Towards Industrial Security Through Real-time Analytics

Prajjwal Dangal
Department of Computer Science
University of Colorado Colorado Springs
Colorado Springs, CO, USA
0000-0001-7835-3867

Gedare Bloom
Department of Computer Science
University of Colorado Colorado Springs
Colorado Springs, CO, USA
0000-0002-5677-7092

***Abstract*—Industrial control system (ICS) denotes a system consisting of actuators, control stations, and network that manages processes and functions in an industrial setting. The ICS community faces two major problems to keep pace with the broader trends of Industry 4.0: (1) a data rich, information poor (DRIP) syndrome, and (2) risk of financial and safety harms due to security breaches. In this paper, we propose a private cloud in the loop ICS architecture for real-time analytics that can bridge the gap between low data utilization and security hardening.**

***Index Terms*—industrial, real-time, security**

I. Introduction

Security of an ICS deals with the protection and resiliency of the underlying devices while making sure their services meet timing constraints. The timing constraints manifest in terms of high availability as well as real-time requirements, i.e., the necessity for these devices to perform tasks such as issuing control commands within a bounded amount of time. ICS security is a critical issue as demonstrated by attacks such as Stuxnet or the German Mill Attack [1]. The financial cost of such attacks can individually reach from millions to billions of dollars.

Although ICS attack surfaces are extremely broad, we focus on the aspect of attack detection at the Programmable Logic Controller (PLC) interconnect network specifically, relying on real-time analytics. PLCs are used widely in ICSs to relay commands and automate functions. In an attack scenario, real-time analytics of the network traffic could reduce the time to threat discovery and mitigation.

II. Approach & Background

We take real-time analytics to mean the streaming of data from a (plant) process through an algorithm to an output within a bounded time. As seen in Figure 1, that output may be presented to a Human Machine Interface (HMI) for an operator to observe, or relayed to another, potentially non real-time data processing pipeline, or even used to further the automation of the subject plant device. Historically, real-time analytics in ICS have been popular for prognostics and health management.

Standard IT security practices like strong passwords and certificates for authentication, and closing of unnecessary ports and services to reduce the attack surface also apply to ICSs. Real-time analytics can further enhance the arsenal of ICS operators to defend the infrastructure against attacks as well as zero day vulnerabilities.

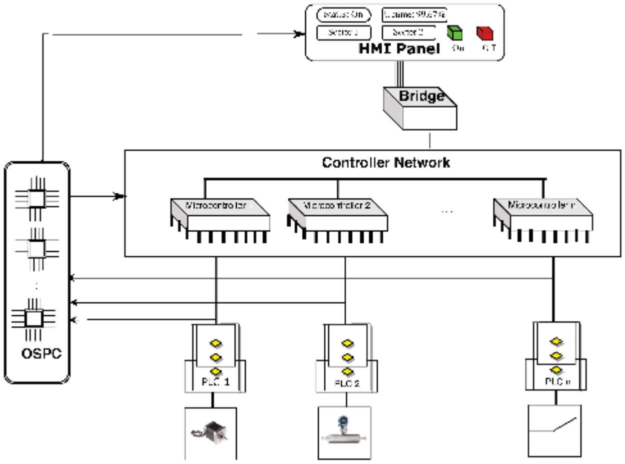

Fig. 1: An ICS architecture for real-time analytics.

We propose embedding an On Site Private Cloud (OSPC) within an ICS architecture to create a real-time plant data processing pipeline, as also shown in Figure 1. The figure shows a typical ICS architecture consisting of a HMI connected to the controller network connected to a layer of PLCs as well as the OSPC. Finally, the PLCs are connected to motors and sensors, which are also known as Process Connected Devices (PCD) and are the first point of telemetry data in an ICS. The PCD-PLC connection features real-time communication requirements, and the protocols employed are called Class C. The connection between the HMI and the Bridge does not have real-time requirements and the protocols used in that part of the architecture are called class A protocols [2]. Table I shows the response time of common ICS protocols [3]. Class C protocols have the lowest response times (latency), followed by class B while class A protocols are not time sensitive.

In our approach, we choose Open Powerlink protocol in conjunction with OSPC in order to create a real-time analytics based Intrusion Detection System (IDS). We believe an OSPC cloud-in-the-loop approach is superior for this application [4] because of its geographical proximity with the control system

This work is supported by NSF OAC-2001789

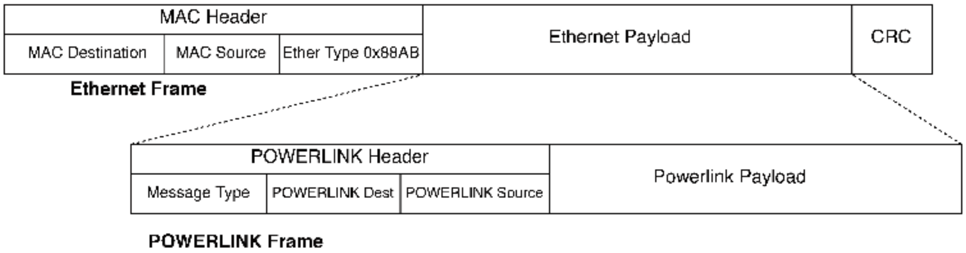

Fig. 2: Standard POWERLINK frame in an Ethernet frame

devices. Cloud-in-the-loop entails embedding cloud computing into a (control) loop with real-time guarantees.

Open Powerlink is the open sourced implementation of the Ethernet Powerlink protocol, which has both a hard and a soft real-time protocol. Powerlink's schedule is periodic TDMA with three phases: (i) Start of Cyclic (SoC) frame phase on which all nodes are synchronized, (ii) isochronous phase when messages with hard real-time deadline are transmitted, and (iii) asynchronous phase when non-time-critical messages are transmitted. Precision Time Protocol (PTP) is used for synchronization. Figure 2 shows the standard Powerlink frame.

Our prototype setup currently consists of hardware viz. Raspberry Pi 2, TP-Link Ethernet Switch, a workstation that has a CPU with four execution units each at 3.10 GHz and a 8 GB RAM. The software consists of Ubuntu 14 based lightweight Linaro OS, Open Powerlink network stack, tcpdump. We will subject our setup to attacks such as rogue frame insertion, electromagnetic interference, and timing synchronization attacks. We plan to evaluate and experiment with defense techniques such as IDS [5], cryptography, and logging. Currently, we are experimenting with inserting the relatively more powerful workstation into the network of the Pis to monitor network traffic with Wireshark, which supports Open Powerlink.

Protocol	Class	Response time
Profinet IRT	C	< 1 ms
Profinet RT	B	< 10 ms
Powerlink	B	< 1 ms
EtherCAT	C	0.1 ms
Sercos-III	C	< 0.5 ms
CC-Link IE	C	1 ms

TABLE I: Response times of common ICS protocols

III. Related Work

Closely related work in this field tackles this issue as an extension of big data analysis or in the context of defining protocol standards.

Lee et al. [6] and Rehman et al. [7] use big data analytics in an industrial architecture similar to Figure 1. Williams et al. [8] deal with high volume and low latency (high velocity) and outline benchmark analytics. Olufowobi et al. [9] developed a real-time based IDS in the automotive domain that identifies attacks as violations of response times.

Three relevant standards to our work are Time Sensitive Networking (TSN) [10], OSI data link layer's mac sublayer security [11], and Switched Ethernet [12]. In particular, the IEEE 802.1 AE standard outlines a set of integrity-related services including frame loss, frame ordering, and frame duplication, although we have observed that not all implementations adhere to the standard, especially the EtherCAT protocol [2].

IV. Conclusion

Real-time analytics addressing integrity attacks on real-time ICS networks is a nascent field with room for experimentation and innovation. We have described our work-in-progress to explore this field.

References

[1] K. E. Hemsley, E. Fisher *et al.*, "History of industrial control system cyber incidents," Idaho National Lab.(INL), Idaho Falls, ID (United States), Tech. Rep., 2018.

[2] E. D. Knapp and J. T. Langill, *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress, 2014.

[3] "The best ethernet protocol for your plc: 5 fieldbuses compared for industry 4.0," 2015-2016. [Online]. Available: https://www.automation.com/pdf_articles/kingstar/Best_Ethernet_Protocol_for_Your_PLC.pdf

[4] G. Bloom, B. Alsulami, E. Nwafor, and I. C. Bertolotti, "Design patterns for the industrial internet of things," in *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*. IEEE, 2018, pp. 1–10.

[5] C. Young, J. Zambreno, H. Olufowobi, and G. Bloom, "Survey of automotive controller area network intrusion detection systems," *IEEE Design & Test*, vol. 36, no. 6, pp. 48–55, 2019.

[6] J. Lee, H. D. Ardakani, S. Yang, and B. Bagheri, "Industrial big data analytics and cyber-physical systems for future maintenance & service innovation," *Procedia Cirp*, vol. 38, pp. 3–7, 2015.

[7] M. H. ur Rehman, E. Ahmed, I. Yaqoob, I. A. T. Hashem, M. Imran, and S. Ahmad, "Big data analytics in industrial iot using a concentric computing model," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 37–43, 2018.

[8] J. W. Williams, K. S. Aggour, J. Interrante, J. McHugh, and E. Pool, "Bridging high velocity and high volume industrial big data through distributed in-memory storage & analytics," in *2014 IEEE International Conference on Big Data (Big Data)*. IEEE, 2014, pp. 932–941.

[9] H. Olufowobi, C. Young, J. Zambreno, and G. Bloom, "Saiducant: Specification-based automotive intrusion detection using controller area network (can) timing," *IEEE Transactions on Vehicular Technology*, 2019.

[10] G. M. Garner, "Timing and synchronization for time-sensitive applications in bridged local area networks-draft v. 1.0," *The Interworking Task Group of IEEE*, vol. 802, 2007.

[11] "Ieee standard for local and metropolitan area networks-media access control (mac) security," *IEEE Std 802.1AE-2018 (Revision of IEEE Std 802.1AE-2006)*, pp. 1–239, 2018.

[12] I. E. Commission *et al.*, "Iec 61784-1," *Digital data communications for measurement and control-Part*, vol. 1.