SUGISAKA MASANORI

Journal of Robotics, Networking and Artificial Life
Vol. 10(2); September (2023), pp. 179–183
ISSN (Online): 2352-6386; ISSN (Print): 2405-9021
https://alife-robotics.org/jrnal.html

Research Article

Securing the Critical Communication in Dam Control System with SDN

I-Hsien Liu, Min-Wei Huang, Hsin-Yu Lai, Meng-Huan Lee, 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

ARTICLE INFO

Article History
Received 08 October 2022
Accepted 23 October 2023

Keywords
Cybersecurity
Industrial control system
Software-defined network

ABSTRACT
Industrial control systems currently heavily rely on the Internet of Things, which poses a higher risk of cyber attacks. This is particularly concerning in critical infrastructure, as an attack could endanger lives and result in military actions. A software-defined network is a common centralized network architecture in the Internet. It has a lot of uses and is easy to manage. In our research, we applied the SDN (Software-defined network) on the ICS (Industrial Control System) to ensure the critical flow between industrial equipment.

1. Introduction

In recent years, the rapid development of the Industrial Internet of Things has promoted the automation of traditional production methods. However, it undoubtedly increases the possibility of external attacks. Threats are no longer limited to the IT field [1], and have spread to OT field. The national critical infrastructure such as nuclear power plants and dams are also kind of industrial control systems. Unlike general production plants, if the equipment of critical infrastructure lacks a complete and reliable defense mechanism, there will be many vulnerabilities and threats, which greatly affect the needs of people's lives. The most well-known case is that in 2010, hackers used Stuxnet worm to attack nuclear power plant in Iran. Such attacks are not allowed to exist for the country. Therefore, cybersecurity protection measures on OT field are gradually becoming necessary. In this research, we added a SDN [2] controller in our dam gate cybersecurity testbed. Therefore, the network between system environment can be managed. Additionally, we created special flow entry to enhance protection of critical traffic. Under our proposed method, the transmission quality can be maintained.

2. Background

The current vulnerabilities and weaknesses in ICS are discussed only from the experimental environment. Hence, restoring the on-site environment on the testbed is necessary for factories and government to discover the harm and threats. There are some small-scale security testbeds, such as power system [3] in the world at present. However, the testbeds for water resources [4] is are less discussed globally. SWaT [5] is one of the most famous testbeds for industrial control system cybersecurity research and training, especially in water resources.

Software-defined network is often known as an efficient and flexible solution in IoT. By separating the control and data planes, software-defined network can achieve effective traffic management such as allocation of resources according to network traffic requirements to reduce network congestion and improve network performance and scalability. In addition, its programmable features enable the customization of

Corresponding author E-mail: jsli@mail.ncku.edu.tw, ihliu@cans.ee.ncku.edu.tw, mwhuang@cans.ee.ncku.edu.tw, hylai@cans.ee.ncku.edu.tw, mhlee@cans.ee.ncku.edu.tw URL: www.ncku.edu.tw

network management for specific IoT applications and provide more effective solutions. Many scholars [6], [7] using SDN structures, which have centralized architecture can manage the network to protect the industrial control system.

3. System Design

3.1. *The dam gate cybersecurity testbed*

The current testbed for water resources is rare, which is unfriendly for researchers to conduct research. For this issue, our team designed a testbed to simulate the dam

Fig. 1. Physical dam gate testbed.

gate system. In terms of technical details, each gate is controlled by the PLC (Programmable logic controller), which utilizes registers to access relevant instructions and data. Therefore, this information on PLC can express various values of the current industrial environment such as water pressure and current. Modbus/TCP protocol is used to design a computer-based testbed that simulates dam gates. Physical PLC is used to connect and transmit data between the gates, providing a platform for research on industrial control. Fig. 1. displays the physical testbed of the dam gates that we constructed.

3.2. *System architecture*

After building the dam gate cybersecurity testbed, in our research, the original Ethernet switch we used at level 4 is changed to the SDN switch. By doing this, we combined the dam gate cybersecurity testbed with SDN. The architecture is shown in Fig. 2. We can then set flow

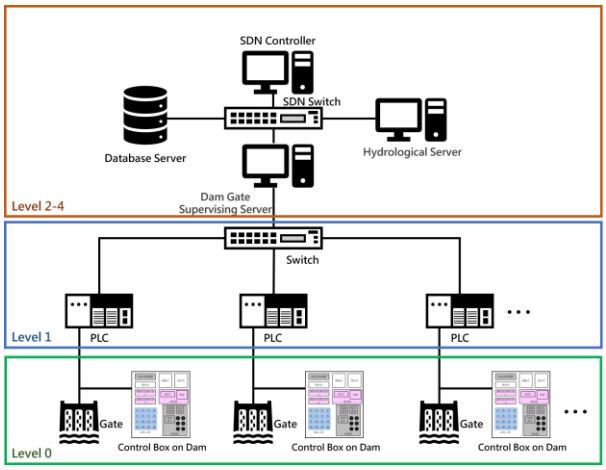

Fig. 2. The dam gate cybersecurity testbed with SDN.

entry rules through the controller, and all traffic passing through the switch needs to follow the rules [8].

3.3. *Flow entry rules*

Between the controller and the switch, flow entries that match the environment are defined [9], so that the OpenFlow switch can forward messages and execute actions based on instructions provided by the controller. In our approach, we set a flow entry rule to ensure the connection between HMI (Human Machine Interface) and PLC via MAC address. Afterwards, set this flow entry rule to have the highest priority. By doing this, the connection can be end-to-end. Secondly, in order to ensure that only authorized packets can be transmitted, we also set another flow entry rule to discard packets from other sources sent to the PLC, also through MAC addresses. Our proposed method enables message protection for critical flow entries in PLC communication, effectively implementing a whitelisting approach.

4. Experiment and Result

In our experiment, we use HPE Aruba 5130 Switch, which supports OpenFlow 1.3, as the normal and the Openflow-supported switch. The attack process shown in Table 1 starts from the attacker's perspective. First, the attacker identifies the manufacturer of the device and opens the TCP port to the device on the network through a reconnaissance attack. Secondly, an inject attack is launched through the response of ARP spoofing to allow the attacker to cut off the communication at both ends and check the master-slave relation and environment. Then, a command injection is launched to attack PLC by using the MODBUS test software. We implemented this attack to change data in the holding register and caused incorrect commands. Finally, a flooding attack, which can interrupt the operation of the system is launched.

Table 1. Attack classification and process.

Name	Classification	Tools
Network Scanning	Reconnaissance Attacks	Nmap
ARP Spoofing	Reconnaissance Attacks	dsniff – arpspoof, Wireshark
Memory I/O via MODBUS TCP	Command Injection Attacks	Modbus TCP test softwarez, Wireshark
ICMP Flood	Denial of Service Attacks	hping
ICMP Advance Flood	Denial of Service Attacks	hping

Table 2. The response time of each gate of normal switch.

	Gate A	Gate B
Max. (ms)	15.67	N/A
Min. (ms)	15.57	N/A
Average (ms)	15.62	N/A
Standard Deviation	0.00001	N/A
Response packets	100	0
Packet Loss Rate(%)	0	100

Table 3. The response time of each gate of SDN switch.

	Gate A	Gate B
Max. (ms)	15.68	15.66
Min. (ms)	15.59	15.57
Average (ms)	15.62	15.62
Standard Deviation	0.00001	0.00001
Response Packets	100	100
Packet Loss Rate(%)	0	0

In our research, we experimented with the normal switch and the SDN switch and obtained the response time when gate B was attacked by ICMP flooding in Table 2 and Table 3, respectively. In Table 2, the gate B cannot respond under the attack of ICMP flooding with the normal switch. But compared with the response time of gate B in Table 3, the gate B can operate without any interruption. By setting the SDN flow entry rules based on the process, we can ensure the protection of the MAC address of the gate PLC, leading to the desired outcome. To maintain uninterrupted service quality in the transmission of critical water infrastructure facilities within the ICS network, it is possible to prevent all the above-mentioned attacks.

5. Conclusions

It is nowadays obvious that the defense mechanism of industrial control systems still needs to be strengthened. Besides, it is necessary to build a test bed to simulate the actual equipment. Since large-scale equipment replacement in OT environments is unlikely, the experiment combines SDN with the test bed to maintain flexibility without sacrificing compatibility. Our research employs a whitelist mechanism that assigns the highest priority to critical traffic to safeguard critical gate PLCs via flow entry rules.

Acknowledgments

This work was supported by the National Science and Technology Council (NSTC) in Taiwan under contract numbers 111-2218-E-006-010-MBK, 111-2218-E-006-079- and 112-2634-F-006-001-MBK.

References

1. I-H. Liu, K.-M. Su, and J.-S. Li*, 2021, "The Security Issue of ICS: The Use of IT Infrastructure", Journal of Robotics, Networking and Artificial Life, Vol. 8, Issue 1, pp. 29–32.
2. N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: enabling innovation in campus networks, " *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69-74, 2008.
3. K. Barnes, B. Johnson, "National SCADA Test Bed Substation Automation Evaluation Report", 2009.
4. L. Faramondi, F. Flammini, S. Guarino, R. Setola, "A Hardware-in-the-Loop Water Distribution Testbed Dataset for Cyber-Physical Security Testing", IEEE Access, vol. 9, pp. 122385-122396, 2021.
5. A. P. Mathur, N. O. Tippenhauer, "SWaT: a water treatment testbed for research and training on ICS security", 2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater), Vienna, Austria, 11 Apr., 2016.
6. R. D. Lallo, F. Griscioli, G. Lospoto, H. Mostafaei, M. Pizzonia, M. Rimondini, "Leveraging SDN to monitor critical infrastructure networks in a smarter way", 2017 IFIP/IEEE International Symposium on Integrated Network Management, Lisbon, Portugal, 8-12 May, 2017.
7. V. Venugopal, J. Alves-Foss, and S. Gogineni Ravindrababu. 2019. "Use of an SDN switch in support of NIST ICS security recommendations and least privilege networking.", Industrial Control System Security (ICSS) Workshop, Dec. 2019.
8. S. Khan, A. Gani, A. W. A. Wahab,M. Guizani, and M. K. Khan, "Topology Discovery in Software Defined Networks: Threats, Taxonomy, and State-of-the-Art, " *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 303-324, 2017.
9. M-W Huang, I-H. Liu, J.-S. Li, "Strengthen the Security of the Industrial Control System using SDN Technology", ICAROB 2023, Oita, Japan, Feb. 9-12, 2023.

Authors Introduction

Dr. I-Hsien Liu

He is an assistant professor in 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. His interests are Cyber-Security, Wireless Network, Group Communication, and Reliable Transmission. He is the deputy director of Taiwan Information Security Center @ National Cheng Kung University(TWISC@NCKU).

Ms. Min-Wei Huang

She is acquiring the master's degree in Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University in Taiwan. She received her B.S. degree from the Department of Communications, Navigation and Control Engineering, National Ocean University, Taiwan in 2021. Her interests are Cyber-Security and Software-Defined Network.

Mr. Hsin-Yu Lai

He got the M.S. degree in National Cheng Kung University in Taiwan. He also received his B.S. degree from the Department of Electrical Engineering, National Chung Cheng University, Taiwan in 2019. His interests are Cyber-Security and Software-Defined Network.

Mr. Meng-Huan Lee

He is studying for his master's degree in Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University in Taiwan. He graduated from the Department of Communications Engeineering, National Chung Cheng University, Taiwan in 2021. His interests are Cyber-Security and Cellular Network Security.

Prof. 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 wired and wireless network protocol design, network security, and network management. He is the director of Taiwan Information Security Center @ National Cheng Kung University. He serves on the editorial boards of the International Journal of Communication Systems.