International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 07 | July-2016 www.irjet.net p-ISSN: 2395-0072

Cyber Security Analysis of Substation Automation System

Aarsha Unni J[1] , Vinukumar A R[2], Shalu George K[3]

[1]*PG Scholar, Control Systems, Dept. of Electrical and Electronics Engineering, MarBaselios College of Engineering and Technology, Trivandrum, Kerala, India*

[2]*Scientist 'E', Control and Instrumentation Group, CDAC, Trivandrum, Kerala, India*

[3]*Assistant professor, Dept. of Electrical and Electronics Engineering, MarBaselios College of Engineering and Technology, Trivandrum, Kerala, India*

Abstract - *The automation of substation is increasing in the modern world. The implementation of SCADA system is necessary for Substation Automation (SA) systems. Generally Substation Automation Systems uses Intelligent Electronic devices (IED) for monitoring, control and protection of substation. Standard protocols used by the Substation Automation systems are IEC 60870-5-104, DNP, IEC 61850, IEC 60870-5-101. In this paper, Modbus protocol is used as communication protocol. Cyber attack is critical issue in SCADA systems. This paper deals with the monitoring of substation and cyber security analysis of SCADA systems.*

Key Words: **Substation Automation system, SCADA system, cyber security of SCADA system.**

1.INTRODUCTION

Electric power generation, distribution and transmission is a critical infrastructure in our society. In the modern world, power demand is at the peak level. In recent years, most of the substations are automated. Substation automation system is more reliable. Substation Automation is an interesting and challenging area and many researchers are working in this area. SCADA system plays an important role in electric power system. The information from SA system can improve the performance and aids the maintenance of the system.

Implementation of SCADA system in substation can perform monitoring, controlling and protection of substation. In SCADA implemented power grid, the power equipments, their communication and computers are interdependent. The measured data from substation equipments is communicated correctly with the help of SCADA systems. The main advantage of using SCADA system is that monitoring and controlling can be done easily and reduce the human labour. The measured value from substation is given to Remote Terminal Unit through wired cables. These values are communicated to the control center through the network provided.

Since the communication to the control center is with the help of network, there may cause cyber attack on the computer systems in the control center. This will surely affect the substation also. Mainly undesirable switching occurs. If attack entered through substation may change the setting of the relay or other equipments. Data are send from Remote Terminal Unit to control center as modbus packets. These packets may get captured. One attack is that the captured values is not send to the control center or may corrupt that data and corrupted data is send to the control center. Such security attacks occur in communication area are sniffing of data packets, ARP poisoning, man-in-the-middle attack etc. There are different types of cyber security in substation communication network. They are physical security and network security.

The organization of the rest of this paper can be summarized as follows. About SCADA system and its block diagram and its components is described in section II. Brief description about cyber security is provided in section III. Section IV describes about the description of the Substation automation system and how the monitoring is done. Conclusion of the work is described in section V. Its future work is mentioned in section VI.

2. SCADA SYSTEM

Supervisory Control and Data Acquisition (SCADA) systems are highly distributed systems. SACDA systems are used for the automation of industrial plant process. SCADA system is a type of Industrial Control System (ICS). SCADA systems are used for monitoring and control of plant process. It is a computer based system. Industrial Control System is a type of control system mainly used in industrial production. ICS includes SCADA system, Distributed Control System (DCS) and other small control system configuration such as PLC. Several industrial plants such as power, oil and gas, chemical, water, transport etc uses SCADA system for the monitoring and control.

A SCADA system consists of several components. Each component has different functions and is described as follows. Remote Terminal Unit (RTU) has hardware telemetry that has the ability to send data to supervisory system and also receive commands from supervisory system. Data collection is by connecting RTU to the process and convert sensor signal from process to digital data. Programmable Logic Controller (PLC) doesn't have hardware telemetry. The functionality of PLC is similar to that of RTU. RTUs or PLCs are commonly known as controllers. For connecting PLCs and RTUs with control center telemetry system is used. SCADA system uses wired as well as wireless telemetry system. Data

acquisition system collects data using standard protocol from field devices. Human Machine Interface (HMI) is a device or software that will present the data processed by the RTU. The main function of HMI is to monitor the process data and provide interaction with the system. A human operator can monitor the plant process using HMI. HMI will request and collect the data from data acquisition system. A supervisory system will receive data from plant process and send commands to the plant process. A communication system is there for connecting the supervisory system and Remote Terminal Unit.

Functions of SCADA systems are monitoring (collects data and sends it to computer in control center), control (gather data from monitoring sensors, process it and send back to equipment) and user interface functions (individuals can monitor SCADA input and output response in real time in control room). The block diagram of SCADA system is shown in Fig -1.

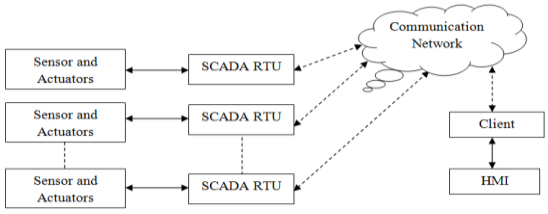

Fig -1: Block diagram of SCADA system

2.1 Remote Terminal Unit

SCADA systems mainly using RTU for achieving control functions. RTU is a microprocessor based device connected to sensors, transmitters or process equipment for the purpose of remote telemetry and control. An RTU can be interfaced using serial ports (RS232, RS482 and RS422) or Ethernet to communicate with central stations. It also supports various standard protocol such as Modbus, IEC 60870, DNP3 etc. An RTU hardware module includes control process and associated memory, analog inputs, analog outputs, counter inputs, digital inputs, digital outputs, communication interfaces and power supply [1].

In this paper, Modbus TCP/IP protocol is used in RTU simulator. Modbus is a serial communication protocol. It was developed by Modicon in 1979. It is a method for transmitting data over serial lines between electronic devices. Modbus network can have one master and several slaves. Each slave will have unique address for communication. Modbus provides communication between many devices which are connected to same network. Modbus provides communication over TCP/IP network. For communication, Modbus TCP requires IP address of the network. Any mismatch in IP will cancel the communication. The function of TCP is to assemble the data into modbus packets. IP will ensure that the messages are addressed correctly. TCP/IP is known as transport protocol.

Datatypes available in Modbus are coil (discrete output), discrete input, input register and holding register. Modbus communication mainly includes device address, function code, data and error checking field. Medium for transmission of messages are provided by TCP/IP.

Modbus works similar to a single serial cable connecting the serial ports of two devices. The data transmission between the devices is through the serial cable. Modbus transmits both analog and digital values. Implementation of Modbus is simple and flexible. Modbus is used by several industries.

2.2 Human Machine Interface

Human Machine Interface provides information of the plant process to an operator. HMI is a part of SCADA system. Human Machine interaction is capable using HMI. HMI permits users to interact with machines for controlling the device. HMI is also known as Man Machine Interface (MMI). There are mainly two types of interactions. They are human to machine and machine to human. Interactions will be realistic and natural if the HMI is good. The advantages of using HMI are error reduction, improved reliability and maintainability, increased comfort for user etc.

3. CYBER SECURITY

The cyber attack on SCDA systems was rare but it is now increasing. The cyber security on real time systems and SCADA systems are facing challenges in the modern world. Cyber security mainly focuses on the protection of computer, programs, networks and data from unauthorized access, change or destruction. It is also known as information technology security. Study on stuxnet reported that changes in controller logic causes the rapid speed up and speed down of centrifuges.

Critical infrastructure has three types layer. They are physical layer, cyber layer and human operations layer. In early days, the layers vulnerable to attack are physical and human operation layer. Now the vulnerability is increased in cyber layer. Main core principles of cyber security are confidentiality, integrity and availability. An intentional violation of a security objective is a called attack. Attacks may be initiated by the persons outside or by insiders. Common types of attacks are Denial of service, Eavesdropping, spoofing, man-in-the-middle, virus, worm etc[2].

Attacks in SCADA systems includes intentional targeted attacks, unintentional consequences caused by worms and viruses and unintentional raised by internal causes. As the

power system is controlled by SCADA system, the effect of cyber attack can be analyzed on SCADA system.[3]

The most important element of cyber security is the software. There are two types of attacks that leads to loss of information and damage the equipments. They are direct attack and intelligent attack. Direct attack may cause loss of load in power system. Intelligent attack is a well planned attack.[4]

4. SYSTEM DESCRIPTION

This paper describes the monitoring of Substation Automation system. For that, there are mainly three steps required. They are simulation of substation, RTU simulator and HMI. Since it is not done in real substation, there is need of simulating substation and RTU. Implementation of control center is done using HMI. For designing HMI, an open source software is used and it is "IndigoSCADA". The overall process is done in this paper is represented by using a block diagram shown in Fig -2. Plant process, RTU simulator and HMI are running in three different computers with different IP. It is tested in a test environment. The substation is simulated using Matlab. The components in substation are converted as its mathematical equations and using matlab script each component is coded. Each component is written as a function and in the main function each sub-function is called according to the need. Graphical user interface is also incorporated with matlab for the visualization of the plant. The substation is simulated and the values are obtained.

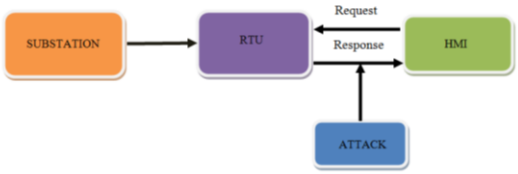

Fig -2: Overall process

These obtained values from matlab are send to the RTU simulator. The RTU receives the data as signal and converting these data as mobdus packets and send to the HMI. Since the protocol used by RTU simulator is modbus. The HMI receives the data from RTU simulator and is displayed in HMI screen. In the designing of HMI, 10 tag points are used. RTU sends both analog and digital signals and are received by HMI. Corresponding to each tag point in HMI, RTU simulator will send data. Matlab simulator will send data to RTU corresponding to the tag value in HMI. The port specified for modbus protocol for communication is 502. Therefore HMI is listening to the port 502. RTU simulator will send data to HMI through the port 502. The HMI is shown in Fig -3. With the help of HMI, the monitoring of substation can be done easily.

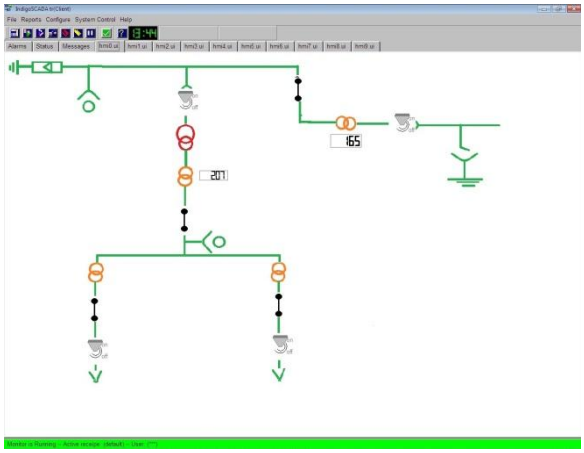

Fig -3: Monitoring of Substation using HMI

This paper deals with the cyber attack occur in the communication between RTU and HMI and cyber security analysis. Some cyber attacks that may occur in between RTU and HMI are sniffing of data packets, identification and analyzing of SCADA protocol, ARP poisoning, man-in-the-middle attack etc. Any eavesdropping on existing traffic is called as sniffing. Packet sniffing captures data when it is transmitted over a network. In this paper, the data between RTU and HMI is captured using Wireshark. By sniffing data, the communication between network can be captured. These data can be analyzed. From the analysis, the devices that communicates more can be identified and also the type of protocol can also be identified. By detailed analysis more information about the data is obtained.

The information of the targeted IP is obtained from the above analyzing. By setting these IP address as targets then the data transfer between RTU and HMI can be obtained. Address Resolution Protocol poisoning is a type of attack in which an attacker changes the Media Access Control (MAC) address and attacks on an Ethernet LAN by changing the target computers ARP cache with a forged ARP request and reply packets. An effective ARP poisoning attempt is undetectable to the user. Man-in-the-middle is a type of attack where the attacker secretly alters the communication between two parties but they strongly believe that they are communicating each other. The attacker captures the data and rewrite it and send back. But the communicating parties are unaware of the attacker. The captured data can also be dropped so that the HMI will not get the data. It can be done using ettercap software.

5. CONCLUSIONS

In this paper substation monitoring is done using HMI. By continuous monitoring, the protection of substation is guaranteed. By using HMI, the concept of control center is cleared. Cyber security analysis is done. Identified possible attack in communication between RTU and HMI and is

analysed. Controlling of substation can be done as future work.

REFERENCES

[1] Francis Enejo Idachaba and Ayobami Ogunrinde, "Review of Remote Terminal Unit (RTU) and Gateways for Digital Oilfield deployments," International Journal of Advanced Computer Science and Applications, vol.3, No.8, 2012.

[2] Maurilio Pereira Coutinho, Germano Lambert-Torres, Luiz Eduardo Borges da Silva, "Attack and Fault Identification in Electric Power Control Systems: An Approach to Improve the Security," IEEE in Power Technology, 2007.

[3] Yichi Zhang, Lingfeng Wang, Weiqing Sun, "Investigating the Impact of Cyber Attacks on Power System Reliability," Proceedings of the 2013 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, May 2013, Nanjing, China.

[4] Chee-Wooi Ten, Chen-Ching Liu, Manimaran Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA systems," To appear in IEEE in Power System.

[5] Chetan S. Kulkani, Narendran Mannazhi, "Substation Automation System for 33/66kV S/S at North Delhi Power Limted," 2006 IEEE PES Transmission and Distribution Conference and Exposition Latin America, 2006, Venezuela.

[6] Vinuta V Koluragi, "A Case Study on SCADA Implementation in 220 kV Substation," International Journal for Research in Emerging Science and Technology, vol.2, July 2015.

[7] Ralph Mackiewicz, "Technical Overview and Benefits of the IEC 61850 Standard for Substation Automation," 2006, USA.