2018 9th ACM/IEEE International Conference on Cyber-Physical Systems

Demo Abstract: An Industrial Control System Testbed for the Encrypted Controller

Xing Li, Mengxiang Liu, Rui Zhang, Peng Cheng, Jiming Chen
State Key Lab. of Industrial Control Technology
Zhejiang University
Hangzhou, P.R. China
xlee@zju.edu.cn, liumengxiang329@gmail.com, rcheung@zju.edu.cn, pcheng@iipc.zju.edu.cn, cjm@zju.edu.cn

***Abstract*—The encrypted controller is a novel and promising approach for enhancing the security of industrial control systems [1]. This approach encrypts both the signals that transmitted over communication channels and the control law, so as to protect all information of a plant and its controller from attackers. However, in spite of considerable research efforts [2]–[12], the encrypted controller is still quite far from its implementation and application in industrial control systems. In-depth experimental studies are necessary for bridging the gap between theory and application of the encrypted controller. In this demonstration, we present an industrial control system testbed for experimental studies of the encrypted controller. Moreover, we carry out an experimental study that improves and evaluates the security of the industrial control system which comprises the encrypted controller using the testbed.**

***Index Terms*—Industrial Control Systems, Encrypted Controller, Security Testbed, Experimental Study**

I. Introduction

In recent years, the frequently happened security incidents related to industrial control systems have made the researchers aware of the importance and urgency of enhancing the security of industrial control systems. Specifically, the encrypted controller is a novel and promising approach for enhancement of the security of industrial control systems. The concept of the encrypted controller was originally proposed in 2015 [1] and since then the emerging idea has been receiving progressively more attention. The key idea of the encrypted controller is to use homomorphic encryption schemes to encrypt not merely the signals over communication links but also the control law inside the controller. Compared with the conventional approach which only encrypts the transmission signals over communication links, the encrypted controller enables cryptography-based protection for the controller and decreases the number of sites that hold private keys. Therefore, implementation and application of the encrypted controller is meaningful for achieving the security-enhanced industrial control systems. However, the existing works about the encrypted controller mainly focus on the theoretical research, which lacks the engineering realization and the experimental research in practical industrial control systems. In order to bridge the gap between theory and application of the encrypted controller, it is necessary to build up an industrial control system security testbed and carry out experimental studies of the encrypted controller.

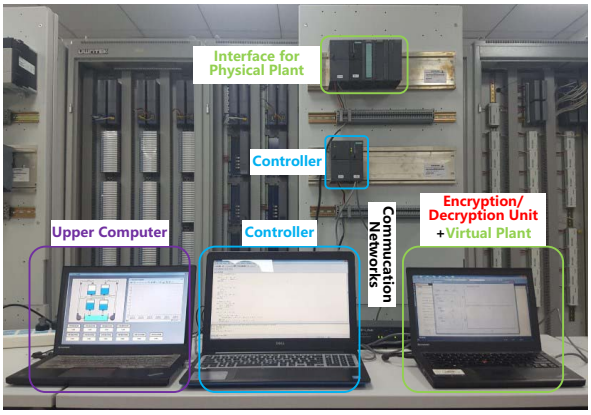

Fig. 1. The physical structure of the testbed.

II. Testbed

The main goal of the proposed testbed is to support implementation and experiments of the encrypted controller in industrial control systems. Considering the requirements for carrying out experiments in practical systems, we carefully develop an industrial control systems testbed (Figure 1). The testbed consists of five parts: the controller, the plant, the encryption/decryption unit, the communication networks and the upper computer. The controller integrates a PLC (Programmable Logic Controller) and a PC (Personal Computer) to perform the calculation of the encrypted control law. The plant includes not only a simulator for virtual plants, but also a interface for physical plants, to provide various types of controlled objects. The encryption/decryption unit implemented by a PC-based solution is used to encrypt and decrypt the messages that are exchanged between controller and field devices. In our testbed, there are two communication networks: field network and control network. The controller communicates with sensors and actuators through the field network. The controller communicates with the upper computer via control network. The upper computer enables us to visualize and control industrial processes. Meanwhile, for the convenience of the experimental research in the testbed, we provide a framework for rapid application development. The testbed serves as a powerful tool for verifying, evaluating and

0-7695-6378-3/18/$31.00 ©2018 IEEE
DOI 10.1109/ICCPS.2018.00045

improving the encrypted controller theory. Further, it features fidelity, flexibility and user-friendliness.

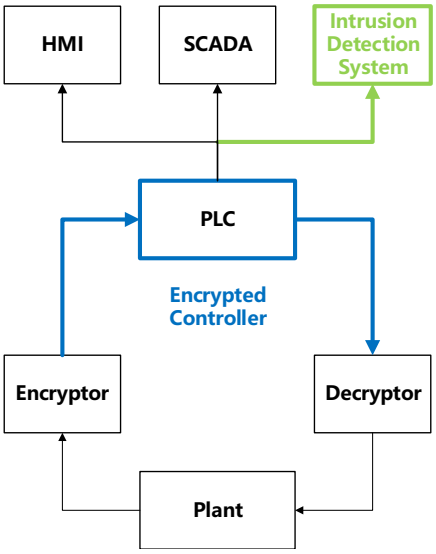

Fig. 2. The schematic diagram of the improving scheme.

III. Demonstration

Although the testbed can be used for different experimental studies of the encrypted controller, this demonstration focuses on improving and evaluating the security of the industrial control system which comprises the encrypted controller. As a cryptography-based approach, the encrypted controller encrypts both the signals over communication links and the signals inside the controller to enhance the security of industrial control systems against attackers. However, the encrypted controller is hard to respond to attacks actively and the industrial control system which only uses the encrypted controller is hard to protect against several attacks such as false data injection attacks. In order to improve the security of the industrial control system which uses the encrypted controller, this demonstration presents an improving scheme (Figure 2) that combines the encrypted controller with the intrusion detection system and is able to very well display respective advantages of these two approaches. Further, the improving scheme makes the encrypted controller and the intrusion detection system stimulate one another for common development. In this demonstration, we show that the proposed improving scheme can play an important role in defending against stealthy attack. We demonstrate why the encrypted controller and the intrusion detection are able to stimulate one another for common development and show how we combine the encrypted controller with the intrusion detection system to defend against stealthy attack (Figure 3, 4).

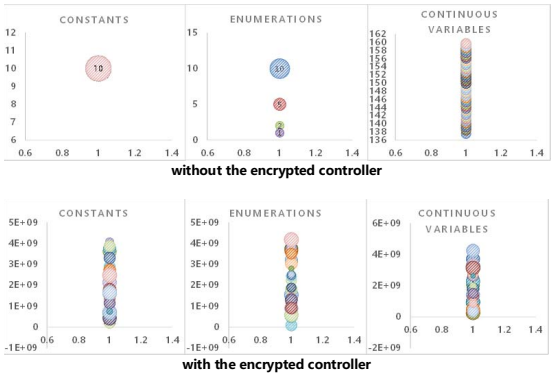

Fig. 3. Results of classification using the normal or encrypted signals.

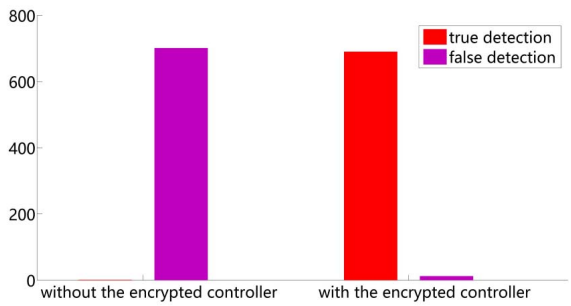

Fig. 4. Comparison of detection results with/without the encrypted controller.

References

[1] Kogiso, Kiminao, and T. Fujita. "Cyber-security enhancement of networked control systems using homomorphic encryption." Decision and Control IEEE, 2016:6836-6843.

[2] Kim, Junsoo, et al. "Encrypting Controller using Fully Homomorphic Encryption for Security of Cyber-Physical Systems." Ifac Papersonline 49.22(2016):175-180.

[3] Farokhi, Farhad, I. Shames, and N. Batterham. "Secure and Private Cloud-Based Control Using Semi-Homomorphic Encryption." IFAC-PapersOnLine 49.22(2016):163-168.

[4] Fujita, T, et al. "Security enhancements of networked control systems using RSA public-key cryptosystem." Control Conference IEEE, 2015:1-6.

[5] Farokhi, Farhad, I. Shames, and N. Batterham. "Secure and private control using semi-homomorphic encryption." Control Engineering Practice 67(2017):13-20.

[6] Chen, Jiming, et al. "Narrow-Band Internet of Things: Implementations and Applications." IEEE Internet of Things Journal PP.99(2017):1-1.

[7] Ishikawa, Kazuto, et al. "Experimental Validation of Encrypted Controller Implemented on Raspberry Pi." IEEE, International Conference on Cyber-Physical Systems, Networks, and Applications IEEE, 2016:1-6.

[8] Shoukry, Yasser, et al. "Privacy-aware quadratic optimization using partially homomorphic encryption." Decision and Control IEEE, 2016:5053-5058.

[9] Darup, Moritz Schulze, et al. "Towards Encrypted MPC for Linear Constrained Systems." IEEE Control Systems Letters 2.2(2017):195-200.

[10] Seong, Jeongmo, et al. "Encrypting Controller Based on Homomorphic Encryption and Application to Path Stabilization of Autonomous Vehicle." INFORMATION AND CONTROL SYMPOSIUM 2017.

[11] Zhao, Chengcheng, et al. "Consensus-Based Energy Management in Smart Grid With Transmission Losses and Directed Communication." IEEE Transactions on Smart Grid 8.5(2017):2049-2061.

[12] Yang, Guang, et al. "Promoting Cooperation by the Social Incentive Mechanism in Mobile Crowdsensing." IEEE Communications Magazine 55.3(2017):86-92.