ISSN: 2641-2039

Global Journal of Engineering Sciences

DOI: 10.33552/GJES.2021.09.000703

Iris Publishers

Mini Review

Leverage Programmable Networks to Increase Resilience of Future Industrial Control Systems

Hui Lin*

Department of Electrical, Computer, and Biomedical Engineering, University of Rhode Island, USA

***Corresponding author:** Hui Lin, Department of Electrical, Computer, and Biomedical Engineering, University of Rhode Island, USA.

Received Date: December 03, 2021

Published Date: December 21, 2021

Abstract

Modern industrial control systems (ICS) like power grids are gradually equipped with dynamic operational technology (OT) components. This environment makes traditional static-configured security solutions less effective. To deploy highly configurable security solutions in ICS, we propose to use software defined networking (SDN), a technology that can monitor and program communications networks at run-time. As a preliminary step, we propose to use SDN to create separate encrypted channels to protect various control applications to meet the security-performance trade-off at run time. This idea can inspire the design of nonintrusive security solutions in various and highly dynamic ICS environments.

Introduction

Industrial control systems (ICS) are advancing to their 4.0 era, featured by automation based on artificial intelligence (AI) advancement. Consequently, the static configuration in traditional ICS becomes dynamic and is gradually equipped with run-time reconfiguration capabilities. Taking power grids as an example, many third-party distributed energy resources, e.g., solar panels or wind plants, can freely join and leave a power grid according to the request of load demands. That reconfigurable operational technology (OT), such as the one used in Microgrid, can increase operational efficiency and reduce management costs [1].

However, reconfigurable ICSs face new security challenges. Many security solutions designed for the information technology (IT) networks used by ICSs are designed and evaluated based on a few configurations and a static set of control devices, including intelligent electronic devices (IED), human-machine interfaces (HMI), and programmable logic controllers (PLCs). When OT configurations change, the security solutions can work in a nonoptimal condition, leaving backdoors in OT components and introducing significant overhead. While some ICSs are starting to use advanced network infrastructure like software-defined networking (SDN), there is still a long and winding road to fully exploit SDN's potential [2]. For example, utility companies, such as Schweitzer Engineering Laboratories (SEL), automate statically defined configuration of networks according to OT operations. Work in [3] adds a complementary layer of security mechanisms for intrusion detections by leveraging SDN's global visibility in its network control plane. When an attack or an incident happens, ICS can benefit from SDN's capability of reconfiguring communications networks (also known as network programmability) to isolate mal-functioned devices. Despite all those efforts, there is a lack of understanding on how SDN can evolve security solutions when facing the changes of ICS configurations.

This concept paper aims to present a preliminary design of programmable security solutions based on SDN technology to accommodate run-time OT reconfigurations in ICSs. Regardless of the specific algorithms that they are using, security solutions are strongly driven by data regarding the OT components exchanged through communications networks. Therefore, we propose to leverage SDN to monitor and manipulate network flows to adjust the data used by different security solutions while OT configurations are changing. We mainly use power grids as an example ICS and fundamental encryption/decryption as an example security solution. In general, encryption/decryption is challenging to implement in power grids, because the latency due to cryptographic operations can jeopardize real-time communications used to deliver critical control operations [4]. By exploiting SDN's programmability on communication networks, we can allocate resources to perform a specified level of encryption/decryption according to control applications' quality-of-service (QoS) requirement, realizing usable security practices in this critical infrastructure.

Main Design

Threat Model: We will assume that an unauthorized adversary can achieve unrestricted access to one or more systems in ICS internal control networks, serving as a foothold to perform integrity attacks, in which the adversary can inject and compromise network packets that piggyback control commands or measurement ata. We are interested in detecting an adversary's activity after he or she has already gained such access, since the initial break-in typically follows common attack vectors (e.g., stealing credentials, exploiting vulnerable software exposed to the outside world, or accessing backdoors intended for maintenance). We trust that devices at field sites (e.g., legacy sensors and actuators) report correct measurements and execute the received commands; attacking them requires physical access. Also, we trust the integrity of lightweight SDN controller applications, network switches to which the SDN controller is attached, and the communication channels connecting them. These assumptions are typical in work that studies attacks targeting SDN [5].

System Model: We are interested in smart power grids, in which OT components can experience unprecedented dynamics triggered by off-the-shelf computing and network technologies. For example, according to different configurations, an IED can have multiple functions, like a programmable relay or a PMU (phasor-measurement unit). Because protecting a relay and a PMU can require different security approaches, it is critical to use SDN's programmability to minimize the response time of reconfiguring security approaches while ICSs reconfigure their physical devices.

Design Overview: SDN's vantage points lie in global monitoring capabilities and dynamic network flow manipulation, enabling programmable, non-intrusive, and end-to-end protection. We present the overall infrastructure in Figure 1 to demonstrate these benefits from SDN.

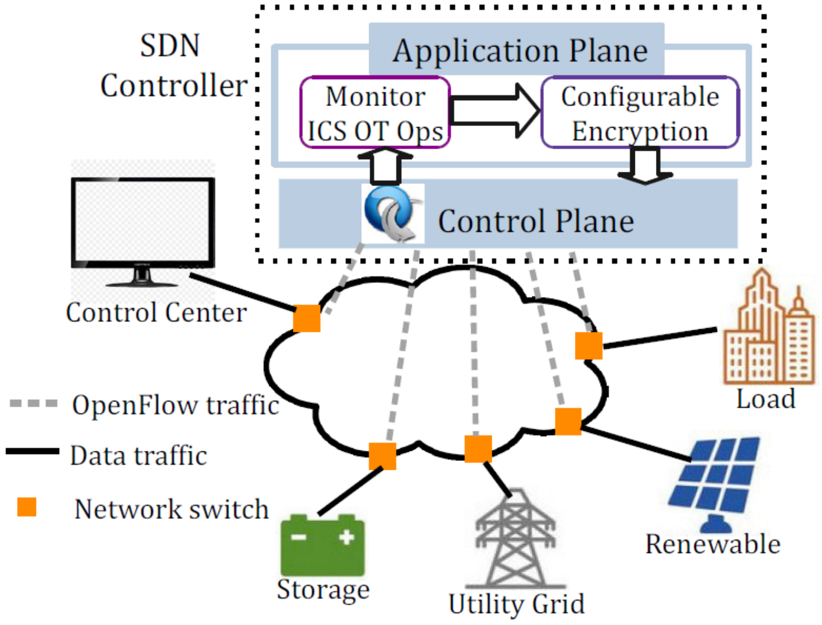

Figure 1: SDN-based infrastructure to enable programmable security solutions.

While control commands or measurements related to ICS' OT components enter a communications network at its perimeter (e.g., through network switches), they are intercepted by an SDN controller, usually deployed in a general-purpose computer. The SDN controller leverages a control plane and standard southbound protocol (like OpenFlow) to communicate with network switches at the perimeter, enabling end-to-end protections on the control commands and measurements. For example, when a PLC issues a network packet to report its health status, it is forwarded from the network switch at the first stop of its communication path to the SDN controller, which performs encryption or other security approaches. When the packet reaches the last stop of the communication path, the network switches forward it to the SDN controller again for decryption. Finally, the destination device can receive the original packet.

In addition, the SDN controller provides an application plane for third parties to develop northbound applications. We propose to implement reconfigurable security solutions as northbound applications to process network packets without instrumenting existing physical devices, making the solutions non-intrusive.

Specifically, we consider encryption/decryption as an example security solution in this concept paper. Encryption/decryption serves as a foundation for digital signature and authentication, common in general purpose computing environments to protect devices from integrity attacks. Consequently, we propose to use the high-performance SDN controllers to build separate encrypted channels for devices and operations that present different QoS requirements. For example, a relay and a PMU have different delivery latency on measurement data. When the packets from these two types of devices are forwarded to the SDN controller, we can use their lower-layer information to identify their source devices and select different encryption mechanisms. By doing this, we can maintain virtually separate communications to meet different performance security trade-offs of those devices on top of the same physical links. Performing encryption/decryption through switches or routers is similar to the setups of virtual private networks. However, SDN can further remove complicated configurations in network switches, reducing the complexity in its easy-to-use application plane.

Furthermore, this design can move beyond using SDN to merely implement encryption and decryption. Even though an SDN controller's high-end computation capability can help reduce the overhead of encryption and decryption, we will further reduce such overhead by dynamically configuring the encryption parameters and the range of data to apply it. For example, research efforts on a false data injection attack identify a critical set of data, the compromise of which can mislead the critical state estimation application into making damaging operations. Instead of applying encryption on all data, we can encrypt only a critical set of data, whose range can be determined based on the study in [6]. One important challenge of applying this idea is that the specific set of critical data varies in operational conditions and OT configurations continuously. We can still overcome this challenge with SDN's capability of parsing network packets according to their application payload, from which we can extract knowledge like run-time operating conditions.

Conclusion

In this concept paper, we demonstrate an idea of exploiting SDN's programmability on communication networks to achieve configurable security solutions. Based on the monitoring of run-time behavior of target ICS systems, we can configure security solutions to meet the performance-security trade-off and specifically focus on critical applications that require protection. Our follow-up work will perform experiments based on our previous development experiences on SDN and power grids, evaluating the idea's feasibility in actual ICS environments.

Acknowledgement

None.

Conflict of Interest

No conflict of interest.

References

1. H Jiayi, J Chuanwen, X Rong (2008) A review on distributed energy resources and MicroGrid. Renewable and Sustainable Energy Reviews 12(9): 2472-2483.
2. X Dong, H Lin, R Tan, RK Iyer, ZT Kalbarczyk (2013) Software-defined networking for smart grid resilience: opportunities and challenges. in the Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, pp. 61-68.
3. N Sultana, N Chilamkurti, W Peng, R Alhadad (2018) Survey on SDN based network intrusion detection system using machine learning approaches. Peer-to-Peer Network Applications 12: 493-501.
4. (2005) IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation. in IEEE Std 1646-2004, pp. 1-36.
5. L Xu, J Huang, S Hong, J Zhang, G Gu (2017) Attacking the brain: Races in the SDN control plane. in the Proceedings of 26th USENIX Security Symposium (USENIX Security 17), pp. 451-468. USENIX Association.
6. RB Bobba, KM Rogers, Q Wang, H Khurana, K Nahrstedt, et al. (2010) Detecting false data injection attacks on DC state estimation. presented at 1st Workshop Secure Control Syst. (SCS), Stockholm, Switzerland.