Strengthen the Security of the Industrial Control System using SDN Technology

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

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

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

Meng-Huan Lee
Department of Electrical Engineering / Institute of Computer and Communication Engineering,
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
E-mail: mwhuang@cans.ee.ncku.edu.tw, ihliu@cans.ee.ncku.edu.tw, hylai@cans.ee.ncku.edu.tw,
*mhlee@cans.ee.ncku.edu.tw, jsli@mail.ncku.edu.tw**
www.ncku.edu.tw

Abstract

In the field of OT, most of the network architectures operated in the way of isolation from internal and external networks. Only firewalls are installed on the external network without any protection measures for the internal network. In this paper, we leverage a Software-defined network (SDN) with an industrial control system (ICS), so controllers can manage the equipment and keep track of each switch and its connection with the programmable logic controller (PLC) in the ICS. Additionally, only the critical flows can be allowed by adding flow entries. So the transmission between the PLC and Human Machine Interface (HMI) can be protected. The transmission quality of the ICS and its availability can be improved.

Keywords: ICS, Cybersecurity, OT security, Software-defined network.

1. Introduction

The network of equipment in the industrial control system gradually operates and develops in the form of the Internet of Things. Operating technicians can access these equipment through the network, but it also means that more and more information is transmitted between these devices through the network, which undoubtedly increases the chance of being attacked. In the current operational technology field, most network structures are operated in the way of internal and external isolation. Only a firewall is connected to the external end, and no protections are taken for the internal network. Once the attacker invaded, the attack will be out of control, and let system weak. The impact even extends to the country's critical infrastructure. In our research, we use a SDN controller to manage the equipment and keep track of each network between the system environment and its connected PLC. And create key flow entry rules to protect the critical flow of communication between in ICS equipment to maintain the transmission quality of industrial network.

2. Background

Most of the critical infrastructures are constructed by industrial control systems. Besides lots of information security issues in the information technology (IT) field, accidents of ICS are also frequent currently. Companies and countries need to think about how to build and use security testbeds to defend against attacks [1], and the establishment of a testbed for water resources will be described in 2.1. And there are also many scholars using centralized management structures in SDN for protecting industrial networks [2] will be described in 2.2

2.1. *Water resources security testbed*

Due to the cost and other various considerations, there is not much large-scale security testbed in the world at present. Most of them are built on power systems [1]. The water resources testbed is much fewer globally. A small-scale testbed was used for simulates dam pumping and distribution in [3]. Moreover, the more well-known SWaT [4] is used for the security research of the ICS for water treatment and for operator training.

2.2. *Software-defined network*

Software-defined network (SDN) architecture is widely used nowadays due to that it can make users get rid of the limitations of hardware in traditional networks. The SDN separates the control plane and the data plane of the traditional switch. Researchers can design the network more flexibly and control network traffic through the centralized management controller to solve the problem caused by a generally distributed network. The data plane has a network topology composed of network devices. The devices at this layer are responsible for packet forwarding. The forwarding rules are determined by the rule table, which can be set and modified by the control layer.

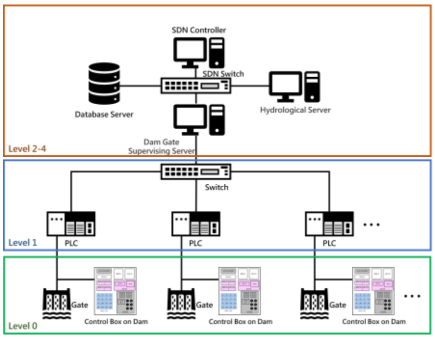


Fig. 1. Water Critical Infrastructure Architecture with SDN

3. System Design

In this section, our architecture and method are described. To enhance the transmission quality of ICS, we combined the SDN technology and the water-critical infrastructure architecture.

3.1. *System architecture*

In the water infrastructure information security testbed built by our team, we replaced the Ethernet switch of the dam gate operating system with another switch that supports the OpenFlow protocol. That made the switch to be the southbound interface protocol in the SDN. The water-based critical infrastructure information security testbed can be combined with SDN. The establishment of the Openflow instance enables the switch to enable the functionality of the Southbound interface protocol with OpenFlow protocol. The critical infrastructure structure for water resources is shown in Fig. 1.

3.2. *Flow entry rules*

Between the controller and the switch, a flow table that matches the environment is set, and flow entries are defined so that the OpenFlow switch can forward messages and perform actions according to the rules of the controller. The priority is set according to the individual flow entry. When the switch executes according to the flow entry in the flow table, the action is

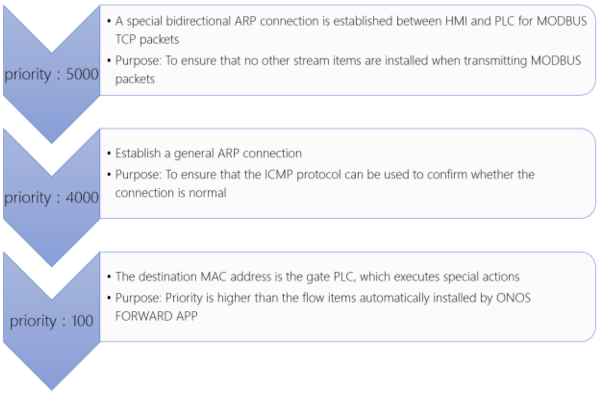
Table 1. Attack Classification and Process.

Classification	Name	Tools
Reconnaissance Attacks	Network Scanning	Nmap
Reconnaissance Attacks	ARP Spoofing	dsniff - arpspoof Wireshark
Command Injection Attacks	MODBUS TCP Read and Write Memory	Modbus TCP test software Wireshark
Denial of Service Attacks	ICMP Flood	hping
Denial of Service Attacks	ICMP Advance Flood	hping

executed according to the set priority, and the message protection of the key flow entry is achieved in the communication of the programmable logic controller. The mechanism is shown in Fig. 2.

4. Experiment and Result

In our experiment, we use Hewlett-Packard 5130 Switch as the original switch and the Openflow-supported switch. To make the connection be end-to-end, we first limited the source MAC, destination MAC address, and the port to Openflow switch. Then, we respectively write the bidirectional flow entry and increases the priority. Besides, flow entry rules between HMI and PLC are set to the highest priority. As for the special settings of flow entries, in this experiment, the packets whose target is the MAC address of the dam gate programmable logic controller and whose priority is higher than that of the general forwarding flow entry are dropped to achieve the effect of whitelisting. That makes sure that only the connection between HMI and PLC can be successful. Additionally, the experiment will be divided into three scenarios: the original switch, the Openflow switch with normal flow rule, and the Openflow switch with key flow entries rules for comparison to do the attack experiment.



- A special bidirectional ARP connection is established between HMI and PLC for MODBUS TCP packets
- Purpose: To ensure that no other stream items are installed when transmitting MODBUS packets

- Establish a general ARP connection
- Purpose: To ensure that the ICMP protocol can be used to confirm whether the connection is normal

- The destination MAC address is the gate PLC, which executes special actions
- Purpose: Priority is higher than the flow items automatically installed by ONOS FORWARD APP

Fig. 2. Flow Entry Rule Sample.

The attack process shown in Table 1. takes the attacker's perspective as the starting point. First, the attacker examines and judges the devices in the network through reconnaissance attacks to identify the manufacturer of the device and open TCP ports. Launch a inject attack through the response of ARP Spoofing, so that the attacker can cut off the communication between the two ends and see the master-slave relationship, and further understand the environment and available equipment. Then, attack PLC by a command injection that is using the MODBUS test software. All the data in the holding register will be changed and operated according to incorrect commands. Finally, a flood attack is carried out, which paralyzes the operation of the equipment on the system. Furthermore, it will destroy the process of the system.

In our research, we take three different switches mentioned earlier to experiment and get the result that the SDN flow entry rules set according to the process in Fig. 2 can make the MAC of gate PLC can under the protection. It prevents the possibility of being attacked by using ARP connections with the gate PLC.

Once we avoid all the above-mentioned reconnaissance attacks and subsequent attacks, the service quality of ICS network transmission of critical water infrastructure facilities can be ensured not be affected.

5. Conclusions

Most of the weaknesses existing in the current ICS environment are due to too much trust in the firewall, resulting in no protections in the intranet. And that weak network will create vulnerability for attackers. However, in the current OT environment, most of the equipment in the ICS is used for many years and has no chance to be replaced due to the cost and difficulties of deployment. Hence, we take use of setting the flow entries rule, prioritizing all devices traffic to let the system communication follow the flow entries. Finally, give critical traffic the highest priority and make a whitelistlike mechanism to protect PLCs for critical infrastructure gates.

Acknowledgments

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

References

1. K. Barnes, B. Johnson, “National SCADA Test Bed Substation Automation Evaluation Report”, 2009.
2. 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.
3. 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.
4. 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.

Authors Introduction

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.

Dr. I-Hsien Liu

He is a research fellow in the Taiwan Information Security Center @ National Cheng Kung University (TWISC@NCKU) and Department of Electrical Engineering, National Cheng Kung University, Taiwan. He obtained his PhD 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.

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.