Journal of ICT, Design, Engineering and Technological Science (JITDETS)
VOL. 2, NO. 2, pp. 30-35, 2018
DOI: https://doi.org/10.33150/JITDETS-2.2.1

ORIGINAL CONTRIBUTION

Modbus Packet Analysis and Attack Mode for SCADA System

Cheng-Hui Chou [1], Chi-Che Wu [2], Kuan-Chu Lu [3], I-Hsien Liu [4], Tien-Hsiang Chang [5], Chu-Fen Li [6], Jung-Shian Li [7*]

[1, 3, 4, 7] Institute of Department of Electrical Engineering, National Cheng Kung University, Tainan, Taiwan

[2] Department of Electronic Engineering, National Kaohsiung University of Science and Technology, Kaohsiung, Taiwan

[5] Department of Information Management, National Kaohsiung University of Science and Technology, Kaohsiung, Taiwan

[6] Department of Finance, National Formosa University, Huwei, Taiwan

***Abstract*— Internet of Things (IoT) and Industry 4.0 have become more and more common in recent years. In fact, smart houses that are common in the home, also include the monitor of the factory. Numerous IoT devices are developed on the basis of Linux. In view of this traditional network installation is more worthy of attention on the IoT. We remember to update the update of the home computer but often overlook the update of the IoT device because most of the IoT devices requires manual updates. Hackers often exploit this vulnerability to attack related devices. So, how to protect the IoT equipments is the topic of this study. This study proposes a honeypot search system based on self-study. The system can be used to search the honeypot system that may exist in the regional network, and design a smart honeypot system to confuse the attack of the hacker and protect the internal system of the enterprise.**

***Index Terms*— I**ndustrial Control Systems, Modbus/TCP, IoT

Received: 21 September 2018; **Accepted:** 13 October 2018; **Published:** 28 December 2018

I. INTRODUCTION

Recent years, Industry 4.0 and IoT technologies have matured. For example, by intelligent zing solar power plants, plant monitors can keep abreast of power generation situations and control the cost of generating electricity. When an warning , it can be processed at the timely to minimize the damage and Power plant power generation data can also be saved as a reference for optimizing solar power generation services in the future. The technology of information technology and the IoT becomes more and more mature, many factories and national key infrastructures use ICS to monitor and collect data [1].

The system for environmental monitoring and data collection, SCADA is an indispensable system for industrial control. The role of the system is mainly for the communication bridge between Human Machine Interface (HMI) and Programmable Logic Controller (PLC) [2], especially PLC is a special type of embedded device that is programmed to input, manage, and control physical objects such as valves, sensors, and so on. The main components required control system software, embedded operating systems, and digital input/output. It can be thought of as a special digital computer that executes specific instructions, collects data from input devices (such as sensors), sends commands to output devices (such as valves), and transmits data to engineering stations.

In the operation of the user, mainly through the interaction of the HMI, the user can query the related information of the device and transmit related instructions such as device control to the Supervisor Control Center (SCC) for processing. After the SCC receives the query and control commands from the HMI, the SCC will process the instructions and send them to the PLC to achieve the purpose of query and control. When the host of the SCC is attacked, or the PLC connected to each sensor is attacked, it is forced to send an abnormal value, so that the HMI provides the wrong information to the administrator, which will have irreparable consequences. Therefore, it is extremely important for the operation of industrial processes. In addition, certain features of ICS field devices make them more vulnerable to cyber-attacks. Usually, they are usually deployed for a long time (for decades). Also, the ICS typically includes several legacy devices that lack basic security features and no new security features [3, 4, 5, 6, 7].

Although the industrial control system is usually on the internal network, since most companies have other computers on the internal network to connect to the industrial control system, if the internal computer is attacked by a hacker, the hacker can directly access the PCL. Modbus protocol control to bypass HMI authority control. Therefore, how to make the data flow of the monitoring system normal to ensure the reliable and safe operation of SCADA is an important safety goal of this research [8, 9, 10, 11].

*Corresponding author: Jung-Shian Li
†Email: jsli@mail.ncku.edu.tw

II. BACKGROUND KNOWLEDGE

A. SCADA

The system for environmental monitoring and data collection is Core system of industrial control. The system has a wide range of applications, including power systems, oil, natural gas, etc., all of which are applications. The main purpose is to use the graphical interface method to display the information collected by various sensors by means of graphs [12] SCADA systems usually consist of a HMI and multiple PLCs. A PLC that can be connected to sensors and actuators, which has internal memory capacity, and runs the logic needed to control the connected devices. It stores the information received from the device and sends the data to the HMI system operator. In addition, it can also receive control data from the HMI and send the modification commands to the appropriate actuators. Among them, Modbus is one of the most common SCADA system protocols. Originally designed for serial line communication, the Modbus protocol was created assuming all SCADA functions are safe and function as expected. Since the protocol does not include authentication and authorization, and no data integrity verification, which leads to many Modbus systems have few defence mechanisms to combat malicious attacks. In addition, all data is transmitted in plain text without any encryption.

The main functions of the system are as follows

- Instant and historical data trend curve display
- Alarm processing system
- Data capture and recording
- Data analysis

The SCADA system is mainly composed of three parts: "HMI, SCC, PLC." The operation mode is mainly to send inquiry and control commands to the SCC for the HMI. When the SCC receives its instructions, it will query and control the PLC devices connected to the bottom, and then read its various sensors via PLC, and return the data to the SCC database for storage, and the results will be queried. Return to the HMI display [13].

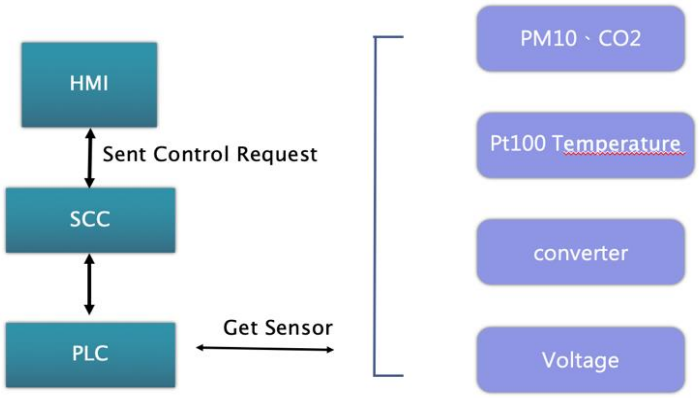

Fig. 1. SCADA architecture

B. Modbus/TCP

The Modbus protocol defines a process control system that emphasizes the exchange of information, and SCADA, structure and communication rules and operation and control of industrial processes [14]. Modbus' open protocol specification and TCP extensions are welcome, especially in the oil and gas sector, and are the primary control protocol for pipeline operations. There are two main variants of the Modbus protocol, Modbus Serial [15] and Modbus TCP [16].

In the Modbus serial communication protocol, messages are transmitted between the primary station and the secondary station (field device) via the serial communication line using the ASCII or RTU transmission mode. The newer Modbus/TCP protocol provides connectivity between Modbus networks (master stations and their slaves) and IP interconnect Modbus networks (multiple masters, each communicating with a set of slave stations that may overlap). Attacks on Modbus systems and networks can have a variety of effects, from sporadic outages to field devices (sensors and actuators) to large-scale outages, and even loss of control in the event of a fraudulent master. Its main targets include the primary station, field devices, serial communication lines (Modbus sequences) or network communication paths (Modbus TCP).

Modbus/TCP protocol provides connection based on TCP network (Master and Slave), and IP interconnection Modbus network (multiple masters, each with multiple slaves) [17]. The packet format of the Modbus/TCP Request is shown in Table I. In the Modbus/TCP protocol, the part of the packet field can be mainly divided into: Header, Address, Function Code, Start Address, and Request Length. In Header, it can be subdivided into: Transaction ID, Protocol ID, and length [18, 19].

TABLE I
MODBUS/TCP REQUEST FORMAT

Transaction ID	Protocol ID	Length	Address	Function Code	Start Address	Request length
2 Byte	2 Byte	2 Byte	1 Byte	1 Byte	2 Byte	2 Byte

C. Address Resolution Protocol (ARP) Attack

ARP attack is mainly an attack method derived from the ARP agreement. Fig. 2 below is an example: When PC1 wants to transmit data to PC3, it will transmit through Switch. If the MAC address corresponding to the IP is not recorded in the Table record, the Switch will send the packet before sending the packet. Send a broadcast packet of the ARP protocol and ask what is the MAC address of the computer corresponding to the IP of the destination under the entire local area network. At this time, when PC3 receives the broadcast packet, it will return its own MAC address to the

Switch. After completing the inquiry once, the MAC address corresponding to the IP is obtained, and the packet sent by the PC1 is transmitted to the PC of the PC3 [20, 21, 22].

The ARP scam is mainly to exploit this vulnerability. When the Switch sends a broadcast packet for inquiry, the attacker will continuously send a response and send its MAC address back to the Switch, so that the Switch believes. Therefore, the attacker continuously sends a response to tell the Switch the IP address of the IP. Although PC3 also responds, since PC2 actively sends a broadcast packet to respond to the Switch, the Switch will eventually trust the attacker's MAC address. Therefore, in this way, you can fool the Switch and pass all the packets to be sent to PC3 to the PC2. In this way, since both parties to the communication do not know that the packet has passed the third party's hand, this is also called a middleman (MITM) attack [23].

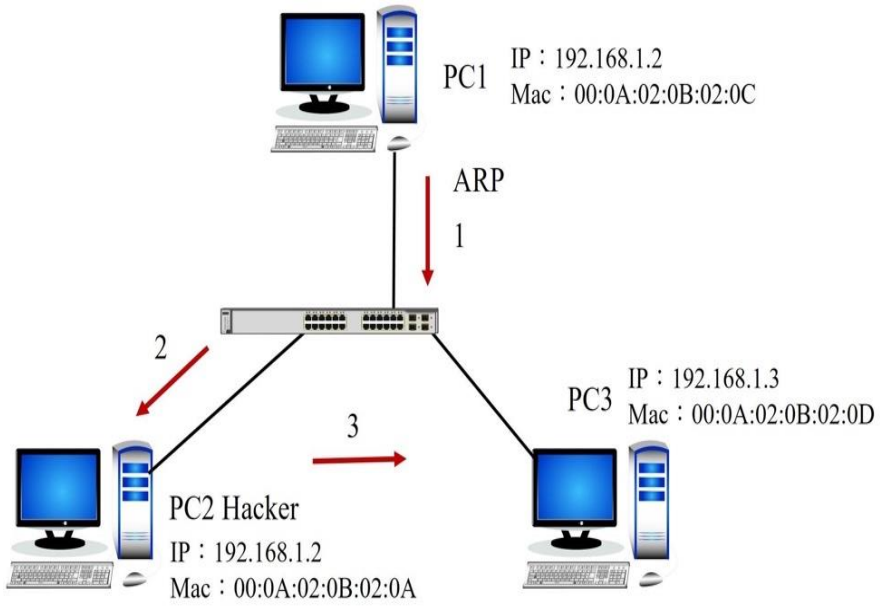

Fig. 2. ARP attack

III. EXPERIMENTAL DESIGN

A. SCADA of System Structure

In order to fully implement the system, we must first understand the communication protocols used by the HMI, SCC, and PLC used in the ICS industrial control system, and what devices are in our target system.

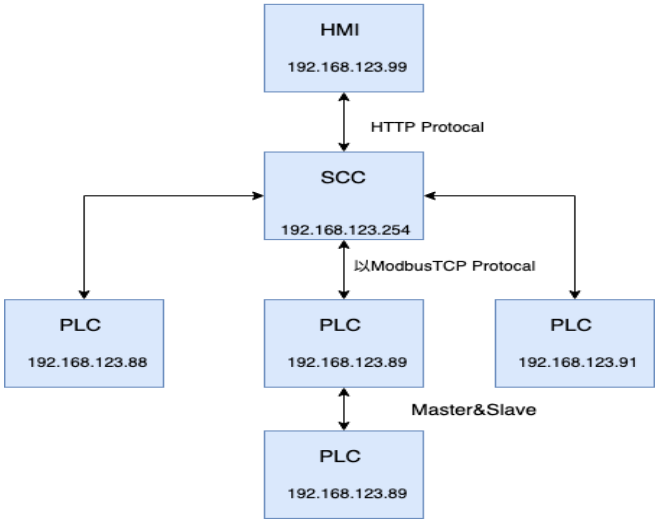

Fig. 3. SCADA architecture

Fig. 3 show the SCADA system is mainly built by WEB as the HMI, and the SCC host is responsible for receiving queries and control commands from the WEB side. In this end, the target system uses the WEB interface as a display, so The protocol used is the HTTP protocol. There are four PLCs connected to our SCC, two of which are PLC developed by Siemens (IP is 192.168.123.88, 192.168.123.91), and the other two are PLCs developed by Delta Electronics. Is 192.168.123.89, 192.168.123.90). The communication protocol they use to connect to the host of the SCC system is Modbus/TCP.

The operation of the SCADA system, the user connects to our HMI man-machine interface with IP 192.168.123.99, the web page sends an HTTP GET request SCC to query various Sensor values; when the SCC receives its command to query the Sensor value, it will pass Modbus. The TCP communication protocol transmits the query command to each PLC to query the various kinds of Sensor information connected to them, and finally returns the data result of the query to the HMI of the webpage as a display.

B. Design Process

The overall communication architecture and process of the SCADA system. Since our goal is to protect their SCC and PLC systems from attack, allowing attackers to attempt to attack the system, we can detect and notify the administrator to minimize damage. Therefore, our design process can be divided into the following two categories: environmental monitoring and construction, active trapping system development process.

The main purpose of environmental monitoring is to establish a packet monitoring environment, because we can ensure that the commu-

nication packets between the SCC system and the PLC system are able to be captured and stored. Therefore, before we start to implement the system design, we must first establish a packet monitoring environment for subsequent use as a development. So next, this study will introduce each section of the process for each step.

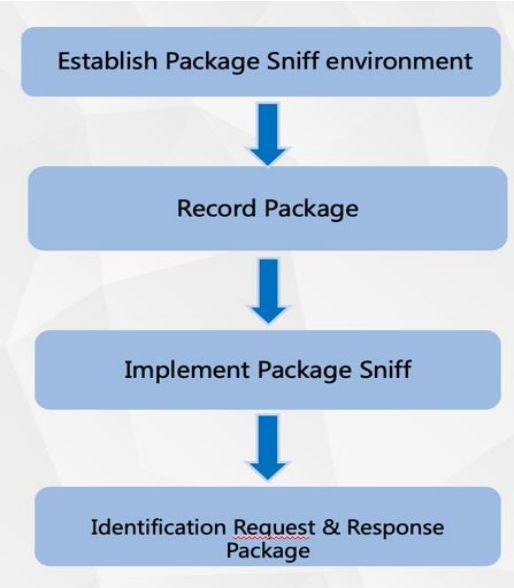

Fig. 4. Environmental monitoring

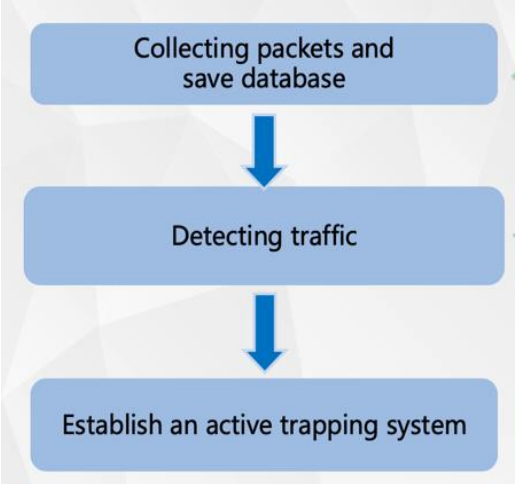

Fig. 5. System development

C. Implementation Monitoring System

We use C# as a programming language to listen to all the connection packets of the switch and record related information.

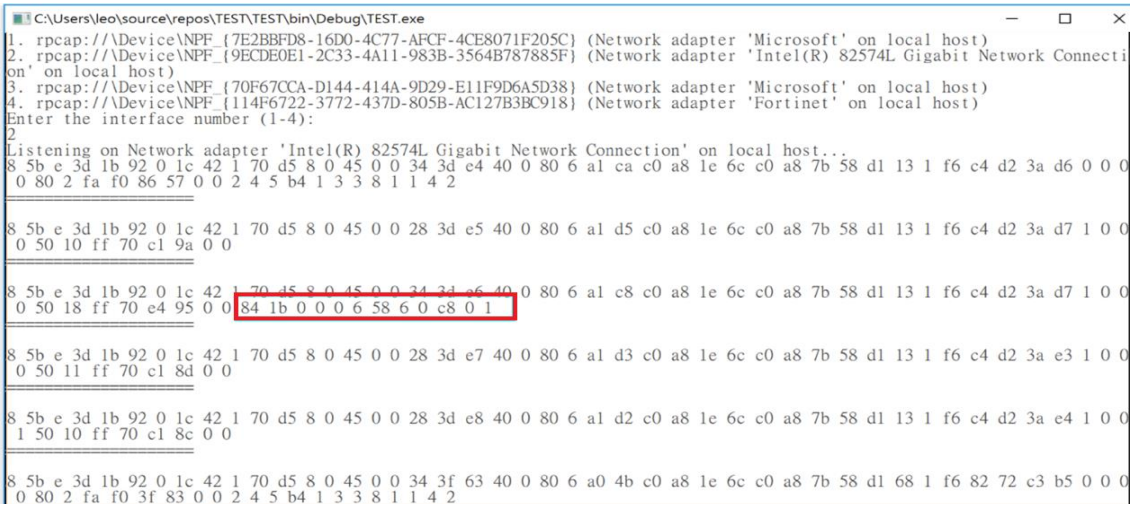

Fig. 6. Implement package sniff

D. Detect Abnormal Traffic

We have classified the request packets according to different sensors and stored them in the database. We group each query's request by group and calculate the total number of packets we have collected. When the training is completed, the number will gradually stabilize and be synchronized, so after the training is over, we can start to enter the detection phase.

In the detection phase, we tried to pretend that the SCC sent the same Modbus/TCP query command to the PLC with the target IP of 192.168.123.88. Since our source IP is not the IP 192.168.123.254 of the SCC, and the Queryed StartAddr does not exist, we can easily retrieve this number of 1 exceptions based on past data during detection. flow. Next, we will further analyze this abnormal traffic and identify the attack mode of the abnormal traffic.

SourceIP	DestinationIP	SourceMAC	DestinationMAC	StartAddr	data	count
192.168.123.254	192.168.123.88	0 50 18 21 e3 10	0 1b c5 0 e2 f8	0 0	47eb84f367ad926c675ef5dff4c346a5	232
192.168.123.254	192.168.123.88	0 50 18 21 e3 10	0 1b c5 0 e2 f8	0 0	4a3ba3722182a7bab1fb221ee4b84f74	232
192.168.123.254	192.168.123.88	0 50 18 21 e3 10	0 1b c5 0 e2 f8	0 0	5d280d08ce8dd363ccbcda36bf4e4bc9	232
192.168.123.254	192.168.123.88	0 50 18 21 e3 10	0 1b c5 0 e2 f8	0 0	9079815015e3dbd48dd17fa514a9cf19	232
192.168.123.254	192.168.123.91	0 50 18 21 e3 10	e0 dc a0 4d f9 15	0 0	9d2c95da313e830a4910466db714d5ca	232
192.168.123.254	192.168.123.88	0 50 18 21 e3 10	0 1b c5 0 e2 f8	0 1	e1123fb89aab1a8051770bd4282985c2	232
192.168.123.254	192.168.123.91	0 50 18 21 e3 10	e0 dc a0 4d f9 15	0 1	e6f29fce6b15b21be445afd89d230592	232
192.168.123.254	192.168.123.88	0 50 18 21 e3 10	0 1b c5 0 e2 f8	0 2	59e9f9bcb473ba8eba783d102b301382	232
192.168.123.254	192.168.123.88	0 50 18 21 e3 10	0 1b c5 0 e2 f8	0 2	83ff89e71881d58b69d8c68ab56c8603	232
192.168.123.254	192.168.123.91	0 50 18 21 e3 10	e0 dc a0 4d f9 15	0 2	c43069b87c8276bdd9e420311d68acee	232
192.168.123.254	192.168.123.88	0 50 18 21 e3 10	0 1b c5 0 e2 f8	0 4	3165638bb8fdb35fb8a62992c23d612b	232
192.168.123.30	192.168.123.88	0 50 18 21 e3 10	0 1b c5 0 e2 f8	0 4	ed0f64c69657c1c6d6e427d3eaeee736	1
192.168.123.254	192.168.123.88	0 50 18 21 e3 10	0 1b c5 0 e2 f8	0 c8	d57187a19896c945703063f80783eeb1	232
192.168.123.254	192.168.123.88	0 50 18 21 e3 10	0 1b c5 0 e2 f8	0 c9	c7c0b2d2f1c1d057253ac367db958368	232
192.168.123.254	192.168.123.88	0 50 18 21 e3 10	0 1b c5 0 e2 f8	1 90	d09b4d8a1bed75156b0f2c2b2b77f42b	232
192.168.123.254	192.168.123.89	0 50 18 21 e3 10	0 18 23 3c 86 c6	10 0	bfce2de435245689fc2cdd480df7951e	232
192.168.123.254	192.168.123.89	0 50 18 21 e3 10	0 18 23 3c 86 c6	10 1	e273a0a7b691c638404f665567dbd44d	232
192.168.123.254	192.168.123.89	0 50 18 21 e3 10	0 18 23 3c 86 c6	10 2	e9e9449757175673524857 4dab435fc7	232

Fig. 7. Detect traffic

IV. CONCLUSION

This article has confirmed that PLC can be attacked by the SCADA through network from the simulation environment. PLCs are the most common devices in SCADA systems. They are located between the HMI and the field devices and are responsible for sending commands to and receiving data from the field devices. Since the PLC is programmable, it can be completely destroyed by a malicious control program. This article explained of attacks (ARP attack). Through these attacks, it can be found that the communication between PLC and SCADA may be affected, resulting in serious instability of the SCADA system. How to improve information security as much as possible has always been a direction and goal we need to think about. In the field of information, there are often attacks that occur, so how to keep the defence so that the system can be properly protected has always been the ultimate goal of our information personnel to pay attention to and think about. Especially in industrial control systems, information security environment construction and protection is more important. However, in an industrially controlled environment, because of the continuous and stable operation of the equipment, it is difficult to continuously update, resulting in a system that is too old and vulnerable to damage from other attacks.

TABLE II
SUMMARY

Item	Attack detection system	Traditional Attack detection system	Non use Attack detection system
ARP attack detected on system	Instantly notify managers and issue warnings	will be issued if it is in the blacklist	Need to wait until an exception occurs
Setting mechanism	Self-learning	Need to be manually set by the administrator	-
Expansibility	Can be linked to honeypots to counteract	only Notification	-

V. ACKNOWLEDGMENT

This work was supported by the MOST (Ministry of Science and Technology), Taiwan under contracts numbers MOST 108-2218-E-006-035-.

References

[1] J. Lee, B. Bagheri, and H.-A. Kao, ``A cyber-physical systems architecture for industry 4.0-based manufacturing systems,'' *Manufacturing Letters*, vol. 3, pp. 18-23, 2015. doi: https://doi.org/10.1016/j.mfglet.2014.12.001

[2] E. Byres and J. Lowe, ``The myths and facts behind cyber security risks for industrial control systems,'' in *Proceedings of VDE Kongress,* Berlin, Germany, 2004, pp. 213-218.

[3] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, ``A review of cyber security risk assessment methods for SCADA systems,'' *Computers & Security*, vol. 56, pp. 1-27, 2016. doi: https://doi.org/10.1016/j.cose.2015.09.009

[4] A. Sajid, H. Abbas, and K. Saleem, ``Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges,'' *IEEE Access*, vol. 4, pp. 1375-1384, 2016. doi: https://doi.org/10.1109/access.2016.2549047

[5] N. Erez and A. Wool, ``Control variable classification, modeling and anomaly detection in Modbus/TCP SCADA systems,'' *International Journal of Critical Infrastructure Protection*, vol. 10, pp. 59-70, sep 2015. doi: https://doi.org/10.1016/j.ijcip.2015.05.001

[6] K. Ozhikenov, E. Tuleshov, R. Ismagulova, G. Aitzhanova, and A. Ozhiken, ``Modeling the control system of sensor movement mechanism of logging unit,'' *International Journal of Technology and Engineering Studies*, vol. 1, no. 3, pp. 69-73, 2015. doi: https://doi.org/10.20469/ijtes.40001-3

[7] L. A. Alindayo and J. C. Maglasang, ``Wireless sensor network development: Targeting and control system for semi-ballistic vehicle

for rapid and precise search and rescue applications,'' *Journal of Advances in Technology and Engineering Studies*, vol. 4, no. 4, pp. 149-161, 2018. doi: https://doi.org/10.20474/jater-4.4.2

[8] A. G. Voyiatzis, K. Katsigiannis, and S. Koubias, ``A modbus/TCP fuzzer for testing internetworked industrial systems,'' in *IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA),* Luxembourg, 2015, pp. 1-6.

[9] S. S. Khuzyatov and R. A. Valiev, ``Organization of data exchange through the modbus network between the SIMATIC S7 PLC and field devices,'' in *International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM),* St. Petersburg, Russia, 2017, pp. 1-3.

[10] B. Chen, N. Pattanaik, A. Goulart, K. L. Butler-purry, and D. Kundur, ``Implementing attacks for Modbus/TCP protocol in a real-time cyber physical system test bed,'' in *IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR),* Charleston, SC, 2015, pp. 1-6.

[11] M. Anwaruddin and M. A. Ali, ``A review on raspberry pi based industrial process monitoring and control using modbus protocol,'' *International Journal of Innovative Technology and Research (IJITR)*, vol. 5, no. 1, pp. 5483-5486, 2017.

[12] R. A. Gupta and M.-Y. Chow, ``Networked control system: Overview and research trends,'' *IEEE Transactions on Industrial Electronics*, vol. 57, no. 7, pp. 2527-2535, 2010. doi: https://doi.org/10.1109/tie.2009.2035462

[13] V. M. Igure, S. A. Laughter, and R. D. Williams, ``Security issues in SCADA networks,'' *Computers & Security*, vol. 25, no. 7, pp. 498-506, 2006. doi: https://doi.org/10.1016/j.cose.2006.03.001

[14] S. Boyer, *SCADA: Supervisory Control and Data Acquisition*, 4th ed. Reserach Triangle, NC: International Society of Automation, 2010.

[15] Modbus.org. (2002) Modbus over serial line specification and implementation guide v1.0. [Online]. Available: https://bit.ly/2S26654

[16] Modbus-IDA. (2004) Modbus messaging on TCP/IP implementation guide v1.0a. [Online]. Available: https://bit.ly/2UujhgN

[17] P. Huitsing, R. Chandia, M. Papa, and S. Shenoi, ``Attack taxonomies for the modbus protocols,'' *International Journal of Critical Infrastructure Protection*, vol. 1, pp. 37-44, 2008. doi: https://doi.org/10.1016/j.ijcip.2008.08.003

[18] C. Queiroz, A. Mahmood, J. Hu, Z. Tari, and X. Yu, ``Building a SCADA security testbed,'' in *Third International Conference on Network and System Security,* Gold Coast, Australia, 2009, pp. 357-364.

[19] N. Ugtakhbayar, B. Usukhbayar, S. H. Sodbileg, and J. Nyamjav, ``Detecting tcp based attacks using data mining algorithms,'' *International Journal of Technology and Engineering Studies*, vol. 2, no. 1, pp. 1-4, 2016. doi: https://doi.org/10.20469/ijtes.2.40001-1

[20] A. Jicha, M. Patton, and H. Chen, ``SCADA honeypots: An in-depth analysis of conpot,'' in *IEEE Conference on Intelligence and Security Informatics (ISI),* Tucson, AZ, 2016, pp. 196-198.

[21] N. Tsalis, G. Stergiopoulos, E. Bitsikas, D. Gritzalis, and T. Apostolopoulos, ``Side channel attacks over encrypted TCP/IP modbus reveal functionality leaks,'' in *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications,* Porto, Portugal, 2018, pp. 219-229.

[22] L. Deng, Y. Peng, C. Liu, X. Xin, and Y. Xie, ``Intrusion detection method based on support vector machine access of modbus TCP protocol,'' in *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData),* Chengdu, China, 2016, pp. 380-383.

[23] N. Cai, J. Wang, and X. Yu, ``SCADA system security: Complexity, history and new developments,'' in *6th IEEE International Conference on Industrial Informatics,* Daejeon, South Korea. IEEE, 2008, pp. 569-574.