SUGISAKA MASANORI

Journal of Robotics, Networking and Artificial Life
Vol. 9(3); December (2022), pp. 229–232
ISSN (Online):2352-6386; ISSN (Print):2405-9021
https://alife-robotics.org/jrnal.html

Research Article

OPC UA TSN Industrial Control System Cybersecurity Testbed

I-Hsien Liu[1], Chuan-Kang Liu[2], Li-Yin Chang[1], Jung-Shian Li[1]

[1]*Department of Electronic Engineering/Institute of Computer and Communication Engineering, National Cheng Kung University, No. 1, Daxue Road, East District, Tainan, 701401, Taiwan*

[2]*Department of Artificial Intelligence and Computer, Engineering, National Chin-Yi University of Technology, No.57, Sec. 2, Zhongshan Road, Taiping District, Taichung, 411030, Taiwan*

ARTICLE INFO

Article History
Received 27 October 2021
Accepted 04 September 2022

Keywords
Industrial control system (ICS)
OPC UA
Cybersecurity
Electroencephalogram
Time sensitive networking (TSN)

ABSTRACT

Due to the advent of Industrial 4.0, the Industrial Internet emphasizes the combination and application of IT technology and OT technology, and one of the features of Time sensitive networking is the feature of separating transmission time. This feature will be able to combine IT technology and OT technology in Industrial control systems. But as a result, the issue of information security in the industry is on the rise. In order to research security issue and protection in Time sensitive networking, we have built a test platform support TSN for industrial control networks for related research. Through the experiments in the research, we can know that TSN has a good effect on the separation of general traffic and TSN traffic. TSN won't be affected by general traffic but is very vulnerable to priority traffic attacks.

1. Introduction

In terms of IT and OT communication in ICS, Ethernet is commonly used in ICS especially like Industry 4.0, However, due to the development of Industry 4.0 and smart manufacturing, the periodic requirements for the network are getting shorter and shorter, The traditional Ethernet system cannot meet the real-time requirements due to random media access and best effort (Best Effort) forwarding mechanism [1]. Therefore, It is difficult to ensure the timing behavior of critical traffic under these circumstances and to provide isolation from noncritical traffic. In order to ensure the security and real-time performance of critical traffic, we have established an industrial control system testbed [2] with TSN equipment and combine OPC UA to test the security and time of industrial critical traffic. The devices are from Intel, Cisco, NXP.

2. Background

In modern factories and smart manufacturing, ICS controls many devices and controllers, and there are many different communication protocols between controllers and devices. For example, MODBUS TCP Ethernet/IP, Open Platform Communication Unified Architecture (OPC-UA), IEEE 1722, Object Management Group (OMG) Real-time System Data Distribution Service (DDS) [3]. These protocols can support the extension of TSN to meet all the requirements of real-time Ethernet because of the characteristics of Ethernet, while making Ethernet transmission more

Corresponding author's E-mail: ihliu@cans.ee.ncku.edu.tw, ckliu@ncut.edu.tw, lychang@cans.ee.ncku.edu.tw, jsli@mail.ncku.edu.tw
web: www.ncku.edu.tw, www.ncut.edu.tw

reliable, reducing jitter and shortening delay. In the part of ICS cyber attack, it can be seen from past research that the OT part is mainly DoS attack and command injection attack [4]. We choose DoS attack because of the time-sensitive characteristics of equipment.

2.1. *TSN-standard*

In order to solve the problem of ensuring that the delay behavior of critical traffic is isolated from general traffic, The IEEE 802.1 working group defined a new and enhanced set of standards, namely Time Sensitive Networking. It is an extension of IEEE 802.1 Ethernet, a series of new specifications established by the Time Sensitive Network Task Group of the IEEE 802.1 Working Group on the basis of existing standards as shown in Table 1 below.

Table 1. IEEE TSN Primarily Standard [5].

TSN standard	Standard description
802.1Qcc	Network management
802.1Qbv	Scheduled traffic
802.1Qav	Credited based shaper
802.1Qcb	Frame replication
802.1AS	Timing and synchronization
802.1Qbu	Frame preemption
802.1Qca	Path control and reservation

In our ICS testbed, we mainly focus on the research and result analysis of 802.1QBV. Below we will mainly introduce several protocols used on the testbed:

- 802.1AS: In the TSN system, time synchronization is the most important part. All devices must be synchronized to the same clock. 802.1AS is an enhanced version of the PTP time synchronization protocol. Compared with the general PTP, 802.1AS has only one central clock, and the rest are auxiliary clocks, and packets can only be transmitted in a synchronized time domain [6].
- IEEE802.1Qbv: In order to achieve the coexistence of various priority flows in the same network and have available separate bandwidth and end-to-end delay specifications, 802.1Qbv defines the mechanism for packet forwarding in the switch, which uses Time Aware Shaper (TAS) to send packets in the different queue [7]. Fig. 1 shows the 802.1Qbv example.

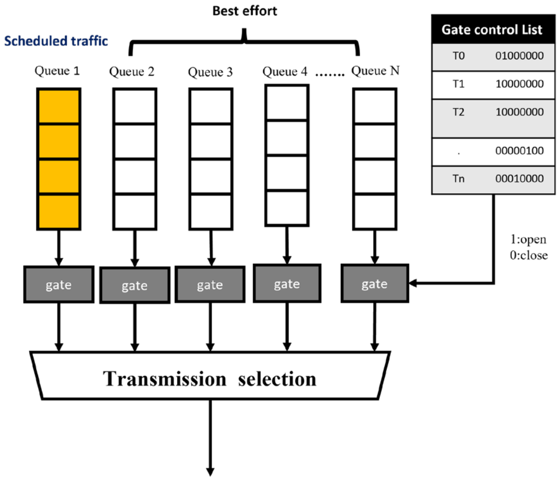

Fig. 1.802.1Qbv example [7].

2.2. *OPC Unified Architecture*

OPC UA announce that it started supported the field level in Industrial Control System in 2018 Because of the Pub/Sub connectionless transmission method, OPC UA can support industrial control equipment that requires real-time transmission [8].

2.3. *OPC UA over TSN*

However, how to ensure the real-time transmission of field-level devices in the local area network is an important issue. OPC UA over Ethernet is an Ethernet based protocol designed with EtherType B62C for transporting UA Datagram Protocol (UADP) messages within the OSI layer 2 Ethernet frame without using any UDP or IP headers, this makes it possible to integrate the TSN characteristics into OPC UA protocol for real-time transmission among field devices in an industrial environment [9].

3. OPC UA TSN Testbed

In our previous research, we had conduct a TSN cyber security testbed, and we are applying OPC UA to this information security testbed. In order to test OPC UA TSN security issue. We use CISCO and NXP TSN switches as a bridge in the industrial environment architecture of OPC UA TSN. On the terminal device, we use the real-time LINUX operating system with supports i210 NIC as the real-time traffic publisher and subscriber of Pub/Sub. Fig. 2 shows the scenario of OPC UA TSN, and we set the publisher publish realtime UADP traffic every 500 microsecond.

In the OPC UA TSN environment, there are a large number of devices in the factory, and the devices rely on each traffic's vlan id and priority as the packets to distinguish whether they are subscribed or not.

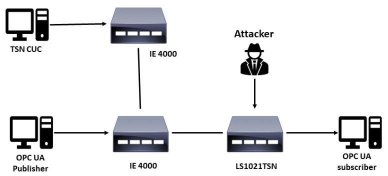

Fig. 2 OPC UA TSN scenario

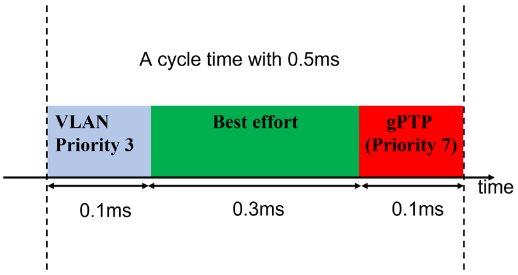

Fig. 3 Qbv schedule on the egress port

In our previous research we found that TSN switch won't suffer any interference from general traffic DoS attacks. However, the attacker can tag his packet with any vlan priority after he control the administrator privileges root. On the egress port to the OPC UA subscriber, we set the timing schedule as the Fig. 3. We set a total cycle time with 0.5ms and divide into three time slot with different priority, priority 3 with pub/sub traffic, priority 7 with PTP packet for 802.1AS time sync, and others with general best effort traffic.

4. Results

In our experiment, we use two different Dos attack types, such as ICMP flooding and Ping of death with VLAN tag priority of 3. On the terminal device, we use the real-time LINUX operating system that supports i210 NIC as the real-time traffic publisher and subscriber of Pub/Sub. Fig 2 shows the scenario of OPC UA TSN, and we set the publisher to publish real-time UADP traffic every 500 microseconds. The result in Fig. 4 shows that the impact of the attack is huge. The Ping of death makes Pub/sub packet drop seriously. The impact of ICMP flooding is relatively minor, causing some packets to 7000 microseconds, on the other hand, ICMP flooding cause arrive in the second cycle and some packets to be lost.

We can see that the ping of death cause a latency of up to up to 1500 microsecond at most.

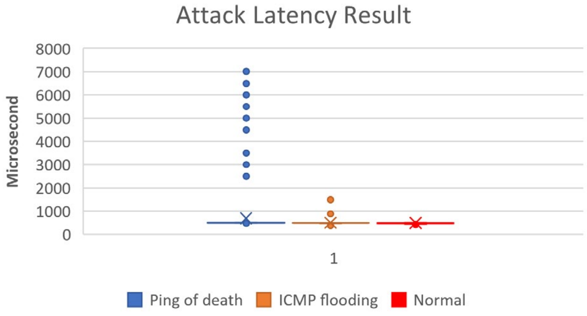

Fig. 4 Pub/Sub Latency result

5. Conclusion

TSN is different from the transmission characteristics of general Ethernet, it can combine IT traffic and OT traffic in industrial control systems. We applied OPC UA and TSN to the testbed. At the same time, we found that TSN can well separate time for TSN traffic without interference from other traffic, but TSN traffic become very sensitive to traffic of the same priority, which amplifies the effect of DOS attack. After analyzing the results, we found that the main factor affecting the attack is the packet size of malicious traffic. The larger the packet, the stronger the attack on TSN traffic and the higher the packet loss rate.

Acknowledgements

This work was supported by the National Science and technology Council (NSTC) in Taiwan under contract numbers 110-2218-E-006-013-MBK and 111-2218-E-006-010-MBK.

References

1. J. Decotignie, "Ethernet-Based Real-Time and Industrial Communications," Proceedings of the IEEE, vol. 93, no. 6, pp. 1102 - 1117, 2005.
2. S. Chouksey, H. S. Satheesh, Johan Åkerberg, "Coexistence, An Experimental Study of TSN-NonTSN," 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, USA, 27-30 Jan., 2021.
3. V. GOLLER, "Time Sensitive Networks For Industrial Automation Systems," Analog Devices, 2016.
4. W. Duo, M.C. Zhou, A. Abusorrah, "A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges," IEEE/CAA Journal of Automatica Sinica, vol. 9, no. 5, pp. 784-800, 26 4 2022

5. IEEE, Time-Sensitive Networking (TSN) Task Group, IEEE, 2016. .
6. M. Rostan, “IEEE P802.1AS-Rev/D8.0, Draft Standard for Local and Metropolitan Area Networks—Timing and Synchronization for TimeSensitive Applications,” 2019.
7. IEEE, IEEE Std 802.1Qbv - Enhancements for Scheduled Traffic, IEEE, 2016.
8. S. K. Panda, M. Majumder, L. Wisniewski, J. Jasperneite, “Real-time Industrial Communication by using OPC UA Field Level Communication,” 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Vienna, Austria, 8-11 Sep., 2020.
9. D. Bruckner, M.-P. Stănică, R. Blair, S. Schriegel, S. Kehrer, M. Seewald, T. Sauter, “An Introduction to OPC UA TSN for Industrial Communication Systems,” Proceedings of the IEEE, vol. 107, no. 6, pp. 1121 - 1131, 2019.

Authors Introduction

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.

Prof. Chuan-Kang Liu

He is an Associate Professor in the Department of Artificial Intelligence and Computer, Engineering, National Chin-Yi University of Technology. He received the B.Sc. degree from the Department of Electrical Engineering, Tam Kang University, in 2000. Then he graduated from the National Cheng Kung University with M.S. and PhD degrees in Electrical Engineering. His research interests are in the areas of optical networks control, wireless networks, EPON, VANET, network security, cloud computing and TCP performance analysis.

Mr. Li-Yin Chang

He was born in Tainan. He received his B.S. degree from the Department of Communiciation Engineering, National Chung Cheng University, Taiwan in 2020. He is acquiring the master’s degree in Department of Electrical Engineering/Institute of Computer and Communication Engineering, National Cheng Kung University in Taiwan.

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.

: