Turkish Journal of Computer and Mathematics Education Vol.12 No.13(2021), 2379-2383

Research Article

Security Design for Modbus protocol against intrusions during implementation on Industrial applications

Mr Sameer S Nagtilak[a], Dr S R Chougule[b]

[a] Assistant Professor,KITs COE, Kolhapur
[b] Professor, KITs COE, Kolhapur
[a] sameernagtilak@gmail.com, [b] chougule.sangeeta@kitcoek.in

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 4 June 2021

Abstract: Security is an important parameter currently as internet communication application is growing widely. As we use large number of protocols in automation field such as Modbus, Profibus etc. Mostly used one of the protocol is open source protocol is Modbus used for large number automation industries but which does not have any security mechanism to protect the data during transmission from sensor to master node from different intrusions. In this paper we are going to discuss different threats and intrusions during data transmission through Modbus protocol and some preventive measures to avoid it.

Keywords: Modbus, SCADA, attacks, Modicon

1. Introduction

In industries Modbus protocol has wide application mostly were SCADA and PLCs are used. In these industries general structure is two kind of nodes namely master node and sensor node. Sensor node can be different sensors used such as temperature, humidity etc which are installed at field from which readings are taken and are transmitted to master devices through Modbus protocol. Guided communication media RS-485 is mostly used to connect these sensor nodes to main PLC or SCADA. Also in some cases Modbus/TCP are used to communicate between sensor nodes and PLCs. SCADA and PLCs are both used in applications such

as chemical plants, electric power generations, transmission and distribution,water distribution and waste treatments. In above system were master and sensor nodes are present along with sensors they only carry data and it has no measures to prevent attacks. Different components and nodes used in application are only concerned with data transmission and do not check whether nodes are authentication and is data coming from authorized nodes. So if attacker modifies the data carrying protocol it may cause malfunction in operation of infrastructure [1].

Further we have to consider different attacks currently present which are namely active attack and passive attacks. In passive attacks the attacker only observes the data being transmitted and do not modify the data. In active attack attacker modifies the data being transmitted. Considering all above facts, it is necessary to introduce security parameters so that attackers may not be able to read the data being transmitted.

2. Passive attacks

Passive attacks are salient observer. These attacks just saliently observe the nature of traffic, network operations, message patterns etc. As it only observes different parameters stated above these attacks are difficult to detect. Along with observation it provides required data for next level of attacks i.e. active attacks were data is modified. Simply we can say that target of passive attack is to listen and take sensitive information without the knowledge of sender and receiver. Some of other information that it can take is length, time and frequency in wireless transmission. Some of passive attacks in wireless transmission are homing, traffic analysis, corrupt AP, war driving, brute force, eavesdropping etc. which can further result in different active attacks [2].

Wormhole is type of passive attacks which collects data in network and which is also useful for active attacks. As compared with active attacks passive attacks are less destructive. Mostly sender and receiver identity are not disclosed. If attacker takes control of unknown system, then it can have control of data flow between sender and receiver by collecting all the information of all intermediate nodes by which in next level it can be used to destroy the performance of whole network and such kind of attack is a category of passive attack termed as collusion attack. Other type of passive attack is latency attack in which delay is observed and controls by attacker from one node to other node. Attacker also control the delay between two nodes which causes late data transmission [3].

3. Active attack

During data transmission some of the major objectives that has to be maintained are confidentiality, Authentication and access control. In all objectives intrusion plays an important role one of which is active

attacks. This attack is not a salient observer but also modifies the data being transmitted from source to destination. It mainly has four categories namely Masquerade, Replay, Modification of messages and denial of services. False identity is introduced between two devices which can send false commands termed as masquerade attack. Multiple copies of a single message can be generated and are transmitted to receiver by which unwanted large number of message travel in a network causing utilization of bandwidth and congestion in the network termed as Replay attack. Any message being transmitted from sender to receiver can be modified and then transmitted which leads to change in the source code and receiver may get wrong content termed as modification of messages attack. In most of the application server is responsible in providing different services to client associated with server. Attacker may block a particular service provided by server to client without giving idea to both server and client by which client will not be able to access any particular service causing malfunction of network termed as Denial if services(DoS).

4. Modbus Programming

Modbus is a protocol published by Modicon currently named as Schneider electric and is implemented on large scale on PLCs in which ladder programming is used. This protocol is an open source were we can modify the fields as per requirement. It consists of different object type such as coil, discrete input, input register and holding register which are programmed and initialized using C programming. Modbus protocol features are combined along with TCP working on transport layer to form Modbus/TCP which can be implemented in Ethernet standards. In this structure we have to design a system consisting of master and slave Modbus node which are connected with each other using RS 485 medium. Master in Modbus system is a brain that is controlling all devices which can read and write commands or instructions to slave devices. Configuration of files has to be done on c programming in which baud rate, loopback IP i.e local host and type of protocol is set. One of the library that can be used to establish and to send data to slave or field devices is libmodbus in C. By defining some of user defined function register or coil can be accessed directly to read the information using protocols.

For implementing Modbus protocol c language along with Golang can be used were Golang is a programming language developed google having some powerful tools. Modbus consist of Query-Response cycle were query consisting of device address, function code data and error check bits are provided to slave devices. In response to query response is given by slave consisting same above four parameters with device address of slave device [4].

Modbus master source code library (SCL) helps manufacturer and HMI vendors to implement Modbus code. Some of important parameters used in SCL are network, session number, slave number etc. Mainly Modbus consist of four kind of data types namely Coils, Discrete inputs, holding Registers and Input Register. Coils provide digital outputs with values 0 or 1. Discrete inputs data ca be only read but not written dependent on field inputs. Holding register stores analog values with size of two-byte value which also provides analog output so can read and written. Input register provides analog input so can be only read. For implementing master SCL some of files are required such as MBDefs.h, MBMaster.h ,MBDriver.c, MBFrames.c,MBLinkUser.h,MBlinkUser [5].

5. System working

In our proposed system we are creating master slave system with one master node and three slave nodes. These slave nodes are being placed on field to which sensor are connected such as temperature, humidity etc. These slave nodes are connected to master node using RS 485. The request or responses from master to slave or vice versa are carried using Modbus protocol. The format and commands for Modbus protocol coded using C language as discussed in above section. Also on master and slave nodes we are using PIC 32MX795F512H which is programmed using assembly language programing. As seen we are using a Modbus protocol to carry important information from field devices to master device through RS 485 standards. As discussed in earlier session number of attacks are present which can effect working of system and cause failure in system. Some attacks may have modified the data being transmitted while some can enter in system using false identity but overall effect is malfunction of the system. To prevent this, we have secure data transmission between both master and slave nodes.

6. Security system

Number of intrusion detection and prevention system are present in software industries but this not the case in industrial control systems (ICS). Depending on requirement it is needed to introduce intrusion detection and prevention methods in ICS to prevent and detect cyber-attacks. FPGA based devices can be introduced to prevent attacks and also can used in the systems were Modbus work with Modbus TCP/IP on Ethernet standards [6].

To avoid cyber-attacks and prevent / detect attacks 50 SNORT based signature based intrusion detection rules are defined. Some of the parameters used by SNORT are network traffic logs, analyse network traffic, alert server regarding suspicious activity. Above 50 rules defined based on reading exception, diagnostics, read and write file record are in non-proprietary format [6].

In some of industrial application authenticated Modbus protocol is used were it is authenticated at master before execution of commands which is not secured as some invalid commands may be executed at slave end. Some of attacks are present were it removes the authority to authenticate the Modbus command. Also some of the attacks disable the capability to defend wrong commands at slave node which can cause the system to collapse. Also it is required to authenticate the commands moving from slave end to master node else the message can be modified are wrong readings can be given to master node. So cryptography tool should be implemented both at master and slave node [7].

Some of common attacks in industrial systems are denial of service, response injection, command injection and reconnaissance attacks. Modbus devices has different configuration settings make devices work in listen mode, to restart the devices in remotely, and also to clear the contents. In industrial applications network stack is developed for Modbus MTU and RTU devices but are not able to handle malformed communication traffic. In such cases Snort is a software used to monitor and analyse the Modbus traffic. This software can be installed and executed on regular PC as well as on single board industrial computers which act as a barrier and helps to detect and prevent attacks on the system [8].

In some cases, attacks are grouped into three categories namely attacks effecting Modbus protocol, second on vendor and third on infrastructure. Considering the fact, it has identified total 20 serial and 28 TCP attacks. These intruders may harm the system if authentication is not present. To protect the Modbus protocol cryptographic tools are used such as hash chain using hash function. Also during design of this storage system storage of system is taken into consideration such that low memory space is required. Two cases are present were in one case fake device act as a master to issue improper commands to slave and second were attacker captures the slave device to read all the data. In one of the above case symmetric encryption is used and in other case public key/asymmetric method is used. In this method m hash chains are used for each slave device such that less slave devices are used [9].

Modbus is basically not designed to provide security and also no inbuilt security algorithms are present. To avoid the malfunction and te design the cryptosystem first it is important to detect the attack were some anomaly based detection algorithm and signature based threshold module are used to detect the flooding attacks. Signature based methods have accuracy were as anomaly based methods have a delay. In flooding attacks are extra packets are inserted in communication channel to create a congestion which destroys the functioning of system [10].

uBUS is associated with Modbus which brings some advanced features for embedded applications. During its application security is also taken care by using RSA algorithm. It uses asymmetric encryption which are implemented on various types of microcontrollers implementing uBus slaves. Address space in uBUS is extended from 247 to 4079 slave address. To control the effects of attack secure layer using asynchronous encryption is introduced in which RSA cipher is used and as the processing time of algorithm is less the keys used for encryption can be periodically changed. Increase in size of key increases security level Considering the time factor STM32-CRYP-LIB library are used to implement cryptographic algorithm [11].

Secured industrial communication protocol (Modbus S protocol) is designed based on original Modbus TCP protocol which uses symmetric method to make data secure based on hash algorithm and digital signature. The filtering mechanism used is white list to avoid damage of all the function codes used in above protocol. Some of the attacks considered are replay attack, tampering attack, eavesdropping attack etc. To test the above system windows 7 virtual machine, Modbus poll/slave simulation software and Modbus- S client server software developed by author are used [12].

As HMI systems are connected to internet on which Modbus protocol are used for data transmission the system gets more exposed to attacks in which one of the prominent attack is side channel attack. This paper describes even with encryption side channel attacks effects the communication system of TCP/IP running Modbus RTU. Mostly attacks take place were unpadded encryption with specific block cipher modes and stream cipher are used. In this system Modbus uses eight different function such as read coil status, read input status, read holding register etc. Still with appropriate measures such as padding namely round up and random padding effect of attacks can be reduced up to certain extent. Padding alters the actual size which provides uniformity in packets were roundup padding can be implemented on AES which may require block of smaller length were as random padding can be used in IPsec VPN and SSH. Thus looking after the results padding in many cases can reduce effect of side channel attacks [13].

Modbus since arrival has no confidentiality and data integrity so its not a secured protocol. So using it in real time application is dangerous and also same is the case for Modbus TCP/IP. Two attacks one infecting the master with malware and man in middle attack effects the working of the SCADA system and effect the data security in applications used. To see the effect experimental set up consisting of virtual machine running linux OS along with master and slave simulator is used. Virtual box used permits us to simulate a SCADA network and also develop

the attacks with no cost. After simulation master accepts incorrect information from slave so it is required that the channel between master and slave should be also secured. In future more attacks can be taken into consideration along with to investigate different detection schemes namely signature and anomaly based schemes [14].

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 [15].

In electric power companies were switching modules are used Modbus protocol is used at common interface. Modbus here is used as one of the common interface for systems at power plant. For encryption of data that is sent from master to slave diffie - hellman protocol is used by which data is transmitted in encapsulated form. Due to this man un middle attack is avoided. Modbus uses transport layer security protocol for authentication were it assigns a certificate with a public key were server has private key to check validity. Often used asymmetric algorithms are RSA, RC4 or AES. As discussed for end to end transmission diffiehellman protocol is used in which keys are not shared between two devices but are generated at both ends separately so that security of keys are maintained [16].

7. Conclusion

As discussed in this paper Modbus has a wide range of applications in industrial field. But as it's a communication system and data gets travelled from one point to other possibility of attacks takes place namely both active and passive. In our system as sensor nodes are located far away from master nodes are data is carried using RS 485 physical standard data should be encrypted and then transferred so that possibility of reading the data and its manipulation is avoided. For this task we can use symmetric method or asymmetric which includes in our future work. We have to study different types of cryptographic tools and then implement it on our hardware to secure data transmission from master to sensor node..

References

1. Niv Goldenberg and AvishaiWool,"Accurate Modeling of Modbus/TCP for Intrusion Detection in SCADA Systems" School of Electrical Engineering, Tel Aviv University, January 4, 2013.
2. Shafiullah Khan, Noor Mast, Kok-Keong Loo, Ayesha Salahuddin, "Passive Security Threats and Consequences in IEEE 802.11 Wireless Mesh Networks" International Journal of Digital Content Technology and its Application Vol. 2 No 3 , December 2008.
3. Tianbo Lu1, Pan Gao, Lingling Zhao,
4. , Yang Li and WanJiang Han.
5. https://aranair.github.io
6. Modbus master source code library, User manual.
7. Thomas H. Morris ,Rayford B. Vaughn and Elena Sitnikova " Advances in the Protection of Critical Infrastructure by Improvement in Industrial Control System Security", CRPIT Volume 138 - Information Security 2013, Adelaide, Australia.
8. Raphael C.-W. Phan, "Authenticated Modbus Protocol for Critical Infrastructure Protection" , IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 27, NO. 3, JULY 2012.
9. Thomas Morris , Rayford Vaughn and YoginderDandass," A Retrofit Network Intrusion Detection System for MODBUS RTU and ASCII Industrial Control Systems", 2012 45th Hawaii International Conference on System Sciences.
10. Gen-Yih Liao, Yu-Jen Chen, Wen-Chung Lu, and Tsung-Chieh Cheng, "Towards Authenticating the Master in the Modbus Protocol", Taiwan Institute of Nuclear Energy Research under Grant 962001INER007.
11. Sajal Bhatia Nishchal Kush Chris Djamaludin James Akande," Practical Modbus Flooding Attack and Detection", Proceedings of the Twelfth Australasian Information Security Conference (AISC 2014), Auckland, New Zealand.
12. JurajDudak, Gabriel Gaspar, Stefan Sedivy, Peter Fabo, LubomirPepucha and PavolTanuska, " Serial Communication Protocol with Enhanced Properties - Securing Communication Layer for Smart Sensors Applications" JOURNAL OF SENSORS, 2018.
13. Luo Xuan, Li Yongzhong, " Research and Implementation of Modbus TCP Security Enhancement Protocol" Journal of Physics: Conf. Series 1213 (2019).

14. NikolaosTsalis, George Stergiopoulos, EvangelosBitsikas,DimitrisGritzalis and Theodore Apostolopoulos , " Side Channel Attacks over Encrypted TCP/IP Modbus Reveal Functionality Leaks", International Joint Conference on e-Business and Telecommunications (ICETE 2018).
15. Christopher Parian, Terry Guldimann, Sajal Bhatia, "Fooling the Master: Exploiting Weaknesses in the Modbus Protocol", Third International Conference on Computing and Network Communications (CoCoNet'19).
16. George Stergiopoulos, Nick Kapetanas, EfstratiosVasilellis, Dimitris Gritzalis," Leaking supervisory controls and data acquisition commands over unpadded TCP/IP encryption through differential packet size analysis", 2019 John Wiley & Sons, Ltd.
17. F R Ametov, E A Bekirov and M MAsanov, "Organizing the information security in Modbus TCP interfaces for use in the energy complex", ICES 2020.