MOD Bus

S. Venkatesan

Acknowledgement: The contents, example scripts and some figures are copied from various sources.
Thanks to all authors and sources made those contents public and usable for educational purpose

Introduction

- It is a communication Protocol.
- Introduced in 1979.
- Originally implemented as an application-level protocol intended to transfer data over a serial layer.
- Modbus has expanded to include implementations over serial, TCP/IP, and the user datagram protocol (UDP).
- Each device communicating (i.e., transferring data) on a Modbus is given a unique address
- Modbus is a request-response protocol implemented using a master-slave relationship.

Master-Slave

- In a master-slave relationship, communication always occurs in pairs—one device must initiate a request and then wait for a response—and the initiating device (the master) is responsible for initiating every interaction.

- Master
  - is a human machine interface (HMI) or Supervisory Control and Data Acquisition (SCADA) system.
- Slave
  - is a sensor, programmable logic controller (PLC), or programmable automation controller (PAC).

Data Format

- Protocol Data Unit (function code and data) - cannot exceed 253 bytes.
- The Modbus protocol uses 2 types of data:
  - Single bit
  - Register (16 bits)
- In Modbus RTU, Modbus ASCII, and Modbus Plus (which are all RS-485 single-cable multi-drop networks), only the node assigned as the 'client' may initiate a command.
- All other devices are 'servers' and respond to requests and commands.

Data banks or Address Ranges

Memory Block	Data Type	Master Access	Slave Access
Coils	Boolean	Read/Write	Read/Write
Discrete Inputs	Boolean	Read-only	Read/Write
Holding Registers	Unsigned Word	Read/Write	Read/Write
Input Registers	Unsigned Word	Read-only	Read/Write

Data Block	**Prefix**
Coils	0
Discrete Inputs	1
Input Registers	3
Holding Registers	4

Instructions

- Change the value in one of its registers, by write to Coil or Holding register
- Send back one or more contained values, by read from Coil or Holding register
- Read a physical input port, by read from Discrete Input or Input register

RS-485 vs Ethernet

- The major drawback of RS-485 is its limited communication speed which is maxed out at 10 Mbaud.
- RS-485 is designed for a master/slave topology.
  - In this system, the master polls each slave waits for the response, and then polls the next slave.
  - This allows a deterministic behavior by avoiding collisions of data packets.
- Ethernet however has no built-in methods to avoid data packet collisions.
- In applications like process control or robot control, for us, deterministic behavior is mandatory while the speed of communication is usually more than high enough.
- Communicating at lower speeds also has the advantage of being more resilient to the noise present in industrial environments.

MODBUS Master/Slaves protocol principle

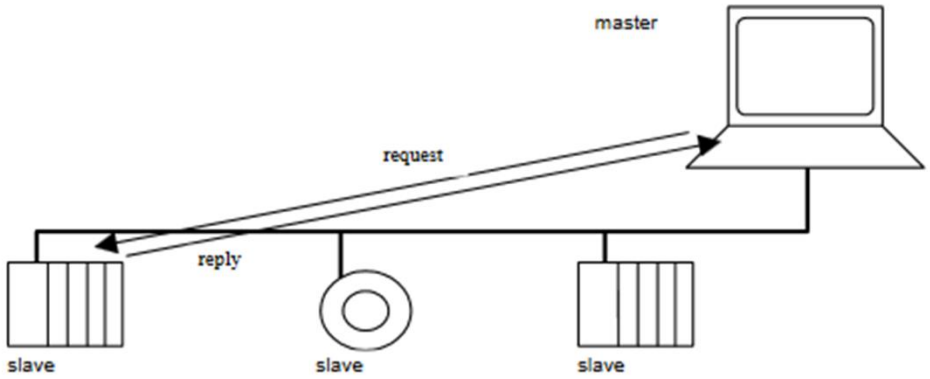


Figure 3: Unicast mode

The address 0 is reserved to identify a broadcast exchange.

From 1 to 247 – Slaves individual address

From 248 to 255 - Reserved

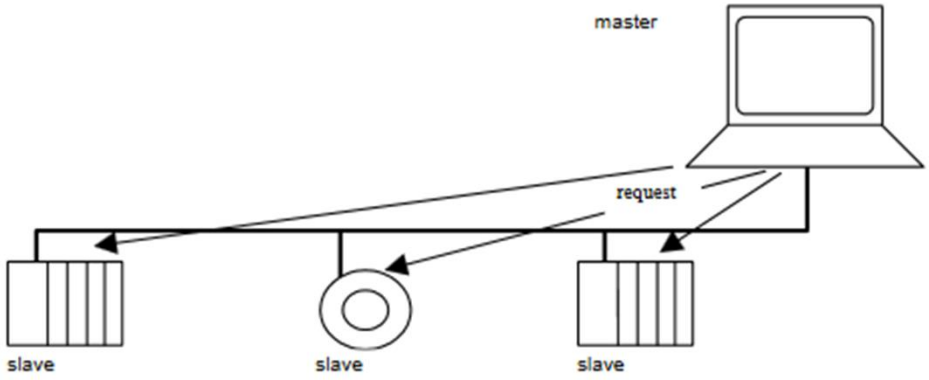


Figure 4: Broadcast mode

Source - https://www.modbus.org/docs/Modbus_over_serial_line_V1_02.pdf

Protocol Versions

- *Modbus RTU* (Remote Terminal Unit)
  - used in serial communication, and is the most common implementation available for Modbus.
  - Modbus RTU makes use of a compact, binary representation of the data for protocol communication.
  - follows the commands/data with a cyclic redundancy check checksum as an error check mechanism to ensure the reliability of data.
  - Message must be transmitted continuously without inter-character hesitations. Modbus messages are framed (separated) by idle (silent) periods.

- *Modbus ASCII*
  - used in serial communication and makes use of ASCII characters for protocol communication.
  - The ASCII format uses a longitudinal redundancy check checksum.
  - Modbus ASCII messages are framed by a leading colon (":") and trailing newline (CR/LF).

- *Modbus TCP/IP* or *Modbus TCP*
  - a Modbus variant used for communications over TCP/IP networks, connecting over port 502.
  - It does not require a checksum calculation, as lower layers already provide checksum protection.

- *Modbus over TCP/IP*, *Modbus over TCP*, or *Modbus RTU/IP*
  - a variant that differs from Modbus TCP in that a checksum is included in the payload, as with Modbus RTU.

Protocol Versions

- *Modbus over UDP*
  - Using Modbus over UDP on IP networks, which removes the overhead of TCP.

- *Modbus Plus* (*Modbus+*, *MB+*, or *MBP*)
  - Modbus Plus is proprietary to Schneider Electric and unlike the other variants, it supports peer-to-peer communications between multiple clients.
  - It requires a dedicated co-processor to handle fast HDLC-like token rotation. It is a high speed peer to peer network protocol based on token passing communication.
  - It uses twisted pair at 1 Mbit/s and includes transformer isolation at each node, which makes it transition/edge-triggered instead of voltage/level-triggered.
  - Special hardware is required to connect Modbus Plus to a computer, typically a card made for the ISA, PCI, or PCMCIA bus.

- *Pemex Modbus*
  - An extension of standard Modbus with support for historical and flow data.
  - It was designed for the Pemex oil and gas company for use in process control and never gained widespread adoption.

- *Enron Modbus*
  - another extension of standard Modbus developed by Enron with support for 32-bit integer and floating-point variables, and historical and flow data.
  - Data types are mapped using standard addresses.
  - The historical data serves to meet an American Petroleum Institute (API) industry standard for how data should be stored

Transmission Mode - Serial

- RTU Transmission Mode
- ASCII - The byte 0X5B is encoded as two characters : 0x35 and 0x42 (0x35 ="5", and 0x42 ="B" in ASCII).

Frame Formats

- Application Data Unit : ADU = Address + PDU + Error check.

- Protocol Data Unit: PDU = Function code (1 Byte) + Data.

MOD Bus RTU

Name	Length (bits)	Function
Start	3.5 x 8	At least 3½ character times (28 bits) of silence (mark condition)
Address	8	Station address
Function	8	Indicates the function code e.g. "read coils"
Data	*n* × 8	Data + length will be filled depending on the message type
CRC	16	Cyclic redundancy check
End	3.5 x 8	At least 3½ character times (28 bits) of silence (mark condition) between frames

MOD Bus TCP/IP

Name	Length (bytes)	Function
Transaction identifier	2	For synchronization between messages of server and client
Protocol identifier	2	0 for Modbus/TCP
Length field	2	Number of remaining bytes in this frame
Unit identifier	1	Server address (255 if not used)
Function code	1	Function codes as in other variants
Data bytes	*n*	Data as response or commands

Frames

Field	Definition	Size	Description
1	Slave number	1 byte	Destination of the request o0: broadcasting (all slaves concerned) o1–247: unique destination
2	Function codes	1 byte or 2 bytes	Based on the data bank
3	Data	n registers	Request or reply data NOTE: Number of registers n is limited to 52 with MasterPact MicroLogic E trip unit.
4	Check	2 bytes	CRC16 (to check transmission errors)

Function codes are defined.

Master-Slave Principle

- Only 1 master is connected to the network at a time.
- Only the master can initiate communication and send requests to the slaves.
- The master can address each slave individually using its specific address or all slaves simultaneously using address 0.
- The slaves can only send replies to the master.
- The slaves cannot initiate communication, either to the master or to other slaves.

Security

- Blending of Transport Layer Security (TLS) with the traditional Modbus protocol.
- TLS was selected as it is a well-known, widely accepted internet standard. TLS will encapsulate Modbus packets to provide both authentication and message-integrity protection.
- The new protocol leverages X.509v3 digital certificates for authentication of the Server and Client
- The protocol also supports the transmission of role-based access control information using an X.509v3 extension to authorize the request of the Client.
- Modbus Security will use a new port; traditional Modbus uses port 502.
- The new Modbus Security protocol will utilize port 802

MOD Bus - Serial

- RS-232 and RS-485.
- Modbus RS-232 Allows Concurrent, Full-Duplex Flow of Data.
- Modbus RS-485 Is Half-Duplex and Indicates Values Using Differences in Voltage.
- Modbus using the RS-485 protocol is more common than RS-232 due to its support for multi-drop communication.

MOD Bus VS CAN Bus

Parameter	MOD Bus	CAN Bus
Hierarchy	Master Slave	Multi-Master no Slave
TCP/IP	Possible	Not Possible
Device	Dedicated master device required	Not required
Network Size	Large	Small
Data Frame Format	Register-based Data Frame	Message-based Data Frame
Transmission Rate	Low Speed (up to 115.2 Kbps)	High Speed (up to 1 Mbps)
Event Reporting	No	Yes

Security Issues

- **Lack of Authentication:** Modbus often lacks strong authentication mechanisms, allowing unauthorized access to devices and systems. This can lead to unauthorized control or manipulation of critical infrastructure.

- **Lack of Encryption:** Modbus typically lacks encryption, meaning that data transmitted over the network is vulnerable to eavesdropping and interception. Attackers can gain access to sensitive information and potentially manipulate or disrupt the control system.

- **Default Configurations:** Many Modbus devices are shipped with default configurations and default passwords that are well-known and easily exploitable. Failure to change these defaults increases the risk of unauthorized access.

- **Lack of Authorization:** Modbus devices often lack granular authorization mechanisms, making it difficult to control and restrict access to specific functions or data points. This can result in unauthorized manipulation or disruption of critical processes.

- **Vulnerable Firmware**: Modbus devices may run outdated or vulnerable firmware versions, exposing them to known security vulnerabilities. Without regular firmware updates and security patches, these devices remain at risk.

Security Issues

- **Lack of Logging and Monitoring:** Modbus devices may not provide sufficient logging and monitoring capabilities. This makes it difficult to detect and respond to suspicious activities, such as unauthorized access attempts or unusual data patterns.

- **Denial of Service (DoS) Attacks:** Modbus implementations can be vulnerable to DoS attacks, where an attacker floods the target device or network with excessive requests, rendering it unresponsive and disrupting critical operations.

- **Man-in-the-Middle Attacks:** In the absence of encryption or weak authentication, Modbus communications can be intercepted by attackers who position themselves between the communicating devices. This allows them to manipulate or eavesdrop on the data flow.

- **Protocol Vulnerabilities:** Modbus may have inherent vulnerabilities in its design and implementation, such as buffer overflows or input validation issues. Exploiting these vulnerabilities can lead to remote code execution or system crashes.

Security Issues

- **Command Injection:** Modbus devices may be vulnerable to command injection attacks. If input validation is not properly implemented, an attacker can inject malicious commands into the device, leading to unauthorized control or manipulation of the system.

- **Replay Attacks:** Modbus communications may lack mechanisms to prevent replay attacks. Attackers can capture and replay legitimate network traffic to perform unauthorized actions, impersonate valid users, or disrupt system operations.

- **Insecure Remote Access:** Modbus devices often provide remote access capabilities without adequate security measures. Weak or unsecured remote access mechanisms can be exploited by attackers to gain unauthorized access to the devices or network.

- **Lack of Integrity Checks:** Modbus lacks built-in integrity checks for data integrity verification. Without proper checksums or cryptographic measures, attackers can modify data during transmission, leading to data corruption or manipulation.

- **Insider Threats:** Insider threats pose a significant risk in Modbus environments. Unauthorized or disgruntled employees with access to the system can misuse their privileges to sabotage operations, steal sensitive data, or cause disruptions.

Security Issues

- **Physical Security:** Modbus devices are often deployed in areas that susceptible to physical security breaches. Unauthorized physical access to devices can allow attackers to tamper with the equipment, extract sensitive information, or disrupt operations.

- **Lack of Security Awareness:** Insufficient security awareness among system administrators, operators, and employees can lead to inadvertent security breaches. Lack of knowledge about security best practices, such as password hygiene or social engineering, can result in successful attacks.

- **Vendor-specific Vulnerabilities:** Modbus devices from different vendors may have their own unique vulnerabilities. These vulnerabilities can stem from implementation flaws, insecure default settings, or inadequate testing and quality assurance processes.

- **Lack of Network Segregation:** Inadequate network segregation between Modbus devices and other network segments can increase the attack surface. A compromised device or network segment can potentially impact other critical systems or expose them to additional vulnerabilities.

- **Supply Chain Attacks:** Modbus devices may be susceptible to supply chain attacks, where attackers compromise the devices or their firmware during manufacturing, distribution, or software updates. This can introduce backdoors or other malicious functionalities into the devices.

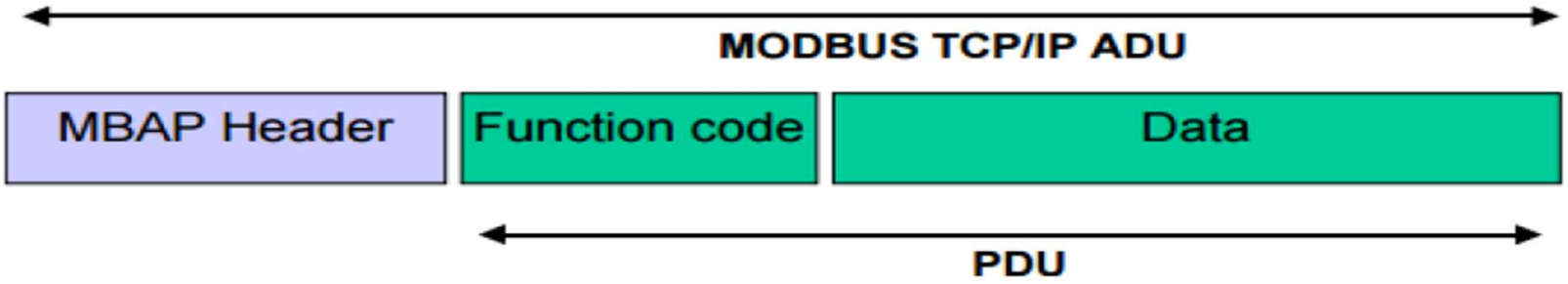
Can Modbus slave report events to master?

- No, only the master can send data requests and also in Modbus RTU (serial) there can only exist a single master in the entire network.

- With Modbus TCP there can be several masters.

https://stackoverflow.com/questions/62101400/can-modbus-slave-report-events-to-master

MODBUS TCP/ADU Application Data Unit (ADU)



The difference between a traditional Modbus Protocol Data Unit (PDU) and the Modbus/TCP ADU is the addition of the Modbus Application Protocol (mbap) header at the front of the frame.

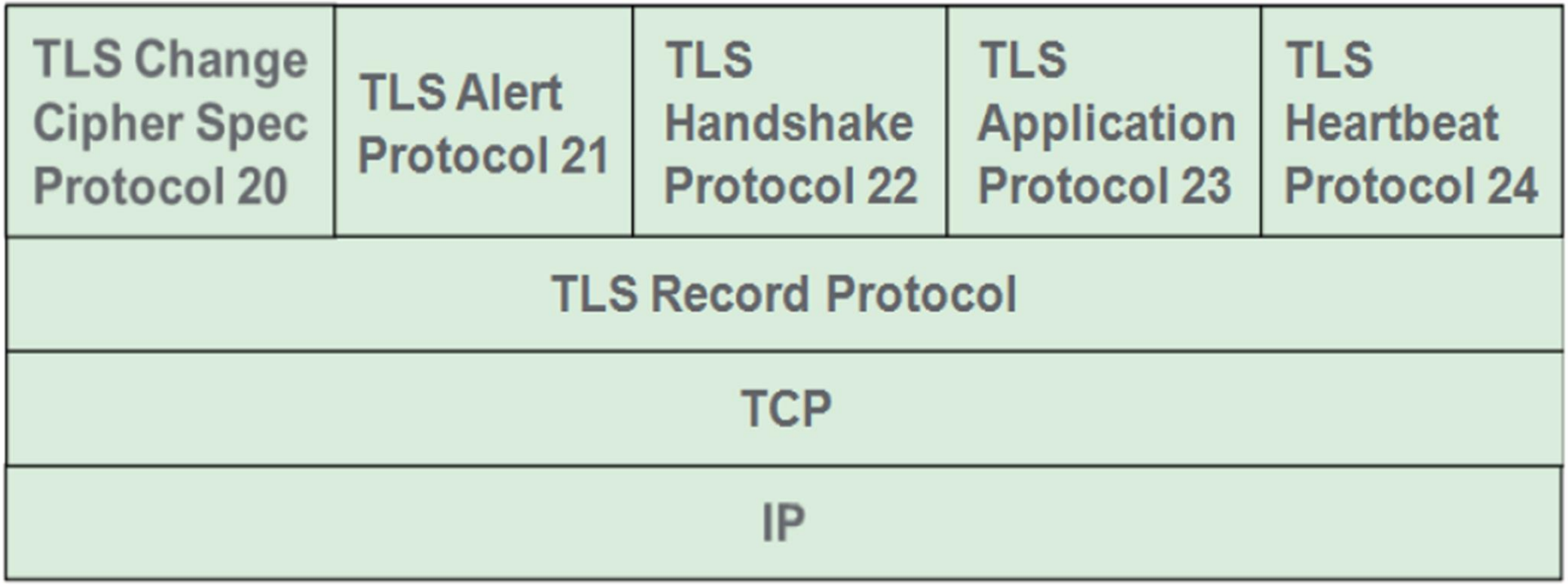
Port number 502 (mbap)

Port 802 mbap/TLS/TCP (mbaps)

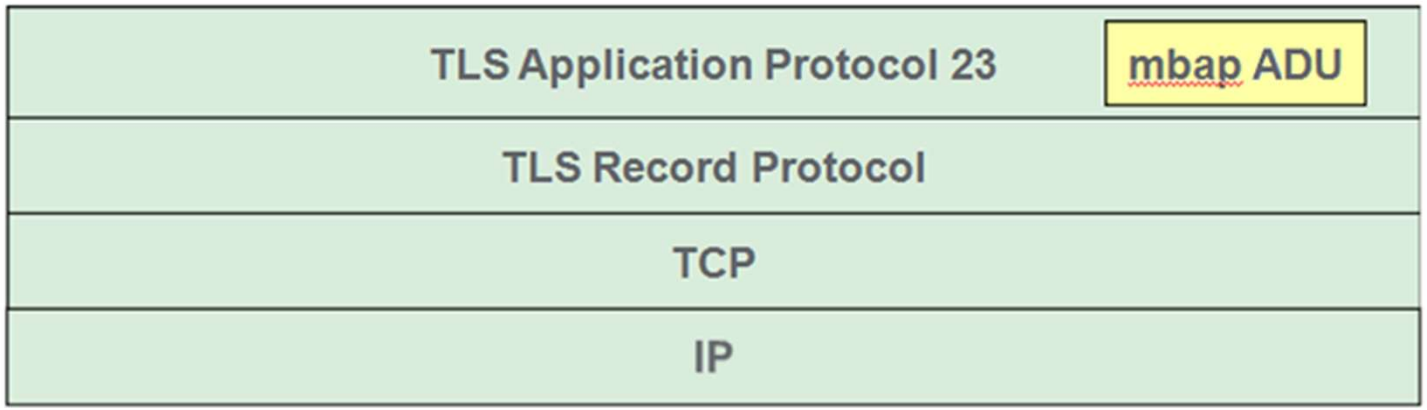
Fields	Length	Description -	Client	Server
Transaction Identifier	2 Bytes	Identification of a MODBUS Request / Response transaction.	Initialized by the client	Recopied by the server from the received request
Protocol Identifier	2 Bytes	0 = MODBUS protocol	Initialized by the client	Recopied by the server from the received request
Length	2 Bytes	Number of following bytes	Initialized by the client (request)	Initialized by the server (Response)
Unit Identifier	1 Byte	Identification of a remote slave connected on a serial line or on other buses.	Initialized by the client	Recopied by the server from the received request

Whenever a MODBUS request or response is sent over in a UDP package, there is a need for this additional information header, MBAP, for the recipient to recognize the message boundaries even if the message has been split into multiple transmissions packets.

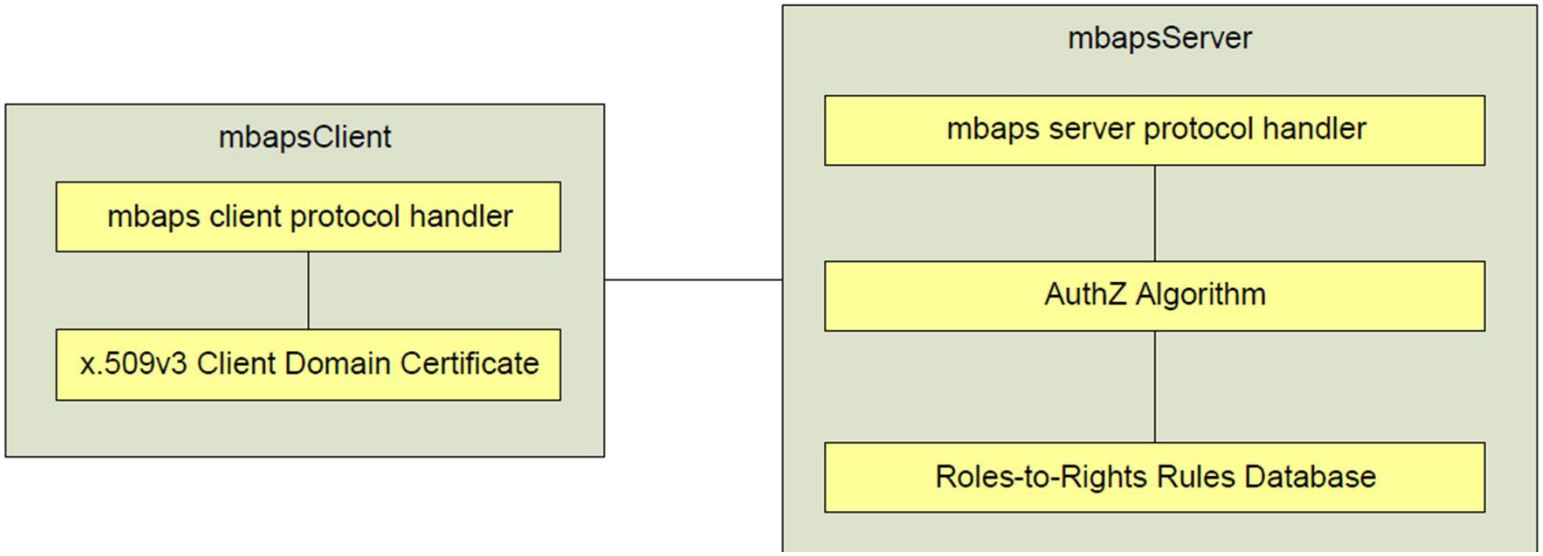
TLS Communication Stack



mbap ADU Encapsulated in TLS



Role Based Authorization



Limitations

- Restricted to addressing 247 devices on one data link, limiting the number of field devices connected to a master station. [Ethernet TCP/IP proving the exception]
- No way for a field device to “report by exception”.
- No security against unauthorized commands or interception of data. [TLS]
- There is no standard method for a node to find the description of a data object, i.e., finding a register value representing a temperature between 30◦ and 175◦.

Source and References

- https://www.ni.com/en-in/shop/seamlessly-connect-to-third-party-devices-and-supervisory-system/the-modbus-protocol-in-depth.html
- https://product-help.schneider-electric.com/ED/ES_Power/NT-NW_Modbus_IEC_Guide/EDMS/DOCA0054EN/DOCA0054xx/Master_NS_Modbus_Protocol/Master_NS_Modbus_Protocol-2.htm
- https://modbus.org/docs/Modbus-SecurityPR-10-2018.pdf
- https://www.veridify.com/modbus-security-issues-and-how-to-mitigate-cyber-risks/
- https://wiki.dfrobot.com/Modbus_vs_CAN_bus
- https://www.mindolife.com/blog-post/modbus-protocol-disadvantages-limitations/
- https://devicebase.net/en/schneider-electric-modbus-tcp/questions/what-is-a-mbap-header-and-what-is-it-for/38q