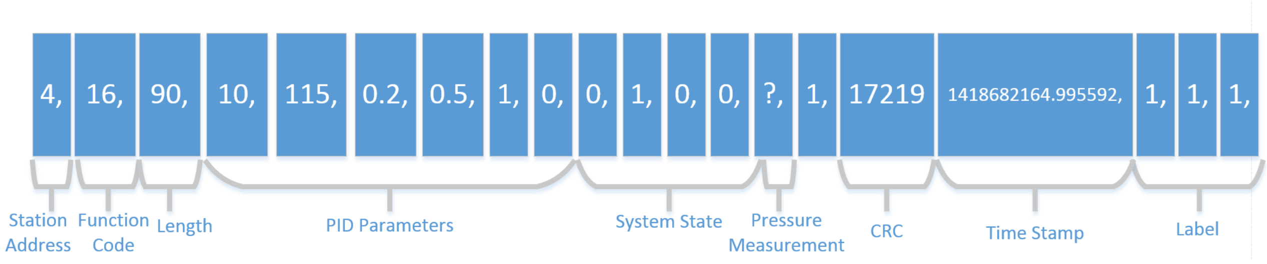
MODBUS/RTU Serial Frame Analysis

Cyber Attacks

Attack Name	Numbers	Category	
Setpoint Attack	1-2	MPCI	Changes the pressure set point outside and inside of the range of normal operation.
PID Gain Attack	3-4	MPCI	Changes the gain outside and inside of the range of normal operation.
PID Reset Rate Attack	5-6	MPCI	Changes the reset rate outside and inside of the range of normal operation.
PID Rate Attack	7-8	MPCI	Changes the rate outside and inside of the range of normal operation.
PID Deadband Attack	9-10	MPCI	Changes the dead band outside and inside of the range of normal operation.
PID Cycle Time Attack	11-12	MPCI	Changes the cycle time outside and inside of the range of normal operation.
Pump Attack	13	MSCI	Randomly changes the state of the pump.
Solenoid Attack	14	MSCI	Randomly changes the state of the solenoid.
System Mode Attack	15	MSCI	Randomly changes the system mode.
Critical Condition Attack	16-17	MSCI	Places the system in a Critical Condition. This condition is not included in normal activity.
Bad CRC Attack	18	DOS	Sends MODBUS packets with incorrect CRC values. This can cause denial of service.
Clean Registers Attack	19	MFCI	Cleans registers in the slave device.
Device Scan Attack	20	Recon	Scan for all possible devices controlled by the master.
Force Listen Attack	21	MFCI	Forces the slave to only listen.
Restart Attack	22	MFCI	Restart communication on the device.
Read Id Attack	23	Recon	Read ID of slave device. The data about the device is not recorded, but is performed as if it were being recorded.
Function Code Scan Attack	24	Recon	Scans for possible functions that are being used on the system. The data about the device is not recorded, but is performed as if it were being recorded.

Attack Name	Numbers	Category	
Rise/Fall Attack	25-26	CMRI	Sends back pressure readings which create trends on the pressure reading’s graph.
Slope Attack	27-28	CMRI	Randomly increases/decreases pressure reading by a random slope.
Random Value Attack	29-31	NMRI	Random pressure measurements are sent to the master.
Negative Pressure Attack	32	NMRI	Sends back a negative pressure reading from the slave.
Fast Attacks	33-34	CMRI	Sends back a high set point then a low setpoint which changes fast
Slow Attack	35	CMRI	Sends back a high setpoint then a low setpoint which changes slow

Features of ARFF Dataset



Attribute	Description
address	The station address of the MODBUS slave device. This address is the same on a query and response to a given slave device.
function	MODBUS function code.
length	The length of the MODBUS packet.
setpoint	The pressure set point when the system is in the Automatic system mode.
gain	PID gain.
reset rate	PID reset rate.
deadband	PID dead band.
cycle time	PID cycle time.
rate	PID rate.

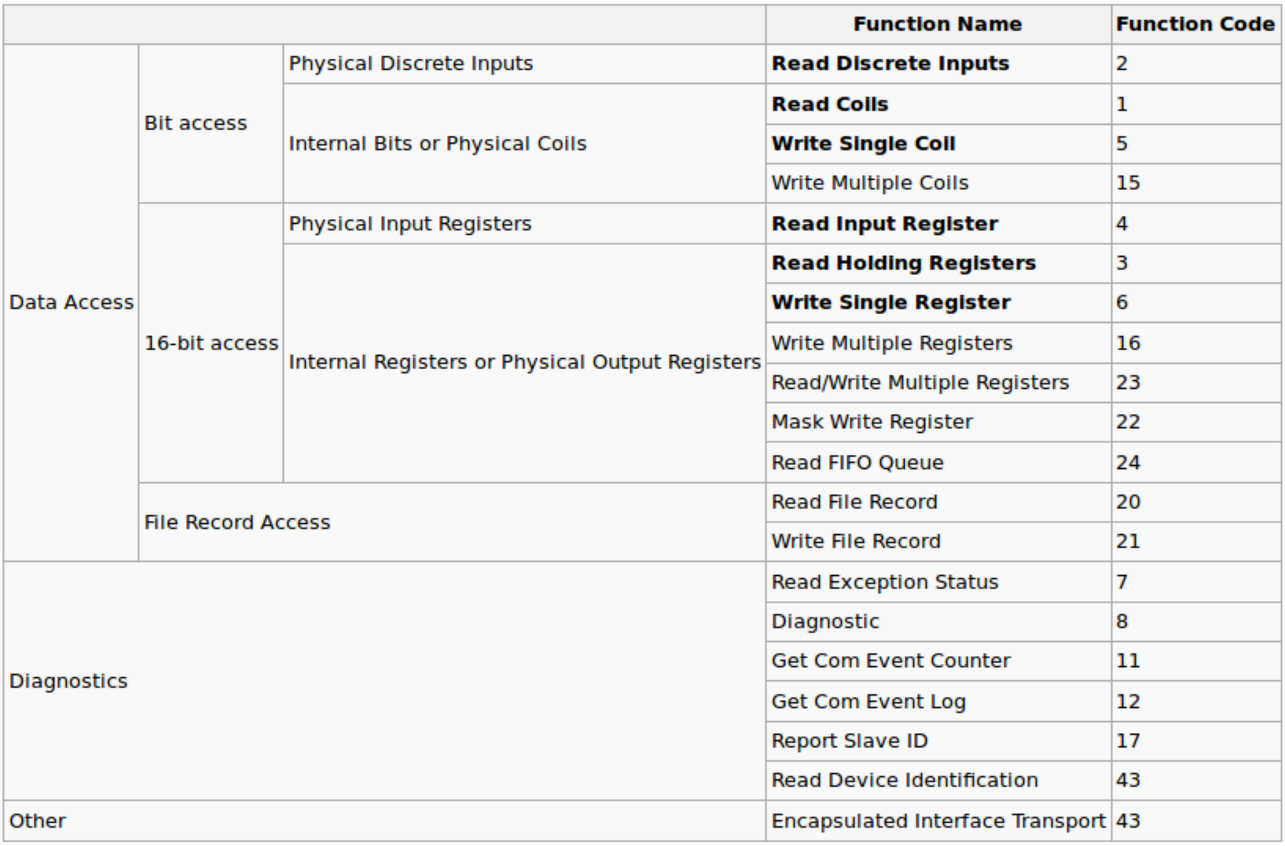
Attribute	Description
control scheme	The control scheme is either pump (0) or solenoid (1). This determines which mechanism is used to regulate the set point.
pump	Pump control; on (1) or off (0). Only used in manual mode.
solenoid	Relief valve control; opened (1) or closed (0). Only used in manual mode.
pressure measurement	Pressure measurement.
crc rate	
command response	Command (1) or response (0).
time	Time stamp.
binary result	Binary class; attack (1) or normal (0).
Attack category	Category of attack (0-7).
specific result	Specific attack (0-35)

NMRI: Naive Malicious Response Injection
CMRI : Complex Malicious Response Injection
MSCI : Malicious State Command Injection
MPCI : Malicious Parameter Command Injection
MFCI : Malicious Function Code Command injection

MODBUS Function Codes

1 : Read Coil
2 : Read Discrete Input
3 : Read Holding Registers
4 : Read Input Registers
5 : Write Single Coil
6 :Write Single Holding Registers
7 : Read Exception Status
8 : Diagnostic
9 : Program 484
10 : Poll 484
11 : Get Com Event Counter
12 : Get Com Event Log
13 : Program Controller
14 : Poll Controller
15 : Write Multiple Coils

16: Wr Multiple Holding Registers
17 : Report Slace ID
43: Read Device Identification
128 : Duplicate Station



			Function Name	Function Code
Data Access	Bit access	Physical Discrete Inputs	**Read Discrete Inputs**	2
		Internal Bits or Physical Coils	**Read Coils**	1
			Write Single Coil	5
			Write Multiple Coils	15
	16-bit access	Physical Input Registers	**Read Input Register**	4
		Internal Registers or Physical Output Registers	**Read Holding Registers**	3
			Write Single Register	6
			Write Multiple Registers	16
			Read/Write Multiple Registers	23
			Mask Write Register	22
			Read FIFO Queue	24
	File Record Access		Read File Record	20
			Write File Record	21
Diagnostics			Read Exception Status	7
			Diagnostic	8
			Get Com Event Counter	11
			Get Com Event Log	12
			Report Slave ID	17
			Read Device Identification	43
Other			Encapsulated Interface Transport	43

Approach :

1. Split the fields from the data and structure it into an object
2. Check for the “specific result” filed of the object.
3. if the value of “specific result” is between (1-35) identify that as an attack and process the object and get the Attack Name, Address and other informations.
4. Collect the number of attacks and its type