ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 8, Issue 6, June 2021

Review of MODBUS and Various Components with Its Application along with Security Study Against Attacks

[1] Mr Sameer S Nagtilak, [2] Dr S R Chougule

[1] Assistant Professor, KITs COE, Kolhapur, India
[2] Professor, KITs COE, Kolhapur, India
Email: [1] sameernagtilak@gmail.com, [2] chougule.sangeeta@kitcoek.in

***Abstract*---In automation field the application is very large for which large different protocols are used such Modbus, Profibus, Canbus etc. In this paper we have discuss Modbus protocol and different devices which can be interface with each other on which Modbus protocol can be implemented with RS 485. Different devices such as RS 485, PIC 32MX are discussed. Also we have discussed different application in which Modbus protocol is used.**

I. INTRODUCTION

Industrial Applications based on PLC scada are at large number currently. Number of protocols are used for transmitting the data such as Modbus,Profibus, CANbus etc. Such protocols can be implemented using various series PIC, Microprocessor and Microcontroller and physical media such as RS-232, RS- 485 etc. Using above components we can create master slave structure in which number of sensor such as pressure, humidity, temperature etc can be controlled in various industrial application in which serial communication takes place.

II. MODBUS PROTOCOL

Based on the requirement Modbus protocol is coded by programmer based on industrial requirement, having large applications in ICS. It is basically used to transfer discrete or analog I/O information between master and sensor nodes located at remote locations industrial. It is basically an open source protocol whose frame structure can modified as per applications and no registration is required. In this master initiates the connection by sending command to slave or client after which client will send response frame consisting of data required by master. A slave device is located at remote location on field which receives the function code describing the function to which client sends the data using Modbus [1].

Master query consist of field address to which commands are to be sent, description i,e function code of operation to be done and bits for error correction and detection. In response field device sends query message contains confirming the action taken, any data to be returned and error checking field. For normal response mode at slave, the function code in the response is an echo of the function code in query. If any problem occurs, error message is constructed in which the details are specified about the problem occurred. [2].

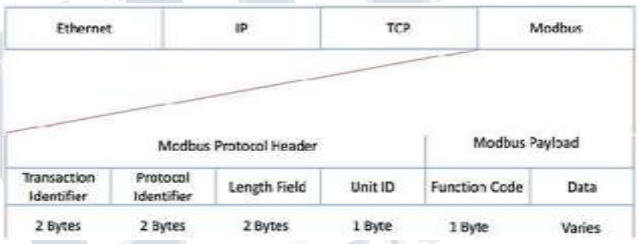

Fig 1. Modbus Protocol Format

Above protocol works in two transmission modes: ASCII mode and RTU Mode. ASCII mode consist of two 8 bye character having size 8 bit byte and RTU consist two 4–bit hexadecimal characters. RTU has advantage over ASCII mode as it gives more output regarding data communication than ASCII

And also it gives more output for same bandwidth and baud rate[2].

III. MODBUS TCP

Ethernet is used in large applications connecting various nodes in network on which Modbus TCP/IP is used having TCP interface. In this blocks of binary data are transferred between two devices such as laptops, PCs etc. It also supports the services such as www. TCP and IP plays two different roles. TCP looks after whether data transmitted in the forms of packet are delivered correctly or not. IP looks after whether the data is correctly addressed and routed

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 8, Issue 6, June 2021

through the shortest path from correct source to destination [3].

In the applications were Ethernet standards are used both TCP/IP and Ethernet standards are responsible from data transmission in the form of Modbus frame between devices. Modbus is an application layer protocol that combines Ethernet with TCP/IP. In above case frame is combined together with Ethernet standard [3].

IV. PIC 32MX

It is widely used RISC CPU with 64 pin and 32 bit core controller having number of stages. It contains 32 – 512 K flash memory and 8-32k data memory with additional 32KB Boot flash memory. It consists number of power modes, number of interrupts whose priorities can be changed in the form of maskable and non maskable. It has 32-bit address and data paths with 32 bit linear addressing two 32 bit core register [4].

The PIC32MX family incorporates a range of serial communication peripherals to handle large number of applications. It is equipped two independent UARTs with built in IrDA encoders/decoders. It supports master and slave operation using two independent IIC modules [4].

One of the main part is the core paert were load/store structure is executed having ALU which has a single cycle and independent multiplication and division unit. It has a register file which has two ports in read mode and one port with write mode which gives minimum latency [4].

V. RS 485

It can be used to mount keypad at the front of control panel along with extension cable. With Modus RTU we can connect it using an 8 wire RJ 45 connector or terminal block. It consist of start stop synchronization method of character. Total number of available station address 1 to 247. With respect to Modbus RTU the frame length is variable. The transmission character format used is binary with variable frame length. It consist of 8 bit fix character length. The error checking method used is CRC-16 [5]. For serial communication between devices above physical standard is used commonly. Digital form of data is transmitted between connected nodes using physical medium as twisted pair. Distance between devices and repeater is upto 4000 feet. The bandwidth between the devices is up to 10. To avoid noise and distortion balanced outputs and differential inputs are used at both ends which is one of the advantage over RS-232 [3].

VI. APPLICATIONS

1. SCADA, DCS uses Modbus in number of applications having human machine interface. It also consists of Model based IDS using DFA based approach [6].
2. In smart grid application data information needs to be transferred for diagnostic, readings, balancing using protocols such as Modbus, DNP etc [7].
3. Different control laws have their own advantages. If we use all these loops on controller, then system is simple and less expensive. Arm is one of the main part of LPC2148 or family IC can be used. Communication of the system is through MODBUS protocol, and GUI using SCADA tool [8].
4. Domestic power plant has Modbus protocol in fieldbus system to transmit data in DCS. Ethernet provides digital data, less noise and real time diagnostics. It has also scope and application in power plant. To get high efficiency serial module can be used so that we need not to change the components of DCS [9].
5. It is also used in genset application to monitor the parameters. The in charge can monitor it online remotely without visiting the actual site and can observe all data and make analysis on web browser, So its user friendly as all analysis and comparison can be done on single platform [10].
6. Modbus when used by SCADA then industrial infrastructure is designed not to be exposed to an open network environment, seriously vulnerable to security threats. Method has to be used to help key exchange for RS 485. Method used has unicast and multicast message structure so that to avoid load with respect to congestion and collision to increase the network capacity [11].
7. Snort helps to avoid attackers to damage the system and also repairs if any attacker has effected the system. Huge traffic on serial channel is diverted to Ethernet and then over LAN so that snort rules can be used to avoid attacks on system. Snort is approved in software atmosphere and also practically on ICS, DCS, SCADA system having both hardware and software applications which can be also used in commercial applications. [12].
8. In industrial applications attacks are monitored in control rooms. ICS is not responsible to monitor the traffic and network parameters between PLCs and RTU.

50 rules have been used to detect unusual conditions in ICS, DCS and SCADA system. [12].

VII. CONCLUSION

In this paper we have discussed Modbus protocol, Modbus/TCP, PIC 32MX, RS 485 and some sensors

which has wide range of applications in industrial field. Using above components, we can design a Client and server model with PIC 32MX as controller with some pressure, temperature etc sensor with RS 485 driver. As number of applications can be implemented but as discussed number of attacks are currently present in industrial system and as we can combine Modbus along with TCP to be implemented on Ethernet the possibility of attacks is also large as applications are wide. So as discussed we have to developed a cryptography algorithm through which the Modbus and Modbus/TCP protocol content can be encrypted and then transmitted which will be decrypted at receiver end.

REFERENCES:

[1] Introduction to MODBUS TCP/IP technical reference Acromag.
[2] Umesh Goyal and Gaurav Khurana "Implementing Modbus and Canbus protocol conversion interace" in IJETT
[3] Introduction to Modbus TCP/IP Technical reference ACROMAG.
[4] PIC32MX family data sheet by Microchip.
[5] RS 485 User manual,Fuji Electric ,Innovating Energy Technology.
[6] Accurate Modeling of Modbus/TCP for Intrusion Detection in SCADA Systems, Niv Goldenberg and Avishai Wool, School of Electrical Engineering, Tel Aviv University.
[7] Universal Controller Design Using Arm Controller" , by Mohsin A. Bandi, Mr. Naimesh B. Mehta, ISSN: 2231-5381
[8] "Design and Application of Communication Gateway of EPA and MODBUS on Electric Power System",by Li Hui, Zhang Hao, Peng Daogang, 2012 International Conference on Future Electrical Power and Energy Systems
[9] "Developing Controller Area Network Management Application Based on Modbus in Multi Generator Set Controller through Local Network and Internet" by Derwin Suhartonoa, Aryan Wibowob, Setiady Wigunac, Robby Salehd International Conference on Advances Science and Contemporary Engineering 2012 (ICASCE 2012)
[10] "Research on A-Key Distribution Algorithms for Protecting Data of RS-485-based Industrial Infrastructure" Jae-gu Song, Sungmo Jung, Seoksoo Kim, WSEAS TRANSACTIONS on COMPUTERS, Issue 9, Volume 9, September 2010
[11] "A Retrofit Network Intrusion Detection System for MODBUS RTU and ASCII Industrial Control Systems", Thomas Morris, Rayford Vaughn, Yoginder Dandass, 2012 45th Hawaii International Conference on System Sciences
[12] ["Deterministic Intrusion Detection Rules for MODBUS Protocols",Thomas H. Morris, Bryan A. Jones, Rayford B. Vaughn, Yoginder S. Dandass, 2013 46th Hawaii International Conference on System Sciences