Review of Modbus Security and its applications in 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— **In Automation applications are growing in large scale in various fields. Previously human man power was used for various work in industries such data reading, data monitoring, device control etc. The task is to take the readings, send signals in form of request and response commands for control station to the end node and maintain the record. This task has to be done at regular interval of time by human operator. Also it involves task to identify the faulty nodes, channel and replace it. It has a possibility of errors in human operators reading which has to be rectified with higher priority.**

Keywords— Attacks, Modbus, intrusion, attack.

I. INTRODUCTION

Different protocols can be used in automation fields such as Modbus, Can bus, Profibus etc. In our work we have used Modbus along RS 485 as a communication channel along with PIC32MX795F512H, power supply, LCD module, reset circuit, RS 485 transceiver, sensor connector, pc connector and LED indicator. We are going to review the work in different areas such as Industry requirement, Modbus protocol and its applications, possible threats and security measures for the system. Some of the important parameters which are responsible for network security are authentication of user, to modify data content, fake identity, denial of service etc. Network security is very important to secure the data transfer between end devices passing through communication channels. Following are some parameters responsible:

1. Network topology
2. Type of communication channel
3. Attacks on network
4. Hardware and software
5. Protocols and its features used
6. Methods to avoid attacks
7. Security methods to implemented

II. INDUSTRY REQUIREMENT

Automation is a key aspect to increase the overall productivity of any company but still it is not used and implemented in wild application. So it is necessary to see the challenges and hurdles to implement automation technology in existing industries. An awareness about current state and future state of operations to make it effectively has to be done. Also robotic process automation (RPA) is also having large demand in industries along with artificial intelligence (AI). Depending on quantity of production programmable automation is selected mostly for small and medium scale. Intelligent robots play an important role in programmable automation with accuracy [1].

Software engineering plays an important role in automation industries and also in manufacturing industries. In recent decade the use software in automation industries is increased from 20% to 40%. If it continues then in coming days' software will cover major section in industrial applications. Depending on increasing application of software large number of research projects are growing along with combination of PLCs and SCADA system on which number of communication protocols are implemented. In this work various protocols such as Modbus, Profibus, Canbus are used which takes care for reliable data transmission of data between master and sensor nodes. Also certain problems related to data security during transmission of data in which possibility of attacks can place also due to software involved the exposure of network is now to internet through Ethernet standard [2].

III. MODBUS PROTOCOL AND ITS APPLICATION

Automation In automated industries large number of sensors are extensively used and integrating it with PLCs, SCADA large number of industrial applications are implemented. With new technology emerging like IOT(Internet of Things), large number of low cost sensor are in great demand. Basic idea of IOT is to connect low power devices such as sensors, actuators etc. which are termed as things with existing internet technology which can support large number of devices. Industrial system also require very large security network but unfortunately currently it is not implemented. As sensors and actuator are directly having communication with Physical layer possibility of attack is very high [3].

Bus are used to carry the data between the nodes in the network which are designed on the basis of protocols used such as CAN bus, Modbus. As in network two types of interface are used namely user-network interface and network – network interface at which different types of interface are used where protocol conversion is required which are to be studied. Field bus standards are not uniform which leads for large difficulty in design of system having different sensor nodes used for reading different values. So to make effective communication in network with serial communication with different interface Modbus and Canbus are two protocols used in large number of industrial application [4].

Serial communication is an important mode of transmission of data between the nodes in number of application which mainly consist of three versions namely: RS 232, RS 422 and RS 485 which use both at industry and laboratories. Considering the factors such as number of end nodes, balanced or unbalanced configuration, data rate, length of transmission it was suggested that RS 485 has advantage over other two serial communication versions. Also in networking Ethernet standard is also used but comparing it with RS 485 we will see both will have several advantage and disadvantage over each other. Ethernet has good data rate but has length limitation and collision avoidance methods are to be incorporated where as in RS 485 data rate is less but length is large and due to polling method collision avoidance is incorporated. Each system has connected to Ethernet has possibility of attacks also for RS 485 which are running Modbus TCP/IP when connected to internet has attacks but RS 485 can provide an additional level of security [5].

Zigbee is one of the protocol which is also used in large number of application in mostly wireless sensor network. It is a less expensive protocol which is used in number of applications in home, industries, PLC automation along with in toys and games were sensors are involved. If we combine Modbus along with Zigbee then extra conversion methods are avoided and good communication is established along with data can be viewed at different interface. Combining Zigbee with Modbus has a good application in plant physiological plant monitoring application as advantages of both Zigbee and Modbus are added in above applications [6].

Modbus can be also used to design a communication gateway for EPA and MODBUS. This gateway has main application in process control of power plant which is secure, stable and real time. Mostly DCS system are used in domestic power plants along with fieldbus, Modbus protocols. ARM7 along with OS II is used where result is shown using EPA-RT serial module without changing original DCS structure. In this gateway bidirectional protocol conversion is done. Different equipment’s are also connected using RS 485 bus connection. Modbus messages are directly delivered using ARM 7. It makes clear that Modbus has an application in power system device digitalization and informatization [7].

In modern application uninterrupted power supply is required along with secure data transmission. SCADA systems are mostly used in power station which require some communication protocol for data transfer. SCADA is used to control electric power station which also requires broad range of surveillance. These system uses number of protocols such as Conitel, Profibus, Modbus, RTU and RP -570. MACICO is an agency has proposed some methods to remove problem having in interconnecting different telecommunication networks. Also using DSiP TCP related problems are resolved [8].

Power system consists of different sections such as generation, transmission and distribution where existing communication network is to be combined with power network in smart grid systems. In this paper experimental results of WSN based on mesh topology are discussed where mesh topology is used in which Modbus protocol is used. In WSN nodes microcontrollers with IEEE 802 standard having

Modbus application are running on WSN stack. Modbus node performs number of application such a read energy meter etc. In this system Modbus master and slave model is used which polls a specific Modbus slave for measurement of data. It consists of four slave devices and a master device [9].

In market different control strategies are present and also some are proposed on ARM embedded platform. These controller different control methods. Currently industries PID are extensively used to optimize the control action. PID also has applications in fuzzy, adaptive etc. LPC2148 microcontrollers are based on 16 / 32 bit ARM7. Advantage is different control loops can be implemented on single arm controller by which device is used again and communication of system is through Modbus protocol [10].

CAN bus along with Modbus are two commonly used field bus protocols along with protocol conversion. During initiation of communication interrupt is generated and on receiving interrupt CPU enters ISR. Also PIC32MX microcontroller is used as intermediate between RS485 and CAN ISO1050 as a conversion interface [11].

Software is developed to collect dissolved values in environment after regular interval of time using visual C++ and RS 485 for communication process. The oxygen meter used DO -200-S which has LCD panel, four keys used to set relevant references, two relays and RS485 supporting Modbus protocol. Two physical connecting methods are introduced one with desktop connecting with meter and other laptop with meter [12].

Large number of applications are based on network embedded systems such as green house. In green house applications embedded web servers along with Modbus protocol for connecting sensors and actuators used for 24 hrs monitoring. Modbus based 24 greenhouse is a small size network with number of sensors, actuators etc. with dynamic topology. In this application data is gather together from local sensor/actuator and routed to other network situated on internet. Connection between internet and web server is done through Ethernet [13].

Multiple genset can be also monitored using Modbus protocol through local network and internet. It helps genset technician to monitor multi genset located at different location only by using interface. Advantage is previously monitoring was done manually but now it can be done via computer. Generator control information is transmitted using Modbus protocol to client that uses TCP/IP. In this topology number of genset are connected together to a single computer server. The data monitored and collected is stored in data base where it will have presented online via website. Also convertor is required for RS – 485 to RS – 232 as server computer is connected via serial port RS -232[14].

Currently large demand in applications on smart devices is present in different commercial industries. Sensor are used in place of analog devices which are used to measure temperature and pressure. Microcontrollers are used for data processing and result are shared using RS 485 on which Modbus is implemented. Also ARM Cortex M3 along with USART connected to ADC. Modbus/TCP or Modbus/RS 485 are used for communication between PLC and PCs [15].

In manufacturing industries data monitoring is very important in which status of machine running produces large amount of data which should continuously analysed at regular interval. Sensor values are noted through serial port through devices. In industrial automation microcontrollers are used along with RS 485 on which Modbus protocol is implemented. This system also consists of PLC, Arduino, analog module, GSM/ GPRS module, Wi-Fi etc. All data in PLC are accessible through Modbus over Ethernet Modbus TCP. Arduino is also configured as Modbus client in which both Modbus request and response command are used. Also in future the work is scaled up to read data from different protocols such as Modbus TCP/IP, Modbus RTU protocol. Along with Modbus protocol based on Ethernet standard TCP combine together with Modbus namely Modbus TCP is used in number of application based on automation and tele control systems. MQTT is used for machine to machine data transfer along with Modbus TCP in an IIOT applications. Mostly it is based on polling and request response pattern. In one scenario Modbus TCP can be also considered as an IoT protocol which is based on request response pattern and in second Modbus TCP can be also used in conjunction with message queuing telemetry transport(MQTT) in which the need of gateway is eliminated. Number of applications combine MQTT which works on polling based principle along with Modbus which works on request and response model. Also we can compare HTTP, CoAP, MQTT and

Modbus TCP based on parameters such as infrastructure, layers, pattern, methodology encoding, security etc. In number of applications message structure of Modbus TCP is maintained throughout communication as MQTT lacks of interoperability [16].

In some applications Modbus slave is designed and implemented on Modbus RTU over RS-485. Applications consist of cortex, 32- bit ARM processor that provides communication between master and slave using RS 485 in two ASCII and RTU mode. Considering the parameters such as reliable, fast data acquisition, real time speed etc cortex MO is efficient on which RS485 is used so that network can communicate with number of devices. Modbus RTU and TCP is used for batch of control of an pharmaceutical company using PLC as slave and Modbus TCP and RTU to communicate with master. Slave Modbus can be also configured using RS 485 and FreeRTOS used for real time application. Also in combination with cortex Modbus is also used for data acquisition for electrical parameters used in smart meter to obtain voltage, current, three phase voltage and current [17].

In coming year industrial wireless sensor network (IWSN) has a important role in industrial automation to help in competitive growth in Industry 4.0. In some industries Node-RED is used for smart factories for data transfer in wireless mode between different nodes. [18].

Problem of power outage, short circuit is present in number of electrical applications for which data analytics has to be done to avoid adverse effect of above parameters and improve energy consumption. These parameters are measured by multifunction meter (MFM) installed in various commercial or residential buildings. For data analytics extraction of data is required which is important as it has to be taken from multifunction meter (MFM). Raspberry pi is used as master controller to which server is connected in 26 wireless mode. The multifunctional meter works on RS 485 Modbus protocol which collects the data from different devices only when devices sends request which avoid extra traffic on bus to avoid congestion. Mostly this system is half duplex in which Modbus protocol supports maximum 247 devices without repeater [19].

As the role of internet is crucial now a days and its importance is growing now a day in residential applications as demand of smart applications is growing among people. Controllers uses Modbus TCP which is packet transmission protocol to connect different nodes. Serial number 502 is assigned to Modbus TCP in instrumentation and automation applications. Only the case is using Ethernet is expensive as we have remove existing cables and place Ethernet cables so that TCP/IP can be implemented which consist of security aspect as it is working on transport layer were Modbus does not have any security parameter so we have implement separate algorithm [20].

IV. SECURITY REQUIREMENTS

Mostly on industrial applications attacks are rare but still it should be avoided. Process flow may be changed when attacks take place. To avoid the threat three things are to be considered one to extract value of process variables from traffic in network, second based on time series characterize variables and third regularity in variables are to be monitored. Prototype is to be implemented and then it is to be evaluate with real world network traffic. Above approach does not completely detect PLC code updates but when PLC code update takes place means special command is issued to PLC. So it is important to find such events by taking commands from application layer. Also attacks are not in above preview which can be overcome by gaining approach on PLC, in above approach use of automation protocols is beneficial as data model of protocols is generic and defines two process variables registers and coils which makes coding easy [21].

Large efforts are currently going on to identify different attacks and possibility of system being exposed. Also with respect to above attacks efforts are also been taken to prevent the attacks. Signature based attack detection used and is effective to monitor serial port in ICS. In this research one of the automation protocol Modbus RTU and Modbus ASCII where demonstrated on which signature based intrusion detection system was used. Thus malicious activities are detected on ICS using Modbus protocol in which SNORT intrusion detection system is introduced.

Basically in number of automation protocols are not developed for security and also it does not contain any security measures. Depending on survey it is clear that attacks takes place on these protocol and its applications. One of the type is attackers inserts false command which cause malfunction in normal operation in the application. So we have to discuss different attacks on system and detection algorithm with concerned to above discussion. Also we have to consider flooding attacks in which network traffic dataset is taken into consideration. Flooding attack is the attack where packets are injected into local network connecting HMI. It does not block the messages but sends large number of normal messages which increases network load i.e flood messages which lead to congestion. It successfully detects the flooding attacks in which signature based detection are fastest to detect.

Some attacks continuously monitor the network traffic in some of the applications such as power grid industrial control system. Simulated system consists of two PCs one for SCADA monitoring and second for simulation PC. Raspberry Pi is used as relay controller on simulation PC end and SCADA at monitoring end. C++ python script along with Pybroswer is used. After simulation results it seems that padding namely roundup padding and random padding are one of the effective method to avoid attacks. Even though padding reduces the possibility of side channel attacks but increase the load on the traffic. Also padding may consume one third of bandwidth and also full leakage and attacks are not avoided. So depending applications low level of padding can be used to avoid wastage of bandwidth.

Encryption and decryption is combine together termed as cryptography. This method helps to store important information in hard disk etc. and transmit it over an insecure network so that it is protected from unauthorized users. As cryptography is a process it consists of various components one of which is cipher. Cipher is also a series of well-defined steps which can be termed as procedure. Thus cryptography is process to secure data and cryptanalysis is process to break secure communication in other words we can say it as attackers [22]. Key is generated using some key generation algorithm which is provided to source end and same key is used and transmitted to destination end through secured channel. This coded text is transmitted to destination through communication channel which can be wired or wireless. At destination decryption algorithm takes the input cipher text and another input a key received and gets original message. One of the method is user defined key which are generated by programmer. This key but can be easily identified by attackers and can cause problem in communication. In another method pseudorandom generating sequence is used to generate the key were chance of identification of keys is less. In this algorithm is used to generate a sequence of numbers whose properties are like random number [23].

V. CONCLUSION

So points that can be elaborated from above review are:

- Energy sectors, power sectors, industrial sectors, home and industrial automation sectors.
- Most serial communication application use Modbus and RS 485
- False data transmission may collapse whole system.
- Major parameter - Light, Temperature, Humidity, Pressure etc.

Currently no encryption algorithm is implemented in above protocols. Considering the above fact, a Cryptosystem tools is required to handle different attacks. Cryptosystem tools will be based on the Key generation which will be employed on any one Modes of protocol such as modbus, profibus, canbus etc. Further the Cryptosystem Tool should be applied to Master and Slave structure which can effectively prevent the intrusions affecting the system.

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-of the-Art Review", IEEE Transactions on Industrial Informatics · August 2013.

[3] 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).

[4] Umesh Goyal, Gaurav Khurana, "Implementing MOD bus and CAN bus Protocol Conversion

Interface", International Journal of Engineering Trends and Technology (IJETT) - Volume4Issue4- April 2013.

[5] 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.

[6] JYRI RAJAMÄKI, JARI AHOKAS & PARESH RATHOD, "Proposing a Redundant Communications Model for Critical Infrastructure Protection and Supervisory Control and Data Acquisition (SCADA) System", ISBN: 978-960-474-336-0, Recent Advances in Computer Science and Networking.

[7] Mrityunjai Tiwari, Sasi SR Kumar, Sukumara T, "Adaptibility of Wireless Sensor Network for Integrating SMART GRID elements in Distribution System" 2013 Colloquium November 13-15, 2013.

[8] Yingjuan ZHAO, Jingnan MA, Shaojuan LI,Jia,"Design of Modbus Wireless Communication System Based on Remote Data Transmission" International Forum on Mechanical, Control and Automation (IFMCA 2016).

[9] Mohsin A. Bandi, Mr. Naimesh B. Mehta, "Universal Controller Design Using Arm Controller", International Journal of Engineering Trends and Technology- Volume3 Issue2- 2012.

[10] Umesh Goyal, Gaurav Khurana, "Implementing MOD bus and CAN bus Protocol Conversion Interface", International Journal of Engineering Trends and Technology (IJETT) - Volume4 Issue4- April 2013.

[11] HU Zhong-shan, LIUYuan, LI Yong-de, HU Cheng-xi, "Development and Realization of the Software for Dissolved Oxygen Controller", 2012 International Workshop on Information and Electronics Engineering (IWIEE).

[12] Shashi Raj K, Nayana D K, S S Manvi, "Modbus based Greenhouse Monitoring and Control", International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012.

[13] Derwin Suhartono, Aryan Wibowo, Setiady Wiguna, Robby Saleh, "Developing Controller Area Network Management Application Based on Modbus in Multi Generator Set Controller through Local Network and Internet", International Conference on Advances Science and Contemporary Engineering 2012 (ICASCE 2012).

[14] Stephan Sommer, Michael Geisinger, Christian Buckl, Gerd Bauer, Alois Knoll, "Reconfigurable Industrial Process Monitoring using the CHROMOSOME Middleware", 2012

[15] Samer Jalodi "Protocols of an Industrial Internet of Things Environment: A Comparative Study" Future Internet 2019.

[16] Devanshi N. Patel, Prof. Sunil B. Somani, "A Review on Implementation of MODBUS Communication Protocol and its Applications", International Journal of Electronics Engineering Research. ISSN 0975-6450 Volume 9, Number 4 (2017) pp. 621-629

[17] Mohamed Tabaa, Brahim Chouri, Safa Saadaoui, Karim Alami, "Industrial Communication based on Modbus and Node-RED" The 9th International Conference on Ambient Systems, Networks and Technologies,2018.

[18] Sandhya CSR, Sri Vaishnavi Tirunagari, Shubhasmita Sahoo, Pradeep Kumar Yemula, "Extraction of Data from an RS-485 enabled Multi Function Meter for Building Monitoring Systems"

[19] Zeyu Xiao, "Application of Modbus / TCP Protocol in Smart Home", Advances in Computer Science Research, volume 70, 2nd International Conference on Mechatronics Engineering and Information Technology (ICMEIT 2017).

[20] M. Jamshidi , A.S. Jaimes Betancourt, J. Gomez, "Cyber-physical control of unmanned aerial vehicles", Scientia Iranica D (2011) 18 (3), 663–668.

[21] Valeriy Vyatkin "Software Engineering in Industrial Automation: State-of the-Art Review", IEEE Transactions on Industrial Informatics · August 2013.

[22] Umesh Goyal, Gaurav Khurana, "Implementing MOD bus and CAN bus Protocol Conversion Interface", International Journal of Engineering Trends and Technology (IJETT) - Volume4Issue4- April 2013.