Inferring ICS Topology and Behavior through Network Traffic Analysis

Chien-Wen Tseng
M.S. Degree Program on Cyber-Security Intelligence, National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

Jung-Shian Li
Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

Chu-Fen Li
Department of Finance, National Formosa University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

I-Hsien Liu
Department of Electrical Engineering, National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

E- mail: cwtseng@cans.ee.ncku.edu.tw, jsli@cans.ee.ncku.edu.tw, chufenli@gmail.com, ihliu@cans.ee.ncku.edu.tw *
www.ncku.edu.tw

Abstract

Ensuring the proper operation of industrial control systems (ICS) is a critical issue. Previous studies have focused on observing the controllers directly; however, this research proposes that analyzing network traffic could reduce system interference. This study utilizes a cybersecurity testing platform for dam systems to investigate network traffic to infer the composition of network nodes and the communication behavior between them. By doing so, it provides an alternative perspective for monitoring ICS operations. This model aids in understanding system topology, tracking potential deviations, and ensuring operational stability.

Keywords: Industrial Control Systems, Network Traffic Analysis, Industrial Control Communications.

1. Introduction

In 2024, a significant cyberattack in a rural Texas town targeted the water management system, leading to an overflow incident [1]. Although this event did not pose an immediate threat to public safety, it served as a stark reminder of the potential risks associated with similar attacks. Water overflow incidents can lead to severe consequences, including water contamination, disruptions in supply, and damage to critical infrastructure [2], which could compromise public safety and incur significant economic losses. This incident highlighted the growing vulnerability of critical infrastructure to cyber threats, especially as these systems increasingly rely on interconnected technologies and controllers to manage essential processes [3] . The event emphasized the need for robust monitoring mechanisms to strengthen ICS resilience against cyberattacks.

The scarcity of publicly available datasets related to water resource management systems poses significant challenges to conducting in-depth studies in this field. The limited data not only restricts comprehensive analysis but also makes it difficult to gain a clear understanding of system behaviors and interactions. In response to such challenges, the previous experimental teams leveraged the CANS RT/DT dataset [4] to observe and analyze ICS behaviors. Researchers aimed to gain a deeper understanding of critical elements in the field, focusing on their functional roles, operational behaviors, and how these behaviors evolve under various conditions.

Given the challenges in understanding water resource operations, this study conducts a preliminary analysis of the CANS RT/DT dataset [4] [5] to observe and explore ICS components, their behaviors, and interactions for initial insights. By systematically examining this dataset, the research aims to support the future establishment of a normal operational model. This involves identifying patterns and relationships between system components, which can serve as a foundation for modeling standard behaviors.

2. Background

2.1. Industrial Control System

Supervisory Control and Data Acquisition [6] (SCADA)-based Industrial Control Systems (ICS) are vital for critical infrastructure, enabling centralized monitoring and control of essential processes such as dam operations, energy grids, and manufacturing systems. SCADA systems rely on Programmable Logic Controllers (PLCs) to bridge field devices with higher-level supervisory systems. PLCs execute predefined instructions to manage Digital Inputs/Outputs (DI/DO) for binary operations, such as controlling pumps and alarms, and Analog Inputs/Outputs (AI/AO) for continuous monitoring of parameters like pressure and temperature [7] This hierarchical architecture facilitates real-time control and communication, ensuring efficient and reliable management of processes.

2.2. Modbus Traffic Analysis

Analyzing network traffic provides a non-intrusive and comprehensive approach to understanding the behavior of ICS environments and identifying potential vulnerabilities. By examining communication patterns and packet characteristics, researchers can infer system topology and evaluate interactions between devices.

Within this context, Modbus TCP [8] plays a pivotal role in ICS communication. As an extension of the widely adopted Modbus protocol, Modbus TCP leverages TCP/IP for enhanced connectivity, enabling data exchange between devices such as PLCs and sensors within a master-slave architecture. The protocol uses function codes, such as 0x03 for reading holding registers, to monitor and manipulate device states. PLCs often use Modbus TCP to transmit operational data, including sensor readings and actuator commands. Analog inputs like voltage or current are stored in two 16-bit registers and converted into IEEE 754 floating-point numbers [9] [10] for precise representation. This communication facilitates real-time data sharing and control, making Modbus TCP a fundamental protocol for understanding ICS network behavior.

After capturing the network traffic data, key attributes such as source and destination IP addresses, timestamps, register values, and MAC addresses are extracted from the Modbus TCP packets. These attributes provide a detailed view of communication patterns and operational data within the system, enabling a closer examination of how components interact. The extracted data is further processed to derive statistical insights, such as communication frequency, response times, and register value distributions. These insights are useful for understanding system behavior and establishing references for future analysis.

3. Methodology Overview for Network Traffic Analysis

This study draws inspiration from framework ATT&CK, specifically the Reconnaissance phase [11], to inform the methodology for analyzing the CANS RT/DT dataset and understanding Industrial Control Systems (ICS). While Reconnaissance typically involves active network scanning to map system components and interactions, it has potential to disrupt normal operations and their limited scope in capturing comprehensive data. Instead, Wireshark pcapng file from the CANS RT/DT dataset are utilized to extract and process network traffic data in a non-intrusive manner. The methodology focuses on passive monitoring, leveraging pre-collected network traffic to avoid disruptions to normal operations. By focusing on Modbus TCP packets [12], which are commonly used in ICS communication. This approach emphasizes passive monitoring, utilizing pre-collected network traffic to enable effective observation of system activities.

The data analysis methodology is based on a structured workflow, as illustrated in Fig. 1 Network traffic is captured within the ICS environment using packet tool Wireshark, with a focus on filtering Modbus TCP packet. To ensure passive monitoring, a mirror port is set up on the network switch, allowing traffic to be observed without affecting live operations. The captured traffic is parsed to extract relevant details and generate metrics that reflect communication trends and system interactions.

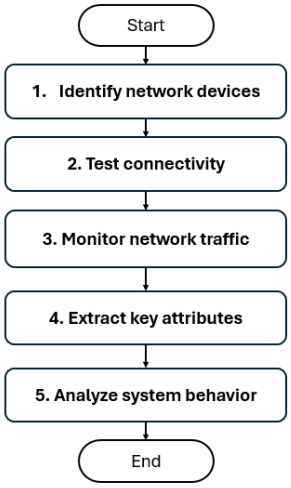

Fig. 1. systematic workflow for data analysis

Further analysis involves correlating the captured packet timestamps with the observed gate states to determine whether changes in flow rates correspond to

variations in gate state indicators. The gate state indicators, such as power supply status, gate movement, and emergency operations, are mapped to specific attributes like register values in the data. By analyzing the relationships between flow rate differences and gate states, it becomes possible to infer how gate operations influence system behavior. These observations help establish a foundational understanding of the dynamic interactions between gate controls and water flow, contributing to a broader perspective on system operations.

4. Result of observation

4.1. *System topology*

Based on the provided network Fig. 2, it is possible to infer that the central node 192.168.1.50 might represent a switch, serving as a hub to facilitate communication between other devices, such as the PLCs (192.168.1.5, 192.168.1.6, 192.168.1.7). The switch could be primarily responsible for forwarding data packets without directly engaging in logical operations. The edges represent the number of response packets exchanged between the devices during a one-hour capture period, with a total of 7176 packets recorded.

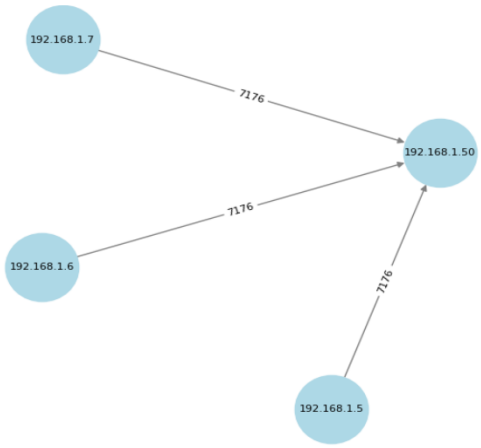

Fig. 2. System topology

4.2. *PLC's state*

The Modbus register values exhibit distinct patterns over a two-minute period. Take Fig. 3 for IP 192.168.1.5 and Fig. 4 for 192.168.1.6 as an example. The Modbus registers in the dataset are organized with specific functions and interpretations. Register 0 records the binary states of 16 digital inputs, where each bit represents the TRUE/FALSE status of corresponding gate operations. This allows for a concise representation of multiple discrete signals within a single register. Register 1 was not observed in the dataset during the analysis. Registers 3 and 2 store gate voltage values, Registers 5 and 4 capture gate current readings, and Registers 7 and 6 record gate opening degree. These paired registers are combined into 32-bit integers and converted to floating-point numbers using the IEEE 754 standard, providing precise measurements for continuous parameters such as voltage, current, and position. The ordering of the registers may appear inverted due to the little-endian format often used in Modbus systems, where the least significant word is stored before the most significant word. This structure ensures compatibility with standard protocols and simplifies data processing for ICS operations.

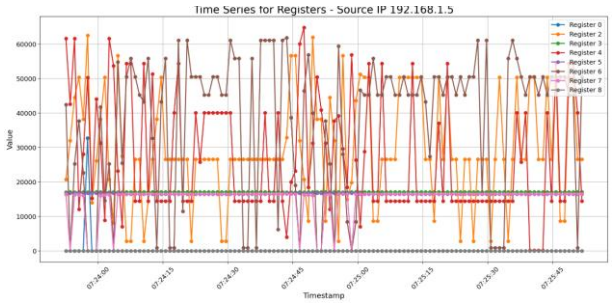

Fig. 3. Response of Register value response from IP192.168.1.5

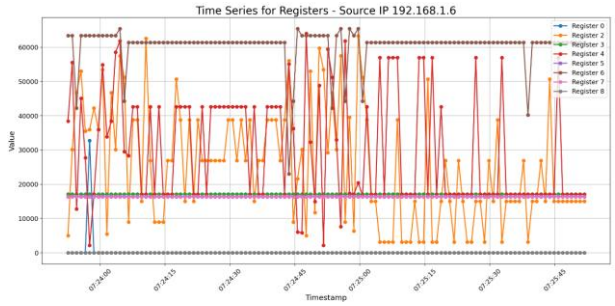

Fig. 4. Response of Register value response from IP192.168.1.6

The dataset reveals several limitations. Most packets used Function Code 3, indicating a focus on monitoring register values, likely reflecting on-site operations, with no observable changes in Function Codes even during remote operations. Additionally, when current spikes coincided with gate opening degree changes, the corresponding gate operation indicators were not captured promptly, likely due to the discrete nature of state recordings, which may miss transient system changes.

5. Conclusion

This study explores the potential of analyzing the operational behavior of industrial control systems (ICS) by interpreting key system attributes, such as IP addresses and register values, to observe device status and operational patterns. The passive monitoring approach minimizes interference with on-site operations, making it suitable for preliminary observations. These observations provide a foundation for developing a normal operational model, which can be used as a reference to enhance system reliability.

Acknowledgment

This work was supported by the National Science and Technology Council (NSTC) under contract number 113-2221-E-006-147-MY2 and 113-2634-F-006-001-MBK.

References

1. Associated Press, "Rural Texas Towns Report Cyberattacks That Caused One Water System to Overflow," 2024 [Online]. Available: https://www.securityweek.com/rural-texas-towns-report-cyberattacks-that-caused-one-water-system-to-overflow/. [Accessed 15 Oct 2024].
2. J-P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," Microprocessors and Microsystems, vol. 77, p. 103201, 2020.
3. M. M. Aslam, A. Tufail, R. A. A. H. M. Apong, L. C. De Silva, M. T. Raza, "Scrutinizing Security in Industrial Control Systems: An Architectural Vulnerabilities and Communication Network Perspective," IEEE Access, vol. 12, pp. 67537 - 67573, 2024.
4. CANS, "CANS RT," 2024. [Online]. Available: https://www.cans.ee.ncku.edu.tw/research/cansrt. [Accessed 15 Oct 2024]
5. M.-W. Chang, J.-S. Li, and I-H. Liu, "Cyber-Physical Security Testbed for Dam Control System", Journal of Advances in Artificial Life Robotics, Vol. 4, No. 2, pp. 63-66, 2023.
6. D. Pliatsios, P. Sarigiannidis, T Lagkas, A. G. Sarigiannidis, "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1942 - 1976, 2020.
7. U. George-Andrei, P. Olga, U. Maria, "PLCs' Inputs and Outputs Response Time Testing Application," 2021 International Conference on Electromechanical and Energy Systems (SIELMEN), Iasi, Romania, 06-08 Oct , 2021.
8. V. G. Găitan, I. Zagan, "Modbus Protocol Performance Analysis in a Variable Configuration of the Physical Fieldbus Architecture," IEEE Access, vol. 10, pp. 123942 - 123955, 2022.
9. S. Jaloudi, "microIoTSCADA: A Tool to Monitor and Control Renewable Energy-Based Systems Using MODBUS," in 2024 4th Interdisciplinary Conference on Electrics and Computer (INTCEC), Chicago, IL, USA, 11-13 Jun , 2024.
10. Microprocessor Standards Committee, IEEE Standard for Floating-Point Arithmetic, IEEE Std 754-2019, IEEE Computer Society, 2019.
11. MITRE, "Reconnaissance," Oct 2020. [Online]. Available: https://attack.mitre.org/tactics/TA0043/. [Accessed 20 Oct 2024].
12. P. Radoglou-Grammatikis, I. Siniosoglou, T. Liatifis, A. Kourouniadis, K. Rompolos, P. Sarigiannidis, "Implementation and Detection of Modbus Cyberattacks," 2020 9th International Conference on Modern Circuits and Systems Technologies (MOCAST), Bremen, Germany, 07-09 Sep , 2020.

Authors Introduction

Ms. Chien-Wen Tseng

She is a postgraduate of M.S. Degree Program on Cyber-Security Intelligence, National Cheng Kung University in Taiwan. She received her B.B.A. degree from the Bachelor of Information Management, Yuan Ze University, Taiwan in 2023. Her interests is ICS Security.

Dr. Jung-Shian Li

He is a full Professor in the Department of Electrical Engineering, National Cheng Kung University, Taiwan. He graduated from the National Taiwan University, Taiwan, with B.S. in 1990 and M.S. degrees in 1992 in Electrical Engineering. He obtained his PhD in 1999 in Computer Science from the Technical University of Berlin, Germany. He teaches communication courses and his research interests include cybersecurity, cloud computing and network management. He is currently involved in funded research projects dealing with cybersecurity and critical infrastructure protection. He is the director of Taiwan Information Security Center @ National Cheng Kung University.

Prof. Chu-Fen Li

She is an Associate Professor in the Department of Finance at the National Formosa University, Taiwan. She received her PhD in information management, finance and banking from the Europa-Universität Viadrina Frankfurt, Germany. Her current research interests include intelligence finance, e-commerce security, financial technology, IoT security management, as well as financial institutions and markets. Her papers have been published in several international refereed journals such as European Journal of Operational Research, Journal of System and Software, International Journal of Information and Management Sciences, Asia Journal of Management and Humanity Sciences, and others.

Dr. I-Hsien Liu

He is an assistant professor in the Department of Electrical Engineering, National Cheng Kung University, Taiwan. He obtained his Ph.D. in 2015 in Computer and Communication Engineering from the National Cheng Kung University. He teaches cybersecurity courses and his interests are Cyber-Security, OT Security, and Wired & Wireless Communication. He is the deputy director of Taiwan Information Security Center @ National Cheng Kung University (TWISC@NCKU).