Industrial Control System Cybersecurity Testbed with TSN Feature

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

Li-Yin Chang [2]
Department of Electronic Engineering/Institute of Computer and Communication Engineering,
National Cheng Kung University, No. 1, Daxue Road, East District
Tainan, 701401, Taiwan

Jung-Shian Li* [3]
Department of Electronic Engineering/Institute of Computer and Communication Engineering,
National Cheng Kung University, No. 1, Daxue Road, East District
Tainan, 701401, Taiwan

Chuan-Gang Liu[4]
Department of Applied Informatics and Multimedia,
Chia Nan University of Pharmacy & Science, No. 60, Sec. 1, Erren Rd., Rende Dist., Tainan City 717301, Taiwan
E-mail: ihliu@cans.ee.ncku.edu.tw[1]*,lychang@cans.ee.ncku.edu.tw*[2]*, jsli@cans.ee.ncku.edu.tw*[3]*, chgliu@mail.cnu.edu.tw*[4]
www.ncku.edu.tw[123]*, www.cnu.edu.tw*[4]

Abstract

Due to the advent of Industrial automation and the Industrial Internet, information security attacks on the industrial environment have emerged one after another. In order to conduct better research and protection against industrial control attacks, we have built a test platform for industrial control networks for related research. We have built equipment that supports time-sensitive networks in this field to conduct research on Cybersecurity with time-sensitive networking.

Keywords: ICS, Networking, Cybersecurity, TSN.

1. Introduction

In terms of IT communication in Industrial Control System (ICS), Ethernet is commonly used in ICS and IT. 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 (BE) 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] and support TSN(Time sensitive networking) equipment and technology and successfully utilize TSN standard to ensure the security and time of critical traffic. The devices are from Intel, Cisco, NI.

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, OLE in Process Control 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 reliable, reducing jitter and shortening delay.

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 **[4]**.

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 and 802.1Qav. 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. [5].
- 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 [6].Figure 1 shows the 802.1Qbv example.

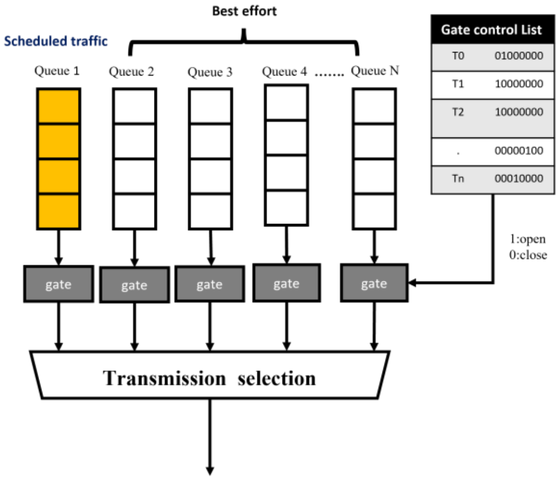


Fig. 1.802.1Qbv example [6].

- IEEE 802.1Qcc: 802.1Qcc defines the management configuration in the TSN network, which defines the distributed configuration and the centralized configuration, Figure 2 shows an example of the centralized configuration, The central network controller (CNC) will manage all the bridge ends in the network. The CNC mainly masters all network topology information, is responsible for calculating the transmission delay of the link, including the packet size and quantity, and then calculates a guarantee to meet Deterministic transmission schedule of traffic demand [7].
- IEEE 802.1Qav :Use credit based shaper to ensure that traditional asynchronous Ethernet data traffic will not interfere with AVB's real-time audio and video streams. it provides bounded latency per stream type. It has been developed for professional audio and video applications, and the major application can still be seen in such streams.

3. TSN Testbed Scenario

We setup a TSN testbed with the device from multiple vendors, we use cisco IE4000 as our bridge because ie4000 supports 802.1as and 802.1qbv. In the part of the speaker and the receiver, we use a computer with an I210 network interface card,because the support of 802.1Qbv, 802.1AS, and 802.1Qav. Figure 3 shows our testbed scenario. In our testbed, we use the ptp4l library in the linux to implement 802.1AS to sync all the device manually because cisco CNC can only sync the bridge.

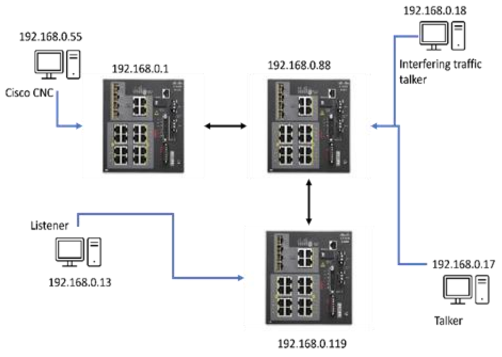


Fig. 2. TSN testbed scenario

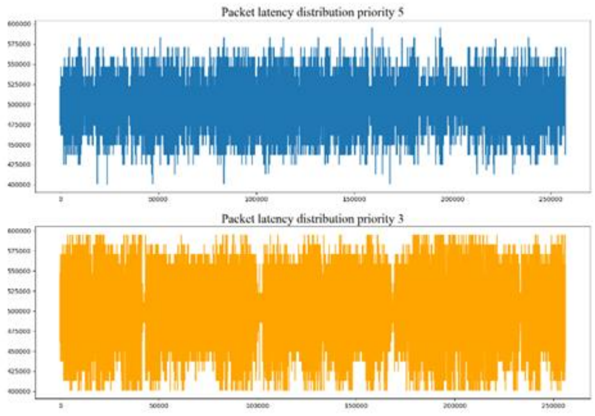


Fig. 3 Delay result without 802.1Qbv

4. Results

In our experiment, we analyze the traffic interference of UDP DOS attacks with Qbv and Qav flow. In the Qbv scenario, we set a cycle time period to 1 millisecond, cut into 10 time slices, the first and the fifth time slices we send BE traffic, and the second and sixth time slices send priority 5 traffic. The third and seventh time slices are priority 3 traffic, so we want the critical priority traffic latencies to be 0.5ms. During the experiment, we use UDP dos attack to interfere with traffic In the experiment, we use UDP dos attack to interfere with traffic.

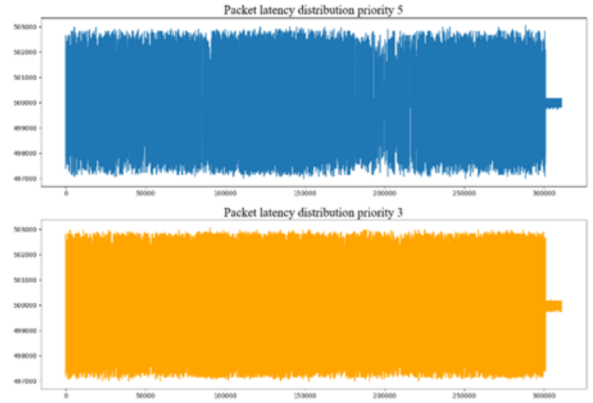
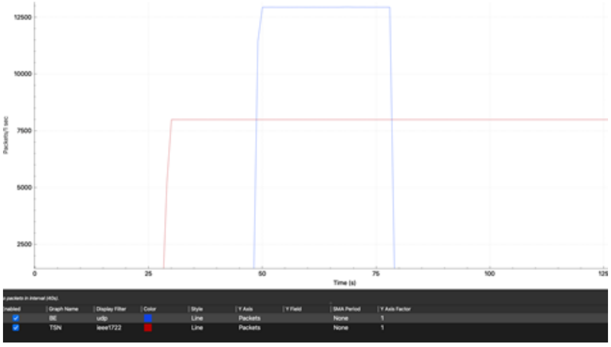


Fig. 4. Delay result with 802.1Qbv

Figure 4 shows the result of not using the 802.1Qbv flow isolation mechanism. It can be seen that jitter is very large even up to 100000ns, therefore the delay of critical traffic cannot be guaranteed.

In Figure 5, it can be seen that the effect of controlling jitter after using 802.1Qbv. Traffic isolation works perfect. Even if the malicious activities happened, jitter was still controlled under 3000ns.After 300,000 packets, we turn off the dos attack and we can see that the delay control can be within a few hundred ns.



s packets in interval (40s).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
☑	BE	udp	🟦	Line	Packets		None	1
☑	TSN	ieee1722	🟥	Line	Packets		None	1

Fig. 5 Qav result with CBS

In the QAV experiment, we will produce IEEE1722 audio packets mixed with normal BE packets. We will transmit 8000 packet/second SR Class A audio frames as represented by the red line in the figure 5. Best effort traffic is in color blue. We generated interfering traffic using the iperf3 tool. As the Fig 5 display, the IEEE 1722 audio frames are consistently 125 µs delta time apart shows that the interference to BE traffic is well controlled.

5. Conclusion

From the experimental results, we can see the two abovementioned standards control the delay to protect critical traffic from jamming and exhibit an encouraging effect on DOS attacks. The actual delay is also related to the CPU computing power and kernel of the hardware device. Our testbed will also continue to be used for conducting more cyber security research on TSN.

Acknowledgements

This work was supported by the Ministry of Science and Technology (MOST) in Taiwan under contract numbers MOST 110-2218-E-006-013-MBK-.

References

1. J.-D. Decotignie, "Ethernet-Based Real-Time and Industrial Communications," Proceedings of the IEEE, vol. 93, no. 6, pp. 1102 - 1117, 6 JUNE 2005.
2. Sameer Chouksey, Hariram Selvamurugan Satheesh, Johan Åkerberg, "Coexistence, An Experimental Study of TSN-NonTSN," in 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), NV, USA, 2021.
3. V. GOLLER, "Time Sensitive Networks For Industrial Automation Systems," Analog Devices, 2016. [Online]. Available:_ [Accessed 11 12 2021].
4. IEEE, Time-Sensitive Networking (TSN) Task Group, IEEE, 2016.
5. "IEEE P802.1AS-Rev/D8.0, Draft Standard for Local and Metropolitan Area Networks—Timing and Synchronization for Time Sensitive Applications," 2019. [Online]
6. IEEE, IEEE Std 802.1Qbv - Enhancements for Scheduled Traffic, IEEE, 2016.
7. Cisco, Time-Sensitive Networking:A Technical Introduction, U.S.: Cisco, 2017.

Authors Introduction

Dr. I-Hsien Liu

He is a research fellow in the Taiwan Information Security Center @ National Cheng Kung Univ. (TWISC@NCKU) and Dept. of Electrical Eng., National Cheng Kung Univ., Taiwan. He obtained his PhD in 2015 in Computer and Communication Eng. from the National Cheng Kung Univ.. His interests are Cyber-Security, Wireless Network, Group Communication and Reliable Transmission.

Mr. Li-Yin Chang

He received his B.S. degree from the Dept. of Communiciation Eng., National Chung Cheng Univ., Taiwan in 2020. He is acquiring the master's degree in Dept. of Electrical Eng./Institute of Computer and Communication Eng., National Cheng Kung Univ. in Taiwan.

Prof. Jung-Shian Li

He is a full Prof. in the Dept. of Electrical Eng,, National Cheng Kung Univ., Taiwan. He graduated from the National Taiwan Univ., Taiwan, with B.S. in 1990 and M.S. degrees in 1992 in Electrical Eng.. 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 Univ.. He serves on the editorial boards of the International Journal of Communication Systems.

Prof. Chuan-Gang Liu

He is an Associate Prof. in the Dept. of Applied Informatics and Multimedia, Chia Nan Univ. of Pharmacy and Science. He received the B.Sc. degree from the Dept, of Electrical Eng., Tam Kang Univ., in 2000. Then he graduated from the National Cheng Kung Univ. with M.S. and PhD degrees in Electrical Eng.QQ. His research interests are in the areas of optical networks control, wireless networks, EPON, VANET, network security, cloud computing and TCP performance analysis.