is a lightweight asymmetric cryptographic protocol, and its function is based for encryption. What makes ECC a strong protocol to be implemented is its feature to utilize small size key size while still providing high security for the host device. [10] Now, to emphasize, asymmetric cryptography is when a host device generates two keys, one private key for itself and a second public key that can be utilized by another authorized device – which the certificate authority provides the digital certificate for authorization of devices – to communicate with the host device. In elliptic curve cryptography, the elliptic curve digital signature algorithm (ECDSA) uses small key sizes to generate the digital certificates and, ultimately, authorizes the devices to communicate.

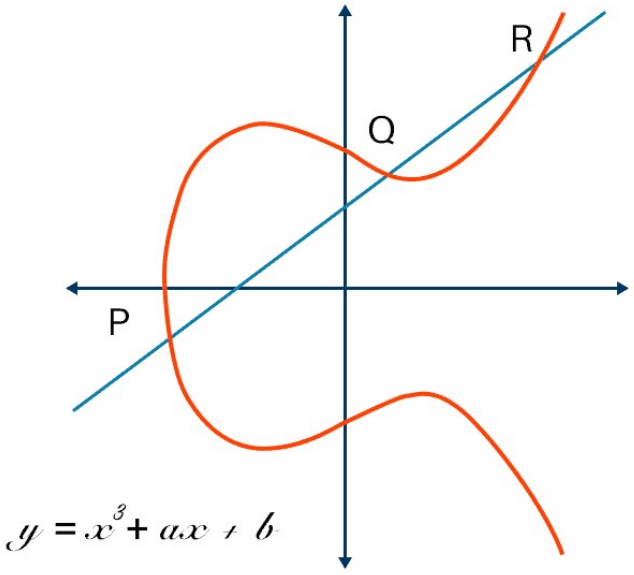

Figure 7.9 – Elliptic Curve Cryptography Formula and Graph [10]

Now, as shown in table 7.1, a comparison is shown between the key sizes of Rivest-Shamir-Adleman (RSA) and ECC algorithms are shown, starting from the smallest key size that is available to the algorithm, to big size keys, and the bigger the key size the more security is implemented into the process of encryption for the message. [10] Moreover, what makes ECC more pleasant to work with when implemented into devices is its capability of utilizing small keys. So, when computing the encryption of a message at the host device with the private key, it's not demanding on its resources to encrypt it, and with a small ciphertext output, it also increases the throughput of the devices because a small message requires less throughput compared to a big message. In addition, for RSA, since it is utilizing a bigger key the process of encryption takes longer and the output is bigger in size. In brief, some differences between symmetric and asymmetric cryptography are how secure is the method and how computationally intensive the method is on the device; for symmetric it is less computationally intensive but provides less security compared to asymmetric, and even though asymmetric provides higher security, it has a higher possibility of creating overhead on the device. As a result, symmetric cryptography is preferred when devices don't have the capability of handling asymmetric, but now with the introduction of ECC, with it being less overwhelming on devices and still providing a strong security, this is a viable option for implementation on capable devices.

Table 7.1 – RSA and ECC Key Size Comparison [10]

Rivest-Shamir-Adleman (RSA) Key Size	Elliptic Curve Cryptography (ECC) Key Size
1024 bits	160 bits
2048 bits	224 bits
3072 bits	256 bits
7680 bits	384 bits
15360 bits	521 bits

7.5 Key Change and Application

For the 6th version of secure authentication, there are two processes that are followed for the distribution of the keys among the devices that are communicating. The first is association establishment, which is responsible for the distribution of the update keys and the second is the

session key initialization to update the session keys for the communication among both devices that are going to communicate.

7.5.1 Association Establishment

Before a communication can begin between a master station and outstation, first they both must generate their update keys, respectively, because they will be utilized for the session key initialization. The protocols that are utilized for this process are the Elliptic Curve Diffie-Hellman (ECDH), and the HMAC-based Key Derivation (HKDF) algorithms. [12] Now, as shown in figure 7.4, the master station is requesting to associate or communicate with the outstation, and this process includes the exchange of their own certificates to demonstrate that both devices are authorized to communicate. After receiving the response, the master station sends a message to the outstation to change the update keys, and the master station first generates its own encryption update key and authentication update key, and the request sent to the outstation includes a message authentication code that was generated using the authentication update key. Afterwards, the outstation receives the message, and it generates both of the update keys as well, then the outstation authenticates the received message utilizing its authentication update key. Finally, after verifying the received message, this is when the outstation replies to the master station with a response, and not an authentication error, then the master station also verifies the response from the outstation with its authentication update key to finalize the association between the devices and begin the communication.

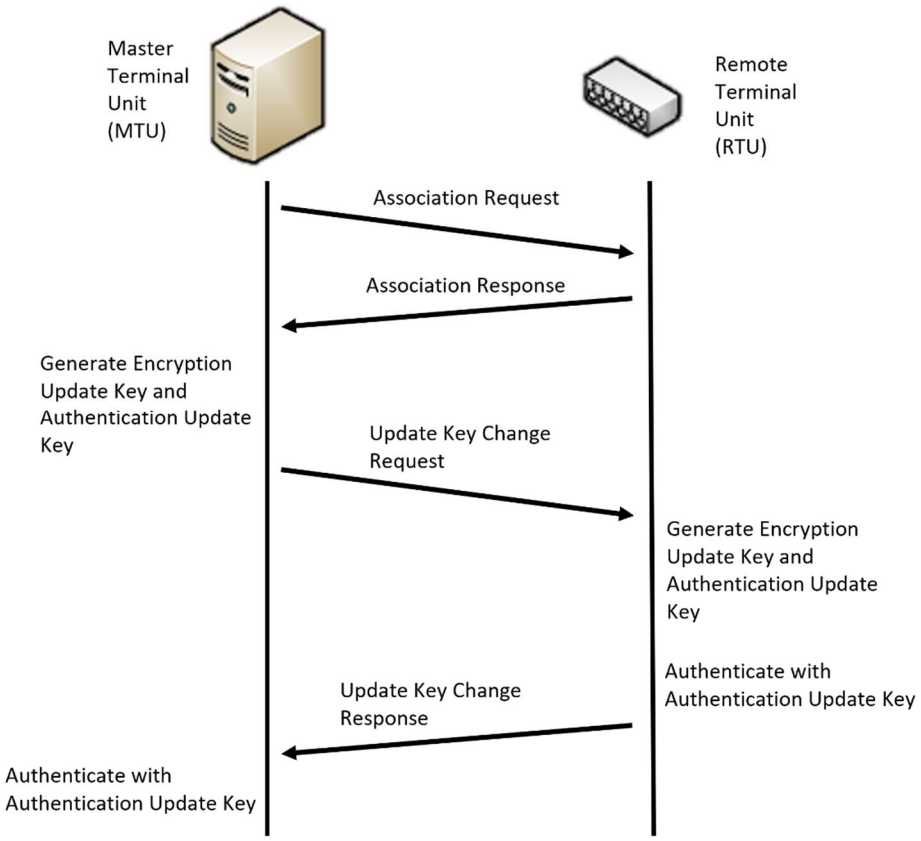

Figure 7.10 – Association Establishment for DNP3 SAv6

7.5.2 Session Key Initialization

After the association has been established between the two devices that are going to communicate, the next step is to initialize the session keys to commence the communication. [12] As shown in figure 7.5, the master station first sends a request to the outstation to begin a session and the outstation replies to the master station to begin the session. Next, the master station sends a request to change the session keys of the outstation, and within this message the new session keys are sent to the outstation encrypted utilizing the encryption update key and, furthermore, a MAC is generated using the authentication update key and send along with the message. Now, at the outstation, when it receives the message, the first step is to verify the MAC that was sent with its authentication update key. After the MAC has been verified, then the session keys are decrypted utilizing its encryption update key and the outstation can begin using its session key. Next, the

outstation sends a response to the master station with a MAC for the master station to verify it and then it can start using the session key.

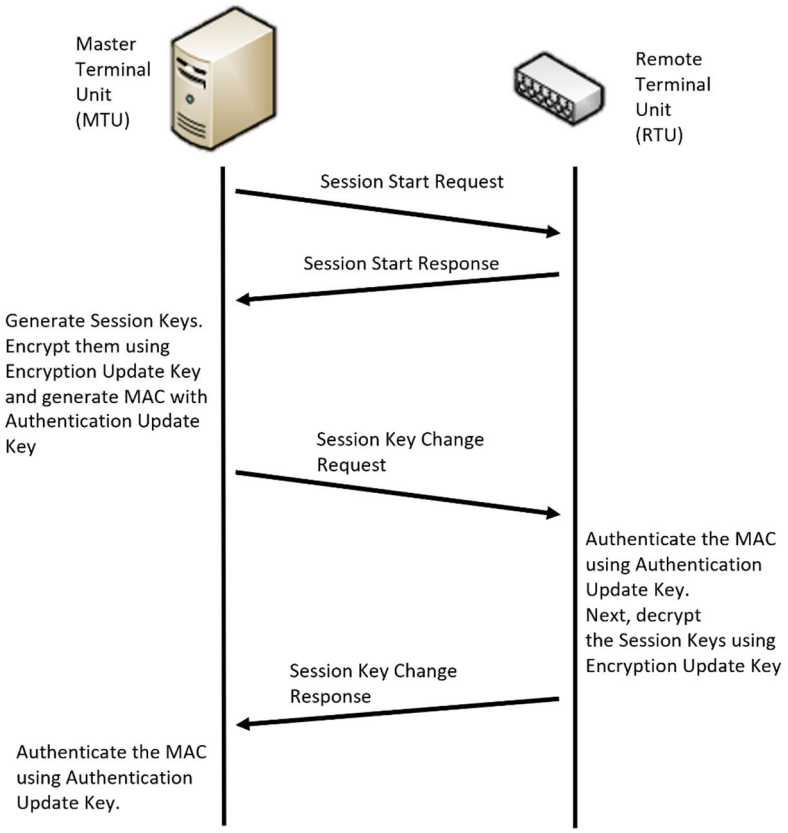

Figure 7.11 – Session Key Initialization for DNP3 SAv6

7.6 Security Mechanism Comparison Between SAv5 and SAv6

In the duration of the DNP3 protocol, ever since its release date, there has been a total of 6 versions of the protocol. Comparing DNP3 secure authentication version 6 to the 5th version of the protocol, from chapter 6, one of the main changes is that DNP3 secure authentication is its own layer now for the protocol, and the integration of the authorization management protocol. Due to these integrations, the challenge and reply mechanism from the 5th version was removed because with the AMP, devices are now provided with certificates for authenticity, so they are able to initialize a communication with a device within the system. Moreover, with the addition of security managers, any infiltrated adversaries can quickly be removed by taking away any privileges that

might have been provided unintendedly and, as a result, mitigating any potential attacks to the system. Furthermore, it now has the capability of encrypting important information by utilizing the AEAD-AES-256-GCM protocol to keep it confidential and for only authorized devices to see the contents of the information. For the 6th version, now it is capable of implementing lightweight protocols such as BLAKE2, SHA-3, and the different algorithms for ECC which, ultimately, provide strong security for the system and avoids overhead on the devices instead of using symmetric algorithms or, for example, the RSA asymmetric algorithm.

CHAPTER 8: CONCLUSIONS

When SCADA systems were first introduced into the critical infrastructures, such as the power grids, as the demand for the services kept growing, so was asked of the infrastructure to keep providing for the public. As a result, manpower was replaced by automation and the introduction to the internet made the SCADA systems a valuable asset when monitoring and collecting the data that was being generated from the field devices that are part of the system, and decisions could be made on the spot on how to continue operating and any changes that must be managed. However, with the integration of the internet to the system, it introduced vulnerabilities that could be exploited and, ultimately, cause harm to the critical infrastructures and the safety of the public. This incited developers to create secure communication protocols that devices would utilize to operate and, at the same time, keep all the information that was being transmitted safe. Furthermore, this topic falls under the security objectives that must be met to ensure the safe communication, and these are availability, authorization, integrity, replay protection, and non-reputability. Now, the main cyber-attacks that target SCADA systems, specifically, are eavesdropping, denial-of-service, spoofing, man-in-the-middle and replay attacks. Cyber-attacks can be either passive attacks, where the adversary isn't tampering a device or making any changes to the communication that is currently happening however, the adversary is intently listening to the communication that is present. The second category of attack is the active attacks, where the adversary is now hindering the communication by attempting to either replay a message, change the integrity of a message, overwhelm the system with irrelevant messages, or by the adversary sending authorized messages to the devices.

Now, with the SCADA systems being vulnerable, as mentioned, it is important to implement it with strong security protocols to avoid or mitigate the cyber-attacks from adversaries. Some protocols that are compliant and utilize ethernet as a method of communication are the IEC 60870, IEC 61850, Modbus and DNP3. For this thesis, the protocol that was researched was DNP3 because of its security capabilities that can greatly benefit the success of the SCADA systems. Even though there are multiple complications with legacy devices, such as not being able to utilize newer protocols due to low computational capabilities and having complex systems, or not being able to scale due to the problems with public key infrastructure implementation. As a result, this

is when versions for DNP3 secure authentication began to be released to solve these problems. First, the 5th version of secure authentication addressed the mentioned cyber-attacks by implementing the authentication of the devices that are operating within the system. The secure authentication version 5 implemented authentication by the mechanism of challenge and response. When a master station and an outstation are communicating, the master station sends a request with a critical ASDU to the outstation and typically the outstation would challenge this message, then the master station would reply with an authentication message and after the verification, the outstation would process the request. This mechanism does, indeed, work for authenticating the devices however, the challenge and reply isn't the most efficient way of approaching the problem of authentication because in this way, the devices are wasting throughput by an ongoing message. In addition, keys are utilized for this communication, and the pre-sharing of the keys in version 5 introduced uncertainty because an employee is responsible for the distribution of these keys. Now, keys being long string values, employees would try to remember but forget, or they would write it down or share it across email where the key can be lost or stolen.

On the other hand, when the DNP3 secure version 6 was introduced, the mechanism was changed where now authorization was handled by the AMP protocol, and privileges could be granted or taken away in a matter of minutes or less. So, all the devices that are part of the critical infrastructure can communicate to the devices that they are linked to since they were provided with a digital certificate by the security managers. This saves throughput to all the devices because now they don't have to worry whether the device that is trying to communicate with them is legit or not. Other process which requires several messages being exchanged are still utilized, such as association establishment and session key initialization, but with AMP being implemented, all the messages that are being transmitted are secure. In brief, the implementation of the 6th version of DNP3 is beneficial to the operation within SCADA systems because it provides primarily authentication between all of the devices, so eavesdropping, spoofing, denial-of-service, replay-attacks and man-in-the-middle attacks are addressed, and with this protocol version now capable of encrypting important information being transmitted among the devices by using AEAD-AES-256-GCM, in the case that there is an adversary eavesdropping, no important information would be misplaced.

8.1 Future Work

Based on the analysis that was presented on this thesis, for future implementations the DNP3 protocol shall be analyzed in further detail when implementing the 6th version of the secure authentication protocol under different topologies. Now, as shown in chapter 7, a future implementation would entail the implementation of a larger system with multiple master stations and multiple outstations connected within the same network. Moreover, with the implementation of the secure authentication protocol, by using AMP, test that all the devices within the network have been verified and, in addition, make a test scenario to model resiliency where adversaries are trying to infiltrate the network under different attacks. As a result, the AMP should be capable of detecting when a device is not authorized and, therefore, be removed from the network. So, testing the different cases where AMP is being utilized to verify that the protocol does indeed ensure safe communication among all the devices within the network, or identify gaps that prevent such operation. In future implementations wide range of simulated cyber-attacks at different variations and scales can be used to test the performance of the system and analyze how well the implementation can handle and mitigate the attacks on the system. The testing should focus on enhancing resilience in the system. In some cases, attacks are strong and strategic, so being able to contain the attack and not let it expand would be the overall goal to achieve an optimal system.

REFERENCES

[1] D. Pliatsios, P. Sarigiannidis, T. Lagkas and A. G. Sarigiannidis, "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1942-1976, thirdquarter 2020, doi: 10.1109/COMST.2020.2987688.

[2] W. Wenye, and Z. Lu. “Cyber Security in the Smart Grid: Survey and Challenges.” Computer Networks, vol. 57, no. 5, Apr. 2013, pp. 1344–1371, 10.1016/j.comnet.2012.12.017.

[3] I. N. Fovino, A. Carcano, T. De Lacheze Murel, A. Trombetta and M. Masera, "Modbus/DNP3 State-Based Intrusion Detection System," 2010 24th IEEE International Conference on Advanced Information Networking and Applications, 2010, pp. 729-736, doi: 10.1109/AINA.2010.86.

[4] C. Cremers, M. Dehnel-Wild, and K. Milner, “Secure Authentication in the Grid: A Formal Analysis of DNP3 SAv5.” Journal of Computer Security, vol. 27, no. 2, 29 Mar. 2019, pp. 203–232, 10.3233/jcs-181139.

[5] C. Gordon R., and R. Deon. “Preview of DNP3.” Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems, London, Elsevier; Oxford, 2008, pp. 66–72.

[6] C. Gordon R., and R. Deon. “Fundamentals of Distributed Network Protocol.” Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems, London, Elsevier; Oxford, 2008, pp. 73–128.

[7] "IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)," in IEEE Std 1815-2012 (Revision of IEEE Std 1815-2010) , vol., no., pp.1-821, 10 Oct. 2012, doi: 10.1109/IEEESTD.2012.6327578.

[8] J.-P. Aumasson, “Fast Secure Hashing.” *BLAKE2*, 29 Jan. 2013, https://www.blake2.net/.

[9] A. Anand, “Breaking down: Sha-3 Algorithm.” Medium, InfoSec Write-Ups, 13 Jan. 2020, https://infosecwriteups.com/breaking-down-sha-3-algorithm-70fe25e125b6.

[10] “What Is Elliptic Curve Cryptography? Definition & Faqs.” Avi Networks, 15 Apr. 2022, https://avinetworks.com/glossary/elliptic-curve-cryptography/#:~:text=An%20elliptic%20curve%20for%20current,curve%20will%20stay%20the%20same.

[11] H. Self, “Overview of DNP3 Security Version 6.” *DNP.ORG*, DNP, 24 Jan. 2020, https://www.dnp.org/Resources/Public-Documents.

[12] R. Farquharson, “DNP-UG Update Webinar - November 2020 - Slides.” *DNP.ORG*, DNP, 18 Nov. 2020, https://www.dnp.org/Resources/Public-Documents.

[13] R. Farquharson, “NEW - Two Page Summary - Next Gen DNP Security.” *DNP.ORG*, DNP, 25 Feb. 2022, https://www.dnp.org/Resources/Public-Documents.

VITA

Isaac Monroy was born in El Paso, Texas and during his early childhood, he studied at Mexico until he finished elementary school. Afterwards, Isaac transitioned to a public school in El Paso, “Harmony Science Academy.” Isaac finished middle school and high school and upon graduation he began his college career enrolled in an Electrical Engineering degree program at the University of Texas at El Paso. During the years he spent studying, he was also part of extracurricular activities, such as being member of the Society of Hispanic Professional Engineers (SHPE), Eta Kappa Nu Zeta Delta Chapter (HKN), and the Institute of Electrical and Electronics Engineers (IEEE). In addition, Isaac held several esteemed positions within IEEE, including being president of the IEEE UTEP Chapter.

In Spring 2021, he graduated and obtained a Bachelor of Science in Electrical Engineering. Isaac was eligible and enrolled in the Fast Track Program offered by UTEP for students who achieve a high GPA during their bachelor’s degree. On Fall 2020, with the semester already started, Isaac transitioned into Dr. Sai Mounika Errapotu’s class of introduction to cybersecurity. Along with the class, Isaac was also enrolled in Dr. Errapotu’s computer architecture, and this is where Isaac’s interest grew in topics regarding cyber security. Eventually in Spring 2021, Dr. Errapotu became Isaac’s mentor and direct supervisor over his thesis where he studied about security analysis and protocol implementation for SCADA systems.

Isaac has participated in a summer project sponsored by Google and has done an internship with a local El Paso company, Bessel, where he was an engineer intern during the summer of 2022. Upon graduation in January 2023, Isaac plans on going to SpaceX as a Software Automation Engineer intern.

Contact email: monroy.isaac.99@gmail.com