Modbus Hardware Architecture for Client server Configuration in Automation Industry

Dr Sameer S Nagtilak[1], Dr Sangeeta R Chougule[2]
[1,2]*Department of E&TC, KITs College of Engineering(Autonomous) Kolhapur, India*

***Abstract*— Modbus is one of important protocol in industrial application but does not have any security parameters to protect the information which is carried by Modbus protocol. For which we have to develop intrusion prevention systems (IPS) to avoid active and passive attacks. For this study we have to design a hardware model on which Modbus protocol is implemented and physical standard used is RS-485. So we have developed following circuit of which one will acting as a master node and second as sensor node. Hardware section is divided into two parts namely master node and sensor node between which RS-485 is used as a physical medium between two above nodes on which Modbus protocol is implemented. Both master and sensor nodes are discussed below.**

***Keywords*— Attacks, Modbus, intrusion, attack.**

I. INTRODUCTION

In industrial application large number of applications require automation to avoid processing time. System are developed in such a way that it requires minimum human assistance. Automation has number of applications in field of boilers, heat treating ovens, stabilization aircraft. Main aim is to compare measured value of any process with expected value of system and to check error value and take corrective action on it [1].

II. MASTER NODE

Considering above facts we require some components such PIC, Driver, LEDs. Master nodes are present in mostly all industries having monitoring applications using PLC, SCADA etc. Also in our work we have connected master to senor node and attacker using RS 485 standard and also to PC using UART. Using RS 485 driver we can see the data transmitting and received at master node. At master node three LEDS are present two red and one green were red are enabled when transmitting and receiving is going on were as green is on when process is on. LCD displays the readings received after decrypting it from the data received from sensor or attacker node in values of temperature, humidity. Other polarity diode, noise reduction resistors are present from smooth functioning [2].

Block diagram of master node used in our system on which Modbus is implemented with RS 485 as a physical medium to connect with slave node n vice versa. As shown in above figure it consist of PIC 32MX, RS 485 driver, LCD 16x2 and LED indicators. In our system master node is connected to three slave node which located at field to which sensors such as temperature, humidity etc are connected which passes the readings from field end to master nodes

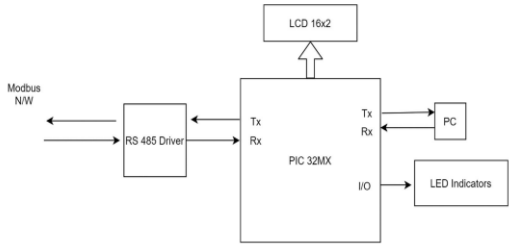

Fig. 1 Master Node

III. PIC 32MX

PIC i.e. peripheral interface controller or programmable intelligent computer is basically a family of microcontrollers has large number of applications in embedded systems. In older days PIC was only having read only memory (ROM) which were having limitations in number of applications. PIC may be of 12,14,16 or 24 bits. Models having DSP functions may have different instruction set. PIC 32MX are based on MIPS32 M4K core which is programmed using MPLAB C compiler which a version of GCC compiler. PIC 32 is 32bit microcontroller providing increased performance at lower operating, sleep and deep currents. It consists up to 512 KB flash and 128 KB SRAM having inbuilt graphics interface, USB port. It is a 32bit RISC microcontroller which supports high performance

applications. It consists of power saving technology such as on the fly clock switching and instruction based power saving modes [3].

PIC 32 can be programmed in two different ways namely self-programming and external tool programming. In self-programming executable code should be present in device with flow and sequence to execute commands. Where as in external method it is not required that code should present in target device but external programmer tool is required. It also provides two physical interfaces namely 2 wire in circuit serial programing and 4 wire joint test action group. Programming executive (PE) is used to execute from target device and hides all the data from programmer. All the overheads is removed by PE which are coupled with data transfer which helps to increase the throughput [4].

PIC is powered by supply voltage in range of 2.3 to 3.6 V with frequency of 80 MHz When PIC is started from programming it enters into Enhanced ICSP mode further into to check device status. After checking the status erase mode in initiated to enter into serial Exec mode to download PE if required. After which data block is downloaded to initiate flash write mode. If flash write mode is initiated, then it verifies the device else it again goes to download the PE. After verifying device, it exits from programming mode for further process. Two interface are used for programming in which device must be properly powered with all signals properly connected [3].

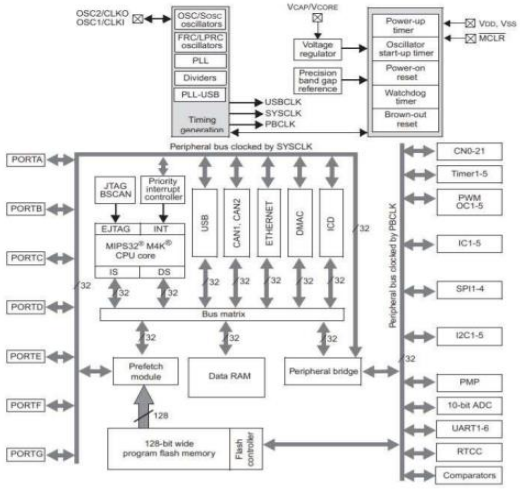

Fig. 2 PIC Architecture

IV. RS 485 DRIVER

Main advantage of RS 485 is it has balanced interface with multipoint operation from single 5V supply so that separate splitter is not required to support 32-unit load also supporting 10 Mbps as maximum data rate. Bus topology were common line is shared between all connected nodes such as drivers, receivers and transceivers is used by RS 485 supporting both full duplex and half duplex communication [5].

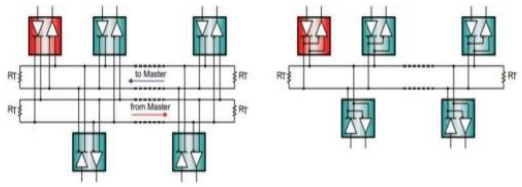

Fig. 3 RS 485 Driver

As shown in above figure in half duplex system only one signal pair is used. RS 485 has advantage than twisted pair cable as it avoids noise from external sources as RS 485 are sheathed, unshielded, twisted pair type. The maximum length to be used in various applications is depended on losses occurring during transmission and jitter [6].

It can be used in both two and four wire network system. Also as discussed above the tristate capabilities helps multiple transmitter and receivers to be connected to any of above two wire bus topology used any applications. If the application is having four wire system, then it can be used were master node is connected to all the slave nodes and divers in system in a daisy chain structure also called as bus topology. Also RS – 485 has an advantage that it supports variety of applications based on bus, ring, star, tree etc. topologies were selection of topology is based on the baud rates low or high, physical distance of system and possibility of noise to be introduced in the system. Also when the data has to be transferred at long distance then we have to use repeaters were these repeaters are placed in a system to avoid load on a single segment and divide it on multiple segments. Also these repeaters can be used in both two wire and four wire applications and also in any kind of topology such as star, tree, bus, ring. In all above cases for choosing transmission line the length of the system has to be known and also the data rate of the system. Considering the fact Cat 5 available in UTP and STP is a good choice for RS-485 systems [7].

RS 485 is used in large number of applications on of which is Boiler header inspection robot (BHIR). RS

485 here provides the communication between PC with BHIR connected to controller [8].

RS 485 has also one more application i.e. it supports multi host online. It works on basic principle which has single chip microcomputer, combined with RS 485 along with triode characters with half duplex master slave. Fieldbus is used for communication between different nodes using protocols such as Modbus, can bus etc. [9].

In ICS, PLC and SCADA applications large number of master and sensor nodes are connected with each other through RS 485. In all above applications it is used as a communicating device and data collection. [10].

In industrial sector heavy engines are installed and used for ICS which makes heavy power consumptions. Saving electricity in industries is major concern today. In this process the Energy meter detects all the parameters like Voltmeters, Ammeters, VAF Meters, Energy Meters, Power Meters, Power Analyzers, Power Factor Meters and so on. All these parameters are transmitted using RS485 based MODBUS protocol by energy meter. The system is based on AVR microcontroller continuously communicating with this energy meter and sending all these parameters using GSM module to the Server Computer for further data logging and monitoring [11].

V. SENSOR NODE

Below figure shows the details of the components used in sensor node. As discussed earlier our system consist of two parts in hardware namely master node and sensor node both consist of PIC 32MX along with RS 485 driver, LCD 16x2 and LED indicators. As shown in above figure sensor node consist of number of sensor that are connected depending on application from which inputs are given to PIC 32MX. In our system we are going to use sensor such as temperature, humidity, terminal adjustable regulator. In large application specifically in automation field sensors are located on actual machinery far distance from the server. The reading taken should be transmitted to server which is located at remote location.

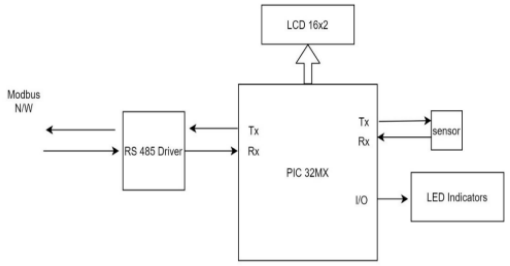

Fig.4 Sensor Node

If both master and server are located at same industries RS 485 is used to carry the data or reading from sensor to master and vice versa. As number of protocols are used in 45 automation field and as discussed earlier in our system we are using Modbus protocol to transfer data from sensor to master and vice versa. Also main aim is to provide security during data transmission from sensor node to master node such that data should not be corrupted and modified by attacker [12]. So care should be taken during transmission of data during transmission as it has to converted from readable format into non readable format and then transmitted from transmitted end and at receiver end again it has to be converted back to readable format from non-readable format. In our system one of the sensor used is DHT11 which is digital temperature and humidity sensor which provides output in digital form. Such sensor is used in applications such as HVAC, dehumidifier, automotive, automatic controls and data loggers, whether stations, home appliances etc [13].

VI. RS 485 TRANSCEIVIER

Figure shows the circuit diagram of RS485 transceiver which has balanced interface to increase noise immunity and is also multipoint bidirectional single pair wires which reduce the cabling cost. For long distance communication large differential signal ranges are used which can achieve signaling rates to 50 Mbps [14]. It has large applications 48 in E- Meters, HVAC, Motor Drives, Automotive sectors, PLCs along with Modbus protocol which act as a communication protocol between master and sensor node. The circuit diagram consists of MAX485 IC to which power supply of 5V is given and HDR1X2RS485 connector is used. Circuit is connected to microcontroller to which readings taken from master or sensor nodes are given to controller so that it can take necessary action.

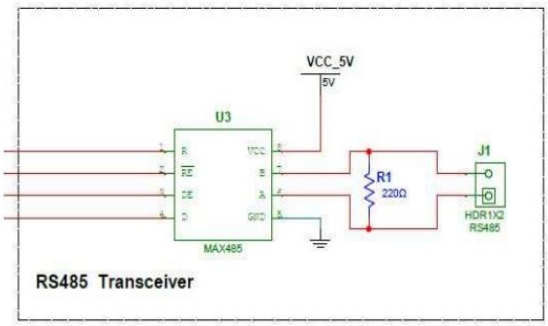

Fig. 5 RS 485 Transceiver

Small network means network having less number of nodes does not require large common mode voltage (CMV). Fractional unit load devices are not required in the networks having less than 32 nodes. Its operating voltage is +5V and rated current is 300µA [15].

VII. CONCLUSION

Even in current days' large number of applications are working on wireless communication still in industries wired communication is preferred due to its robustness and reliable communication, especially in harsh environments. An Android application that allows the management of all network nodes is also developed. The users only need to understand the requirements. Then they can make use of the graphical programming language to change the functions of a node. Entire compilation, communication and firmware upgrade process for network nodes is done automatically and accurately. The hardware used is popular, cheap, and suitable for different deployment environments.

REFERENCES

[1] Naveen Reddy K P, Undavalli Harichandana, "A Study of Robotic Process Automation Among Artificial Intelligence", International Journal of Scientific and Research Publications (IJSRP), February 2019.

[2] Valeriy Vyatkin "Software Engineering in Industrial Automation: State-ofthe-Art Review", IEEE Transactions on Industrial Informatics August 2013.

[3] PIC 32 data sheets

[4] https://datasheetspdf.com/pdf/748111/Microchip Technology/PIC32

[5] Kevin M. Lynch, Nicholas Marchuk, Matthew L. Elwin, "Embedded Computing and Mechatronics with the PIC32 Microcontroller".

[6] The RS- 485 design guide, Texas Instruments, February 2008,Revised October 2016.

[7] RS-422 and RS-485 Application ebook, B+B smartworx

[8] Nur Maisurah Hassan Basri, Khairul Salleh Mohamed Sahari, Syed Sulaiman Kaja Mohideen, Mohd Zafri Baharuddin, Adzly Anuar "RS-485 Interface for Boiler Header Inspection Robot Prototype" 2012 International Symposium on Robotics and Intelligent Sensors.

[9] Yang Cheng-ying, Chen Yong "Research on Multi-master Communication System Based on RS485 Bus" IOP Conf. Series: Journal of Physics: Conf. Series 1237 (2019) 042078.

[10] Liang Zhao, Ruobing Liang, and Jili Zhang "The Solving of Bias Resistor and Its Effect on the RS485 Fieldbus" Journal of Advances in Computer Networks, Vol. 2, No. 1, March 2014.

[11] Ashish K. Rewatkar, Ashwin Y.Ankar, Pradeep B. Dahikar " RS485 Data Transmitter through GSM Service to Server Database Logger" ,IOSR Journal of Computer Engineering (IOSR-JCE).

[12] Pal Varga, Sandor Plosz, Gabor Soos, Csaba Hegedus, (2017), "Security Threats and Issues in Automation IoT" IEEE 13th International Workshop on Factory Communication Systems (WFCS).

[13] Umesh Goyal, Gaurav Khurana, "Implementing MOD bus and CAN bus Protocol Conversion Interface", International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue4- April 2013.

[14] RS 485- Proud Legacy a Technical white paper by ADVANTECH Chengbo YU1, Yanfei LIU1,2, Cheng WANG2, "Research on ZigBee Wireless Sensors Network Based on ModBus Protocol", Wireless Sensor Network, 2009, 1, 1-60.