**2.2 MODBUS AND CYBERATTACKS**

**2.2.1** **Modbus TCP Protocol: An Overview**

To demonstrate the efficiency of the test bed in carrying out cyber-attacks on a power system protocol, the Modbus/TCP protocol was employed as the reference protocol. Modbus/TCP was chosen for the following reasons:

* In power systems, Modbus is extensively used.
* Modbus/TCP is easy to use and set up.
* Modbus protocol libraries for smart grid applications are freely accessible for utilities to leverage.

Modbus TCP is a master-slave communication protocol that works on the application layer of the TCP IP architecture. The slave station and the master station can communicate in a one-to-one or many-to-many manner. The Modbus TCP Application Data Unit (ADU) is made up of a 7-byte protocol header and an N-byte protocol data unit (PDU).

Modbus is a serial communications protocol created by Modicon in 1979 for use with its programmable logic controllers (PLCs) used in factory production, traffic lights, elevators, conveyor belts, substation automation, and other applications. Modbus is still one of the most widely used protocols for field device communication, notwithstanding its antiquity.

As a result, it's no surprise that attackers would try to manipulate an ICS environment via this protocol. Modbus has serial (Modbus RTU and Modbus ASCII) and Ethernet (Modbus TCP) versions. Ethernet has become the de facto standard for both corporate enterprise systems and factory networking (Modbus, 2017). The Ethernet header, IP header, TCP header, Modbus TCP, and data are all part of the Modbus TCP protocol. These headers are shown in Figure 1.

Table

Description automatically generated

**Figure 2.3: Modbus TCP Headers**

Ethernet allows the TCP/IP wrapper to introduce the Modbus TCP protocol,

historically done via serial lines, to unwrap the layers until it reaches the Modbus TCP

header. The Modbus TCP header and its data include the Modbus Application Header

(MBAP) and the Protocol Data Unit (PDU) as seen in Figure 2.



**Figure 2.4: the Modbus Application Header (MBAP) and the Protocol Data Unit (PDU)**

**2.2.2** **Man-in-the-middle attack**

A man-in-the-middle (MITM) attack is a type of cyberattack where attackers intercept an existing conversation or data transfer, either by eavesdropping or by pretending to be a legitimate participant. To the victim, it will appear as though a standard exchange of information is underway — but by inserting themselves into the “middle” of the conversation or data transfer, the attacker can quietly hijack information.

It is often used to steal login credentials or personal information, spy on victims, sabotage communications, or corrupt data. MITM attacks are one of the oldest forms of cyberattack. Computer scientists have been looking at ways to prevent threat actors tampering or eavesdropping on communications since the early 1980s. Because MITM attacks are carried out in real time, they often go undetected until it’s too late.

Diagram

Description automatically generated with medium confidence

**Figure 2.5: Conceptual diagram of a typical Man-in-the-middle attack**

**2.2.3** **Types of Man-in-the-middle attack**

*Active session attack:*

During an active session attack, the attacker stops the original client from communicating with the server and then replaces himself within the session. From this point onwards, the attacker will be communicating with the server, and they will be able to do anything that a normal user can do. He could tamper the data or collect sensitive information that may have a potential impact later.

*Passive session attack:*

In a passive session attack, the attacker monitors the data flowing across the network without interrupting the actual communication. The intruder eavesdrops the communication but does not modify the message stream in any way. He could collect all the data passing through the network which may cause an active attack later.

*ARP Poisoning:*

It is a technique by which an attacker sends spoofed Address Resolution Protocol (ARP) messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

The basic anatomy behind an ARP poisoning attack is to exploit the lack of authentication in the ARP protocol by sending spoofed ARP messages onto the network. ARP poisoning attacks can be run from a compromised host on the LAN, or from an attacker's machine that is connected directly to the target LAN.

An attacker using ARP poisoning will disguise as a host to the transmission of data on the network between the users. Then users would not know that the attacker is not the real host on the network.

Generally, the goal of the attack is to associate the attacker's host MAC address with the IP address of a target host, so that any traffic meant for the target host will be sent to the attacker's host. The attacker may choose to inspect the packets (spying), while forwarding the traffic to the actual default destination to avoid discovery, modify the data before forwarding it (man-in-the-middle attack), or launch a denial-of-service attack by causing some or all the packets on the network to be dropped.