Detecting Flooding Attacks in Communication Protocol of Industrial Control Systems

Rajesh L[1]
Research Scholar, Department of Electronics and
Communications, Koneru Lakshmaiah Education
Foundation, Vaddeswaram, Vijayawada
Andhra Pradesh, India

Penke Satyanarayana[2]
Professor, Department of Electronics and Communications
Koneru Lakshmaiah Education Foundation
Vaddeswaram, Vijayawada
Andhra Pradesh, India

***Abstract*—Industrial Control Systems (ICS) are normally using for monitoring and controlling various process plants like Oil & Gas refineries, Nuclear reactors, Power generation and transmission, various chemical plants etc., in the world. MODBUS is the most widely used communication protocol in these ICS systems, which is using for bi-directional data transfer of sensor data between data acquisition servers and Intelligent Electronic Devices (IED) like Programmable Logic Controllers (PLC) or Remote Telemetry Unit (RTU). The security of ICS systems is a major concern in safe and secure operations of these plants. This Modbus protocol is more vulnerable to cyber security attacks because security measures were not considered in mind at the time of protocol design. Denial-of-Service (DoS) attack or flooding attack is one of the prominent attacks for MODBUS, which affects the availability of the control system. In this paper, a new method was proposed, to detect user application-level flooding or DoS attacks and triggers alarm annunciator and displays suitable alarms in Supervisory Control and Data Acquisition system (SCADA) to draw the attention of administrators or engineers to take corrective action. This method detected highest percentage of attacks with less time compared to other methods. This method also considered all types of conditions, which triggers flooding attack in MODBUS protocol.**

Keywords*—Supervisory Control and Data Acquisition (SCADA); Remote Telemetry Unit (RTU); Programmable Logic Controllers (PLC); Communication Protocol; MODBUS; Industrial Control Systems (ICS)

I. Introduction

Industrial Control Systems (ICS) or Process Control Systems (PCS) are generally using for monitoring the field or process from a centralized location and control the field equipment to run the operations. Some of the examples of the industrial control systems using are oil and gas refineries, process and chemical plants, nuclear power plants, power generation and transportation [1]. The National Critical Infrastructure sectors are mainly depending on these ICS systems. The sectors which are very crucial for any country development in economy, social, technology are defined as National Critical Infrastructure [2].

Earlier these systems were confined to control room where all types of operations are taking place. But now-a-days these systems are connecting to internet, corporate networks to transfer the data to higher layer functionalities to meet corporate requirements like ERP, DMS and 3rd party services. Even though the connectivity of ICS systems to upper layers achieves the data sharing, but these systems are also opens doors to security attacks to destruct the functionality and country growth. It is required to protect these systems from cyber-attacks [3-4].

The Industrial Control Systems are connected to corporate networks and internet for sharing of SCADA data to 3rd party systems, taking remote for debugging and maintenance of the systems. This leads to security attacks and these systems are vulnerable to these cyber-attacks [5]. The Computer Emergency Response Team (CERT), an expert group that handles computer security incidents reports that the number cyber-attacks on ICS systems are increasing every year. These systems should be protected from security attacks for safe and secure operations of national critical infrastructures, where ICS systems play a vital role [6]. The number of cyber-attacks incidents during last 5 years was displayed in bar chart as shown in Fig. 1.

The security measures, which are suitable for Information and communications technology (ICT) systems, are not appropriate for ICS security because of their distinct purpose and functionality. There are areas of ICS systems where attacks may take place like network, computer hardware, controllers, interfaces etc [7]. The communication protocol, which is using for bi-directional data transfer between Data Acquisition Servers (DAQ) and Controllers, is one of the important areas where attacks are taking place. Modbus is most widely used communication protocol in ICS systems [8].

The field data from PLC will be transferred to SCADA Servers through communication protocols like Modbus, DNP etc. Modbus is a most widely used, open, application layer communication protocol for bidirectional data transfer between PLC and SCADA Servers. It is very simple and light weight communication protocol. It is based on simple request and reply message transfer [9]. The frame format of the Modbus protocol is shown in Figure 2. The SCADA Server sends the request to PLC and it will respond to the request and sends the response to the SCADA Server. If the request is valid then it will send valid response or if the request is not valid then it will respond with exception response [10]. The Modbus request frame contains device ID, function address, starting address, number of registers [11].

Modbus is lacking of security measures and suffering form number of security vulnerabilities. The Modbus protocol was designed without considering security in mind. There are number of vulnerabilities in Modbus protocol [12]. There is no checking of integrity, confidentiality, availability of this protocol [13]. The Modbus frame is very simple and knows to everyone because it is an open protocol. The frame is transferring in plain text without any encryption and checking integrity of the frame. There is no checking of authentication or authorization of master or target device. Any attacker which knows the IP address of PLC can send any command or any false command or response and can destroy the filed or process. Man-in-the middle attacks, replay attacks, Denial-of-Service (DoS) or flooding attack are some of the crucial attacks for Modbus protocol [12-13]. The Modbus is suffering from the following attacks [22]:

- There is no checking of authorization of source or target.
- There is no checking of authentication of connection.
- There is no checking of integrity of the frame. Anybody can change the content of the frame.
- The frame is transferring in plain text. Anybody can read the frame content.
- The attacker can seize the PLC.
- Replay attacks.
- Man-in-the middle attacks like false command injection, false response injection etc.

Denial-of-Service (DoS) or flooding attack is very crucial and had high impact on availability of the control system. The control system shall be available more than 99.95% for proper operations of the plant [14]. The PLC will be seized the control and cannot respond to the actual SCADA Server. The attacker can send malicious traffic to PLC and made the PLC busy with the flooding. The attacker can achieve this by sending SYNC packets continuously [15] or Internet Control Message Protocol (ICMP) packets or sending wrong Modbus requests at high rate.

In this paper, a new method was proposed to detect DoS or flooding attacks at user application level in Modbus protocol. Rest of the paper was described as follows: Section II describes the literature survey in this field. Section III explains the components of SCADA systems. The test set up used for this research was explained in Section IV. The proposed method, simulation of attacks and testing, detection of DoS attacks were described in Sections V & VI. The results of the testing and future work was explained and discussed in Section VII. The paper was concluded in Section VIII.

II. Literature Survey

The literature is available for security of industrial control systems and vulnerabilities, security attacks of Modbus protocol. Number of scholars worked for enhancing the security of Modbus protocol. Rajesh L et al. [12] described list of possible attacks and existing literature on security of ICS systems and Modbus protocol. Peter Huitsing et al. [13] list out the common security attacks in Modbus protocol. Rajesh L et. al [14] described the importance of ICS system availability and proposed method to enhance it. DoS attack seized the control of PLC and affects the system availability. Rajesh Kalluri et al. [15] explained simulation and impact of DoS attacks on SCADA systems. They did not propose any solution. Alvaro A. et al. [16] explained the various possible security vulnerabilities in industrial control systems and also described the real incidents where cyber-attacks took place across the world and mentioned the importance of security of these ICS systems. Jason Stamp et al. [17] also described the possible vulnerabilities in industrial control systems.

Fovino et al. [18] proposed a method for enhancing the security of Modbus protocol with AES, RSA algorithms. But the frame was transferred in plain text and attackers can read the message. Aamir Shahzad, S.Musa et al. [19] proposed algorithm for security in multicasting communication of Modbus protocol. This method did not consider the delay in communication response. It mentioned only number of detected attacks in percentage. The performance parameters are not compared and discussed. The research scholars worked and provided solutions for Man-in-the middle attack, replay attacks etc. [20].

The DoS attack was very less addressed. Bhatia et al. [21] simulated flooding attack by DoS by sending false commands. They proposed detection of flooding attacks based on anomaly detection and signature-based detection by Snort tool. They did not mention how many attacks are simulated and % of detection. They also not considered the DoS attack, which stops the services of PLC.

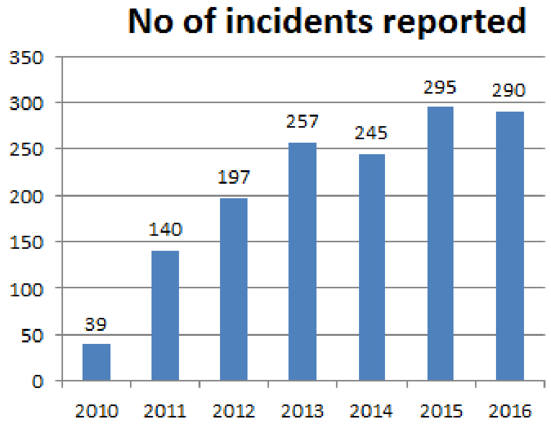


Fig. 1. Number of Incidents Reported by U.S. ICS-CERT (Ref: https://www.us-cert.gov/ics).

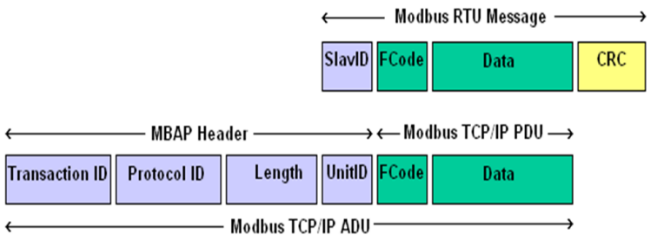


Fig. 2. MODBUS Frame Format.

From the literature review, it was concluded that Modbus protocol is suffering from security vulnerabilities, attackers could easily target this protocol. Some scholars provided solutions for some of these attacks, but DoS attack or flooding attack was not properly addressed for identification and detection, and it needs a solution or new method to properly detect the attack.

III. SCADA System Components

Any SCADA system mainly contains the following main components: [3].

- Sensors or field instruments.
- Programmable Logic Controllers (PLC) or Intelligent Electronics Devices (IED).
- Data Acquisition Servers, display work stations and other IT hardware components.
- Networking equipment.

A. Filed Instruments

Field instruments are basically transducers or sensors, used for measuring the field values like pressure, flow, density etc. These devices convert the physical quantity to electrical quantity and send the data to PLC/RTU. Monitoring and maintaining process variables at the appropriate levels is extremely critical in industrial automation and process control. A sensor in the industrial environment is either continuously or periodically measuring critical parameters such as density, temperature, pressure, flow, etc. The primary challenge of sensing in industrial environments is conditioning low signal levels in the presence of high noise and high-surge voltage.

B. RTU/PLC

Programmable Logic controller or Remote Telemetry Unit used for scanning the I/O and executing interlocks and logics for industry field operations. The basic units have a CPU (a computer processor) that is dedicated to run one program that monitors a series of different inputs and logically manipulates the outputs for the desired control. They are meant to be very flexible in how they can be programmed while also providing the advantages of high reliability compact and economical over traditional control systems. The I/O system provides the physical connection between the equipment and the RTU/PLC. The PLC/RTU will be connected to main SCADA Server though LAN or WAN. The PLC/RTU will have communication module for interfacing with SCADA Server through Serial or Ethernet communication.

C. DAQ Servers and IT Hardware

SCADA Server will be used for processing the received data from PLC/RTU and logging of the data for further future analysis. The Client will be used for display the data in different formats and sending the controls to PLC/RTU. SCADA package will be loaded in Server and protocol driver like Modbus, DNP will be running in this server. The main functionality of SCADA Servers is scanning the RTUs, time synchronization, database management, alarms triggering, report generation, control command execution etc.

D. Network Components

Network consists of Lan switches to connect the various nodes. Routers can also be used for WAN interface i.e to connect various stations. Redundancy is an important factor in SCADA networks. In pipeline applications the RTUs are geographically spread throughout the pipe line. Optical Fiber Communication will be used for bi-directional data transfer between main master station and RTUs.

The sensor data from field instruments will be collected by PLC or RTU. It will process the raw data and it transfers the data to centralized data acquisition system for further processing using suitable communication protocol like Modbus. Modbus protocol is suffering from security attacks and needs to protect the protocol. In next section, the test bench was described which is used in this research.

IV. Test Set up

A test bench was set up in our lab for performing the research and testing as shown in Fig. 3. Two computer systems, one number of Programmable Logic Controller (PLC) were connected in a local network through LAN switch. One of the computer systems were loaded with SCADA software and continuously polls the PLC to get the data or field values from the PLC. The Client component of Modbus protocol was loaded in SCADA Server and the server was polling the PLC through Modbus Protocol. The second system was loaded with Modbus simulator tool, which was used for simulating flooding attack for PLC in the network. The PLC was loaded with Modbus Server component, the developed software module to detect the attacks. The corresponding alarms were configured in SCADA MIMICs and trends. The suitable pop ups were created in SCADA system. The alarm annunciator was connected to PLC to trigger or energies the audible buzzer to draw the attention of engineers and operators in the control room.

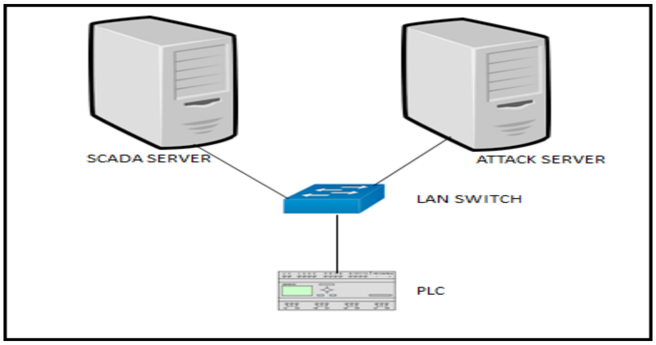


Fig. 3. Network Connectivity Diagram of Test Set up.

V. Proposed Method and Simulation of Flooding Attacks

The DoS attack by flooding PLC using Modbus protocol can be two types; first method is to stop the required services i.e., PLC not responding the legitimate requests from SCADA Server and other one is crashing the target and seizes the services i.e PLC was busy with responding attackers requests and denies the services from legitimate SCADA Server. It can be triggered by number of ways like sending more requests than pre-allocated maximum number of requests, sending wrong requests by making PLC busy, sending continuously SYNC packets or ICMP packets. In this set up the attack was triggered by sending the following cases:

1) By sending number of requests more than maximum pre-allocated in PLC Modbus driver.

2) By sending continuously correct Modbus requests at very high rate and.

3) By sending continuously wrong requests at high rate.

The above-mentioned attacks were simulated by second computer system, which was loaded with Modbus Master Simulator and configured to poll the PLC with arbitrary starting and number of registers continuously without any delay. The Modbus Master tool was configured with reading of coils, status, input registers and holding registers. Table-I displays the parameters configured in Modbus Slave tool.

TABLE. I. MODBUS REQUESTS SENDING TO PLC

Modbus ACTION	**Tag Parameters**		
	Function Code	***Starting address***	***Number of Registers***
Reading Coils	**1**	**1**	**10000**
Reading Status	**2**	**1**	**10000**
Reading Holding Registers	**3**	**1**	**2000**
Reading Input Registers	**4**	**1**	**2000**

An analog signal (PT) was simulated with ramp input in PLC logic and the same was received and plotted in SCADA mimic using Modbus protocol. The signal was started from 0 and incremented by 1 kg/cm2 for every one second in PLC memory registers. The simulation was done in PLC logic. The value was configured in trend for logging in SCADA system. The graph or trend plot was disturbed whenever the DoS attack was generated as shown in Fig. 4. Generally, the signal will be in saw tooth waveform if the system is continuously system available or non-presence of DoS attack. The PLC was not communicated with SCADA Server during DoS attack and the signal was not available at SCADA Server as well as mimic. In Fig. 4 it can be observed that the ramp signal is disturbed and it was flat for some time. The data is not available at SCADA Server during attack time interval because PLC was busy or not responding. DoS attack affects the system availability parameter.

The logic was also implemented for starting the pump to transfer the fluid between two Oil tanks. There are two tanks contains the Oil. The pump will start and the fluid will be transferring between tank A and tank B. Fig. 5 displays the flat curve of two tank levels after pump start and they did not resume the operation back. The PLC was not communicated back and it was out of control.

A digital output drive command was configured for start/stop the pump. Operator can give start/stop command from SCADA MMI to control the pump. The pump was started and the status was updated in SCADA. After launching of flooding attack, the stop command was sent. But PLC could not process the command because the PLC was busy in executing requests/commands from attacker. This was indicated in Fig. 6 In another experiment, the start command was sent and the pump was started at the field. The flooding attack was also triggered immediately after pump start command. The running status of pump was also reported to SCADA with delay of more than 5 sec. The same was observed in Fig.7.

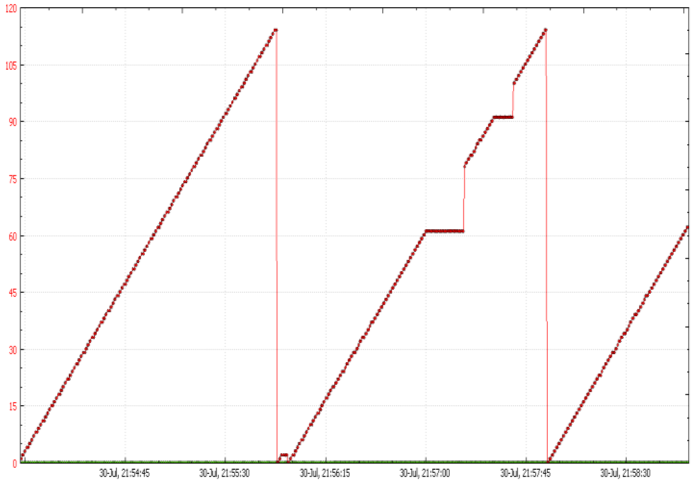


Fig. 4. DoS Attack Shown in SCADA Graph or Trend.

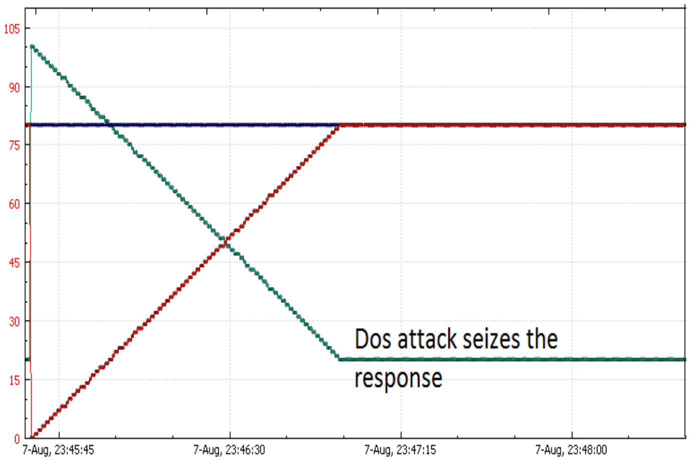


Fig. 5. DoS Attack Seized the Response from PLC.

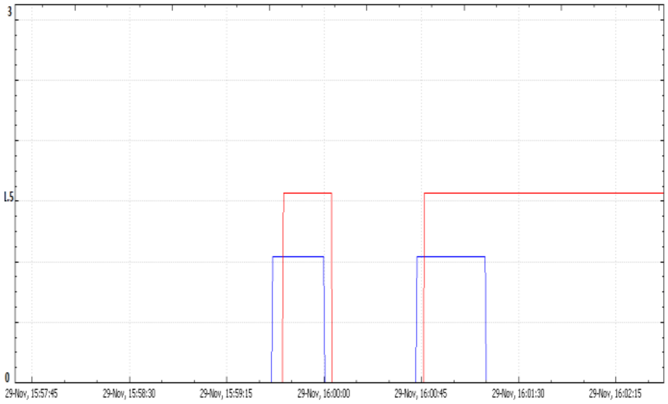


Fig. 6. Stop Command not Executed by PLC.

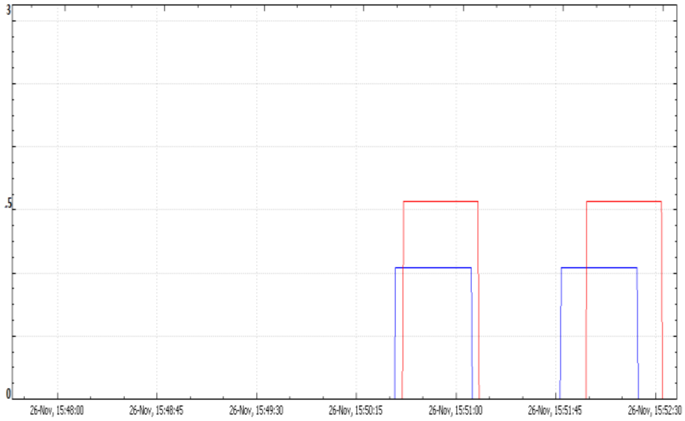


Fig. 7. Reporting of Pump Running Status at SCADA with Delay.

VI. Testing and Detection of DoS/Flooding Attacks

Whenever Modbus Master in SCADA system sent the Modbus request to PLC, the PLC saves the Modbus request parameters in registers or buffers based on these request parameters. SCADA server frames the Modbus requests and polls the PLC periodically. Therefore, PLC updates the starting address and number of registers to be polled, after one cycle of scanning. But it requires at least two cycles to update poll time interval. The buffer contains starting address, number of registers, function code, poll time interval and DoS attack recognition flag. Whenever the PLC receives the Modbus request from attackers, PLC checks the buffer values and detects that these values are not regular values and set the flooding attack recognition flag. If the flag is set, PLC drives a relay for annunciator, which is connected, to PLC. Whenever the PLC responds with exception response, the SCADA Server detects the same and received the flag and it triggers the pop up, generate alarm with audible sound to draw the attention of administrators or engineers that something was happened with PLC.

The PLC continuously monitor the Modbus request frame and stores the above request parameters like Function code, starting address, number of registers. Generally, the system was configured with required request blocks and the poll cycle is periodic with same parameters. The requests will be periodic with the same parameters for every scan. If any new request received with new parameters other than these stored parameters, PLC will set the DoS attack flag. If the PLC received wrong request and respond with exception response continuously more than three times, then also it sets the DoS attack flag. If the time duration between two consecutive Modbus requests is more than the saved values, then also it will trigger DoS flag. Generally, PLC will respond with correct response for Modbus request, but when it receives out of bound memory address or invalid memory address, it will send exception response. The suitable structure was defined in PLC for updating the parameters of Modbus requests.

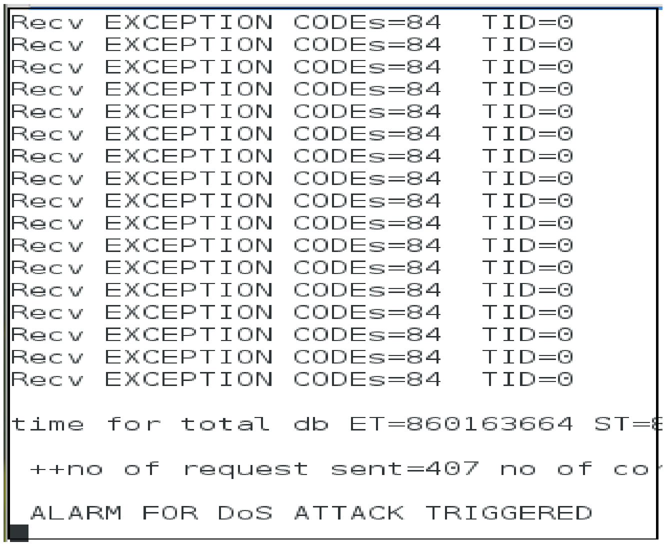
The module also checks the IP address of incoming requests and filters which are not authorized. The PLC stores the authorized IP addresses and allows or passes the requests from the configured IP addresses. The module also filters the queries which are not configured in PLC memory by checking the incoming Modbus request parameters by saved or configured parameters.

The PLC also maintains the same parameters in its memory. Generally, once the system is commissioned and using for operations continuously, there will not be any changes in Modbus Configuration. For testing purpose, the above scenario was simulated by changing starting register and number of registers and the PLC detects that the starting and ending address was not matching with saved values from periodic cycle and sets the flag. Whenever the PLC detects any change in above parameters, it sets the DoS flag and the bit was received by SCADA also. Then SCADA will trigger a pop up with suitable message and audible sound, logs into day event reports and suitable alarm in alarm page.

VII. Results and Discussion

The developed module is useful for detecting DoS or flooding attacks at user application level. The attacker can make the PLC busy with sending wrong or correct Modbus requests to PLC. During the attack, PLC will not respond to legitimate server and data is not available in ICS system.

The DoS attack was detected as shown in Fig. 8 as per above developed module. Fig. 8 displays that DoS attacks received and alarm was triggered at SCADA level. The exception response or no response was received from PLC in SCADA during the attack. The PLC detects the DoS attack as per our developed module, sets a flag in its memory, and can be transferred to Modbus. The SCADA system detects the flag after re-establish the communication with PLC and triggers the pop ups and alarms at SCADA level.



```
Recv EXCEPTION CODEs=84   TID=0
Recv EXCEPTION CODEs=84   TID=0
Recv EXCEPTION CODEs=84   TID=0
Recv EXCEPTION CODEs=84   TID=0
Recv EXCEPTION CODEs=84   TID=0
Recv EXCEPTION CODEs=84   TID=0
Recv EXCEPTION CODEs=84   TID=0
Recv EXCEPTION CODEs=84   TID=0
Recv EXCEPTION CODEs=84   TID=0
Recv EXCEPTION CODEs=84   TID=0
Recv EXCEPTION CODEs=84   TID=0
Recv EXCEPTION CODEs=84   TID=0
Recv EXCEPTION CODEs=84   TID=0
Recv EXCEPTION CODEs=84   TID=0
Recv EXCEPTION CODEs=84   TID=0
Recv EXCEPTION CODEs=84   TID=0
Recv EXCEPTION CODEs=84   TID=0

time for total db ET=860163664 ST=

 ++no of request sent=407 no of co

 ALARM FOR DoS ATTACK TRIGGERED
```

Fig. 8. DoS Attack was Detected in SCADA.

The proposed method was tested for 100 times by simulating DoS attacks by sending the following requests indicated in table 2, continuously as per the table and successfully detect 98 attacks within 5 sec. Two instances of Modbus Clients were configured and connected to PLC. Client 1 was configured with the parameters as shown table and polls for every 10 msec. Client 2 was configured with different parameters and polls for every 1 msec. Table 2 shows one instance of Modbus request parameters for client 1 and client 2. The parameters were changed for every trail and results are recorded. The method was successfully detected 98% attacks. This method offers highest % of detection of attacks with less time compared to other methods. This method also simulated all types of conditions by which flooding attack or DoS attack can trigger. Audible buzzer was energized whenever the attack was detected. Suitable pop ups and alarms were also displayed in SCADA mimic.

TABLE. II. MODBUS REQUESTS SENT TO PLC BY MODBUS CLIENTS

MODBUS CLIENT-1	**For every 10 msec**		
	Function Code	***Starting address***	***Number of Registers***
MODBUS requests by Modbus Client 1	**1**	**1**	**10000**
	2	**1**	**10000**
	3	**1**	**2000**
	4	**1**	**2000**
MODBUS CLIENT-2	**For every 1 msec**		
	Function Code	***Starting address***	***Number of Registers***
MODBUS requests by Modbus Client 2	**1**	**5000**	**5000**
	2	**5000**	**5000**
	3	**2000**	**5000**
	4	**2000**	**5000**

VIII. CONCLUSION AND FUTURE WORK

Industrial Control Systems plays a vital role in National Critical Infrastructures. MODBUS Protocol is most widely used communication protocol in industrial control systems. The protocol is more vulnerable to security attacks and it needs to protect the system. Modbus is prone to number of security attacks because it was designed without security measures. Daniel of Service (DoS) attack is one of the important attacks which affect the availability of the control system. In this paper, a different method was proposed to detect application level flooding or DoS attack in Modbus protocol. In this test set up the DoS attack was simulated at application level by sending correct and wrong Modbus requests at very high rate and sending Modbus requests more than configured maximum number of Modbus counter value and the same was detected by PLC and SCADA systems. The attacks were simulated with various parameters of Modbus requests and 98% attacks were detected successfully. In future, we will work on developing solutions to address other cyber-security attacks of Modbus Protocol.

REFERENCES

[1] Patrick, Dale R., and Stephen W. Fardo. Industrial process control systems. The Fairmont Press, Inc., 2009.

[2] Alvaro A. C ardenas, Saurabh Amin, Shankar Sastry. "Research Challenges for the Security of Control Systems", 3rd USENIX workshop on Hot Topics in Security (HotSec '08). Associated with the 17th USENIX Security Symposium. San Jose, CA, USA. July 2008.

[3] Sullivan D., Luiijf E., Colbert E.J.M. (2016) "Cyber-security of SCADA and Other Industrial Control Systems, Components of Industrial Control Systems", Advances in Information Security, vol 66. Springer, Cham.

[4] Figueroa-Lorenzo, Santiago, Javier Añorga, and Saioa Arrizabalaga. "A Role-Based Access Control Model in Modbus SCADA Systems. A Centralized Model Approach." Sensors 19.20 (2019): 4455.

[5] Alguliyev, Rasim, Yadigar Imamverdiyev, and Lyudmila Sukhostat. "Cyber-physical systems and their security issues." Computers in Industry 100 (2018): 212-223.

[6] Nazir, Sajid, Shushma Patel, and Dilip Patel. "Assessing and augmenting SCADA cyber security: A survey of techniques." Computers & Security 70 (2017): 436-454.

[7] Coffey, Kyle, et al. "Vulnerability assessment of cyber security for SCADA systems." Guide to Vulnerability Analysis for Computer Networks and Systems. Springer, Cham, 2018. 59-80.

[8] Nardone, Roberto, Ricardo J. Rodríguez, and Stefano Marrone. "Formal security assessment of Modbus protocol." 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE, 2016.

[9] MODBUS Over Serial Line Specification & Implementation Guide V1.02, Modbus Organization, Dec 20, 2006.

[10] MODBUS Messaging On Tcp/Ip Implementation Guide V1.0b, Modbus Organization, Oct 24, 2006.

[11] MODBUS Appl Protocol Specification V1.1 b3, Modbus Organization, April 26, 2012.

[12] Rajesh, L & Satyanarayana, P., "Communication protocol security in industrial control systems to protect national critical infrastructure". Journal of Advanced Research in Dynamical and Control Systems. 9. 290-304, 2017.

[13] Huitsing, Peter, Rodrigo Chandia, Mauricio Papa, and Sujeet Shenoi. "Attack taxonomies for the Modbus protocols." International Journal of Critical Infrastructure Protection 1 (2008): 37-44. doi:10.1016/j.ijcip.2008.08.003.

[14] Rajesh, L & Satyanarayana, P, "Dual channel scanning in communication protocol in industrial control systems for high availability of the system", International Journal of Technical and Physical Problems of Engineering. Vol. 11 P.22-27, 2019.

[15] Kalluri, Rajesh & Lagineni, Mahendra & Kumar, R. & Prasad, G.L., "Simulation and impact analysis of denial-of-service attacks on power SCADA". 1-5. 10.1109/NPSC.2016.7858908.,2016.

[16] Alvaro A. C ardenas, Saurabh Amin, Shankar Sastry. "Research Challenges for the Security of Control Systems", 3rd USENIX workshop on Hot Topics in Security (HotSec '08). Associated with the 17th USENIX Security Symposium. San Jose, CA, USA. July 2008.

[17] Jason Stamp, John Dillinger, William Young, and Jennifer DePoy., "Common vulnerabilities in critical infrastructure control systems" SANS SANSFIRE 2003 and National Information Assurance Leadership Conference V – (NIAL), July 14-22, 2003, Washingdon, DC

[18] Fovino, I. N., Carcano, A., Masera, M., & Trombetta, A., "Design and Implementation of a Secure Modbus Protocol"., IFIP Advances in Information and Communication Technology Critical Infrastructure Protection III, 83-96. doi:10.1007/978-3-642-04798-5_6, 2009.

[19] Shahzad, A.A. and S. Musa, "Cryptography and authentication placement to provide secure channel for SCADA communication". International Journal of Security., 6: 28-44, 2015.

[20] Shahzad, A., Lee, M., Lee, Y., Kim, S., Xiong, N., Choi, J., & Cho, Y.,"Real Time MODBUS Transmissions and Cryptography Security Designs and Enhancements of Protocol Sensitive Information". Symmetry,7(3), 1176-1210. doi:10.3390/sym7031176, 2015.

[21] S. Bhatia, N. Kush, C. Djamaludin, J. Akande, E. Foo, "Practical Modbus Flooding Attack and Detection", Proceedings of the Twelfth Australasian Information Security Conference (AISC) ser. AISC'14, vol. 149, pp. 57-65, 2014.

[22] Luo, Xuan, and Yongzhong Li. "Security Enhancement Mechanism of Modbus TCP Protocol." DEStech Transactions on Computer Science and Engineering iciti (2018).