IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 18, Issue 4, Ser. I (July. – August. 2023), PP 26-32
www.iosrjournals.org

Cryptography Security Against Instrusion In Automation Protocol

Dr Sameer S Nagtilak
Department of E&TC
KITs College of Engineering(Autonomous)
Kolhapur, India

Dr Sangeeta R Chougule
Department of E&TC
KITs College of Engineering(Autonomous)
Kolhapur, India

Abstract—
In big networks, security involves the authorization and authentication of data, which is controlled by the server. Firewall technology can be used so that the access to device can be only through one path which avoid unauthorized access but it may have limitation to block worms or Trojans. In such cases we can use antivirus to avoid unauthorized access. Chance may be also to attack the data or codes which are been transmitted from master to sensor nodes. Communication between sensor and master node can be secured using different encryption methods.Currently intrusion detection and intrusion prevention systems are often found in number of software application compulsory, but this is not the case in industrial control systems. It is very much difficult to detect and prevent software attacks such as denial of service, response injection, command injection, and reconnaissance attacks which are known attacks for serial port based industrial control systems. Mostly such attack damage the communication between remote devices and master terminal or human machine interface.

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

Date of Submission: 01-08-2023 Date of Acceptance: 10-08-2023

I. INTRODUCTION

Sensors are one of the influential elements in communication technology. Internet of things (IOT) field is emerging in numbers of industrial applications, in which data transfers takes place between number of sensors and actuators. Communication medium is an important parameter to connect different sensors. Computer networks along with IoT plays a crucial role during setting up physical infrastructure for data transfer between end devices. Large number of intrusions are currently existing which are perilous to existing data transfer methods. Various protocols such as Modbus, Profibus, CANBUS along with merging with OSI layer protocols such as Ethernet, TCP/IP are the backbone of data transfer in various applications [1].

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. ATTACKS

Data security is an important concern during transmission through communication in various application using different protocols. Types of attacks vary in concern with the approach of an attacker towards the data. In some of the applications data is just observe during transmission by the attacker which is termed as passive attacks. In other case data is modified during its transmission by the attacker which is termed as active

attack [2]. Also in some of the application a particular service of the node or end device is block by which the node or sensor cannot access to a particular service which is termed as denial of service. Automation sector consists of four major elements such as Programmable logic controller (PLC), SCADA, Remote terminal unit (RTU) and intelligent electronic device (IED).
Protocol structures used in above elements can be modified to change its content, flag representation which can damage the functioning of system.

Other type of network attack is password based attack were password of device or system is hacked by third party to gain access of the network or device by which he can create false identity and send false messages to the end devices or sensor through the communication channel. IP address is one of unique identity provided by network to device in the network also which gets change when the device changes the network [3]. It is basically used for identifying the devices which include both host id and network id. IP address is hidden into new packet which consist of false IP address by which original identity is lost which is termed as IP spoofing. Spammers mostly modify the IP address to damage the proper functioning of the network. Attackers some time pretend that it is a part of the system and tries to retrieve the information of network using IP spoofing. Currently to detect IP spoofing attack most of the algorithm take help of internet service provider as it consists of database of all IP address. Google Map application program is used to get the location of the hackers.

For weak systems the possibility of more attacks takes place for which security technology needs to be increased. Firewall based on Modbus/TCP combined together with white list policy along with deep packet technology is used on Linux platform [4]. White list is set of rules used in industrial application used to reduced load on firewalls. Still some automation protocols exits were the security system are not yet present mostly in automation fields. In some case concept has been suggested but not yet implemented of hardware circuit or in practical applications. Some of the attacks are categorized in different parts stated below:

A. Common network attacks

Intruders or attackers may enter into system or channel were protocols are implemented in different ways. If we only focus on end devices or sensor, it is not feasible as these are not the only at two end devices were attacker attacks. Communication channel is also one of the points where attacker can attack to disturb the proper functioning of the network. Also as an unauthorized user access the channel it can send false command and response to master and client devices respectively.

B. SCADA and PLC attacks

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. Considering the above fact different protocols can be used in automation fields such as Modbus, Canbus, Profibus etc. As industry application are increasing on large scale using Modbus protocol the possibility of attacks is also increasing which can cause damage to the network. Some of major attacks are man in middle (MIM), Denial of service and Masqurade [5].

C. Softeware attacks

Apart from security algorithms which are to be developed based on the attacks present in the system we have to take care of some basic things and do some best practices in the network so that amount of intruders is reduced. So of the best practices are as follows:

1) Seggregation of network:

In large organizations large machine are used at each floor. Instead of creating a large network in a single organization we can create a small networks based on an application called LAN. Also if some of the attacks leads to the congestion in network we can customize the network bandwidth based on the need of application. Due to segregation on the large network into networks controlling the traffic in also easy.

2) Proxy Server

It acts as an intermediate among client devices and master device. It decides what to block and what to permit between two devices with respect to applications and programs. Without checking the authentication of user the access to the system is blocked. All the request is first processed through the proxy server which is also used as master.

3) Placement

Firewall are to be placed at every nodes and interconnection junction and also at edges of the network. If it is difficult to configure firewall at each and every node, then in this case we can use in built security. If security devices are placed at correct position at least whole network will not be affected by intruders

III. AUTOMATION APPLICATIONS

Automation sector along with computing methods has wide range of application which involves large number of sensor nodes, IOT concepts etc. These applications are spread widely in different industrial sectors such as energy sector, power sector etc. Some of the applications are listed below:

A. Energy sector

- Water saving irrigation applications is one of an important application were Modbus protocol is used along with TCP/IP for water saving.
- Transport traffic monitoring is one of an application were abnormal behavior of the traffic has to be detected through traffic patterns using Modbus TCP connections.
- It is also used in large number of application were temperature sensors are connected in entire building to predict the future changes in temperature.

B. Automation sector

- Transport traffic monitoring used to observe irregular behavior of the traffic has using Modbus TCP connections were data has to be monitored continuously and should be kept secured.
- IoT uses Modbus protocol to manage local interface to connect electronic devices. Modbus in Iot act as a fieldbus standard were at transport layer Modbus RTU type is used and at physical layer RS-485 is used
- Applications consist of cortex, 32- bit ARM processor that provides communication between master and slave using RS 485 in two ASCII and RTU mode.
- Modbus is also used at SCADA workstation and smart SCADA supervisory computers. Also in future it can be used over iOS so that range of application is increased.

IV. SECURITY REQUIREMENTS

IDS studies in detail automation protocol packets such as Modbus, Canbus, Profibus etc. to produces detail analysis of traffic which shows any problems occurring such as out of order packets, pattern changes in packets etc. IDS is tested on system in which 70% of PLCs has been observed a perfect match in traffic received. It is required as the network components do not verify identity and permissions i.e. authentication and authorization when data transfer takes place between nodes. Attackers may enter into various automation protocol to damage the message format so security system has to be designed for various automation applications [6].

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 [7].

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.

For security of data intrusion detection system rules are introduced for Modbus protocol on serial communication. While defining the rules possible attacks are also considered such as both active and passive attacks. Total 50 signature based rules are defined over serial communication. These kind of IDS rules are also required other industrial communication protocol such as CANBUS, Profibus. Automation protocols are used in power system application where possibility of attacks is at large number as no security algorithms are used. If authentication is not used an intruder harms the system by using some malicious commands. Some cryptographic tools are to be used for authenticity of protocol by which it is difficult for attacker to modify the commands issued in format of Modbus protocol. For this cryptographic tools hash chain concept is used by

which low memory space is required.A secure hash function with one-way property SHA-256 provides good efficiency. It avoids two conditions one where attacker fakes a master and send wrong commands by which end device may not work properly, second attacker may attack slave device to read all the important data stored [8].

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.

Cryptography is an absolute mechanism for client server architecture by which Modbus protocol is made more secured in application of IT infrastructure. SCADA communication uses protocol such as modbus, Canbus, Profibus to exchange data between field devices and other SCADA applications such as HMI. To provides security, security development module or security bytes is added at start of Modbus TCP/IP frame. In message unicasting three algorithms are discussed such as AES, RSA and SHA 2 in which authentication, integrity, confidentiality is verified. Considering number of keys asymmetric is inappropriate for broadcast messages. Only the case is certificate authority are not used in this study which has to be considered. To study security performance testbed is used normal flow of data is disturbing during transmission of Modbus message. Thus security is increased in SCADA applications [9].

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 [10]. 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 [11].

V. LIMITITAIONS

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 are used and are effective to monitor serial port in ICS. Some of intrusion detection schemes have been introduced for ICS but correction methodology or schemes are not yet given. Out of number of efforts made event oriented cyber physical fusion method (ECPF) is one of the method used to detect attacks in application such as smart grid. In this method, Snort is used to detect abnormal activities in network parameters in which the false measurement is identified using largest normalized residual test (Rn test). ECPF is thus a one of the method to detect intrusion but not prevention or correction [12].

For security of data intrusion detection system rules are introduced for automation protocol on serial communication. While defining the rules possible attacks are also considered such as both active and passive attacks. Total 50 signature based rules are defined which can used to detect and prevent attacks on protocol over serial communication. The work to define 50 signature based rules to detect intrusion is only the half of the part, because to transfer the data even after detection of intrusion we cannot stop it as system will collapse, for which we have to secure data before transmission so that it will be not affected by intruders.

Authentication to the whole system is important as even if master sends commands to client authentication will be only checked at client end. Intruders may attack the channel and false master may originate to issue false commands to client device. Also it might be case that no command is issued to client and so it will provide no response. But the intruder may send false command to master which is not an authenticate command. In this case master feels that communication has been completed and client is unaware of the communication has took place due to which now both master and client/slave are now out of synchronization. Thus now future communication will be ended. Thus it is important not only to secure the devices but channel security is also important [13].

Bandwidth of the channel is one of the important aspect of network. Creating congestion or collision in network is also one of the role of an intruder. If the bandwidth of channel connecting master and slave in full delay are introduced and also can lead to congestion. One of the reason of above thing is unwanted data in the channel. Intruder may generate large number of unwanted commands between master and slave which are actually of no use to disturb the normal operation of the network. These are termed as flooding attacks. Some signature based detection algorithms are used to detect the flooding attacks but still detection is only half of the part correction and preventive measure is also important. Above detection rules are applied on ICS and successfully detect the flooding attack but has not corrected the flooding attack.

Large number of information can gather by the intruders from a channel and used it to attack on the system which is termed as side channel attack in which packet timing and sizes are the factors. These side channel attacks take place on encrypted data to identify VoIP, web pages etc. These side channel attacks also affect ICS. By using round up padding and random padding effect of this attack can be reduced up to extent on system which changes actual size of original packet in network. But it has not been tested on automation protocols and on any application using these protocols. Also one of the factor that has to be taken into consideration that due to padding method it can consume 1/3 of network bandwidth which may lead into congestion in the network and damage function and introduce delay during data transmission [14].

VI. PROPOSAL

As seen we come to know that the security is not given importance in automation industries were protocols such as modbus, profibus, canbus are used. As in Automation field data is having various applications which also control various sensors and actuators in industries, data should be also securely transmitted because if it is modified then whole network can damage. So to secure data against various attacks we have to develop algorithms to transmit the data in a secured manner from master to sensor node. In Industries were automation are used in large scale we use SCADA, PLCs in large amount. In system control signals are transferred in large amount between nodes. Such system uses registered communication networks to transfer the data between nodes. Very important data is moving between devices in network [15]. The existing network currently lacks to provide protection, reliability and security for data transfer between the nodes. The information signals are critical between central control system and power stations. The network currently used for SCADA, PLCs does not provide protection, reliability and security for data transfer between the nodes.

VII. CONCLUSION

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. In future we can enhance the combination of automation protocols with TCP/IP to implement it on Ethernet network..

REFERENCES

[1] Pal Varga, Sandor Plosz, Gabor Soos, Csabahegedus, (2017), "Security Threats And Issues In Automation Iot" IEEE 13th International Workshop On Factory Communication Systems (WFCS).

[2] Thomas H. Morris, Rayford B. Vaughn, Elena Sitnikova,(2013) "Advances In The Protection Of Critical Infrastructure By Improvement In Industrial Control System Security" Proceedings Of The Eleventh Australasian Information Security Conference (AISC 2013), Adelaide, Australia

[3] Mohan V. Pawar ,Anuradha J,(2015) "Network Security And Types Of Attacks In Network" International Conference On Intelligent Computing, Communication & Convergence, Procedia Computer Science 48 (2015) 503 – 506.

[4] Thomas H. Morris, Bryan A. Jones, Rayford B. Vaughn, Yoginder S. Dandass, "Deterministic Intrusion Detection Rules For MODBUS Protocols", 2013 46th Hawaii International Conference On System Sciences.

[5] 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.

[6] Yingjuan ZHAO, Jingnan MA, Shaojuanli,Jia,"Design Of Modbus Wireless Communication System Based On Remote Data Transmission" International Forum On Mechanical, Control And Automation (IFMCA 2016).

[7] Mohsin A. Bandi, Mr. Naimesh B. Mehta, "Universal Controller Design Using Arm Controller", International Journal Of Engineering Trends And Technology- Volume3Issue2- 2012.

[8] Umesh Goyal, Gaurav Khurana, "Implementing MOD Bus And CAN Bus Protocol Conversion Interface", International Journal Of Engineering Trends And Technology (IJETT) - Volume4Issue4- April 2013.
[9] Shashi Raj K, Nayana D K, S Smanvi, "Modbus Based Greenhouse Monitoring And Control", International Conference On Computing And Control Engineering (ICCCE 2012), 12 & 13 April, 2012.
[10] 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.
[11] Niv Goldenberg And Avishai Wool, "Accurate Modeling Of Modbus/TCP For Intrusion Detection In SCADA Systems" School Of Electrical Engineering, Tel Aviv University, January 4, 2013.
[12] Thomas H. Morris, Bryan A. Jones, Rayford B. Vaughn, Yoginder S. Dandass, "Deterministic Intrusion Detection Rules For MODBUS Protocols", 2013 46th Hawaii International Conference On System Sciences.
[13] 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.
[14] Aamirshahzad, Malreylee,Young-Keun Lee, Suntae Kim, Naixuexiong, Jae-Young Choi And Younghwa Cho, "Real Time MODBUS Transmissions And Cryptography Security Designs And Enhancements Of Protocol Sensitive Information", Symmetry 2015, 7, 1176-1210.
[15] Luo Xuan, Li Yongzhong, "Research And Implementation Of Modbus TCP Security Enhancement Protocol" Journal Of Physics: Conf. Series 1213 (2019).