

# Security Assist Mechanisms for Industrial Control Systems with Authentication

Chia-Wei Tsou\*, Yi-Wei Ma \*, Yi-Hao Tu\* and Jiann-Liang Chen\*

\* Department of Electrical Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan.

m10907517@mail.ntust.edu.tw, ywma@mail.ntust.edu.tw, d11107005@mail.ntust.edu.tw, Lchen@mail.ntust.edu.tw

**Abstract**— Due to a lack of identification and authentication in the communication protocol used for industrial control systems. It is easy for an intruder to forge false information or impersonate a device to send inappropriate commands to other devices, causing them to malfunction or be damaged. This study designs three kinds of identity security mechanisms used in industrial control communication protocols: central control, device to device (D2D), and a hybrid mechanism combining the above two. Using the proposed mechanism can prevent intruders from disguising as legitimate devices to join the industrial network, resulting in information tampering or equipment impersonation.

**Keywords**— Industry control system, security, central control, device to device (D2D), hybrid.

## I. INTRODUCTION

Industrial control systems (ICS) and their communication protocols pervade nearly every industry and critical infrastructure, such as manufacturing, power, transportation, etc. Modbus protocol is one of the commonly used protocols in industrial control systems. It is a communication protocol based on a master/slave architecture with high availability for connecting industrial electronic devices [1], and is easy to deploy and maintain. Modicon released Modbus in 1979 for programmable logic controller (PLC) communications. PLCs are designed to operate only in closed industrial control system networks. Therefore, Modbus only needs to focus on reducing resource requirements and improving generality and thus lacks many security properties such as authentication, encryption, and integrity [2]. However, more and more industrial control systems have been connected to the Internet. The security of the Modbus protocol is insufficient, resulting in industrial control systems becoming the target of cybercrime.

There are many international standards that can be used to solve ICS security issues, such as IEC 62443 or NIST 800-82 and so on. Although the focus of different standards is different, because the purpose is to protect the information security of ICS, the same topic is mentioned in many different standards, such as authentication, system integrity. Because of the main reason for the frequent occurrence of data tampering or stealing and replay attacks in industrial control systems is that the communication protocol lacks an authentication protection mechanism during data transmission, which makes it easy for illegal intruders to launch attacks [3], and some studies have found that although the common ICS suppliers provide security

events, there are still serious vulnerabilities in the authentication mechanism, for example, lack of random numbers [4]. In recent years, many researchers have paid attention to the issue of authentication of ICS and Industrial Internet of Things (IIoT) [5–8], so this article will focus on authentication of ICS to help improve the information security of ICS.

This study proposes a mechanism to allow authentication of industrial control communication protocols such as Modbus to improve their security and prevent intruders from maliciously forge as legitimate devices to join the industrial network, resulting in information theft or tampering.

## II. MECHANISM AND ITS ADVANTAGES AND DISADVANTAGES

### A. Central Control

All devices are certified by the central control station through which data is transmitted, as shown in Fig. 1. The advantage is that it avoids repeated verification. The disadvantage is that it requires a central control device, increasing the delay because the data should be transmitted multiple times.

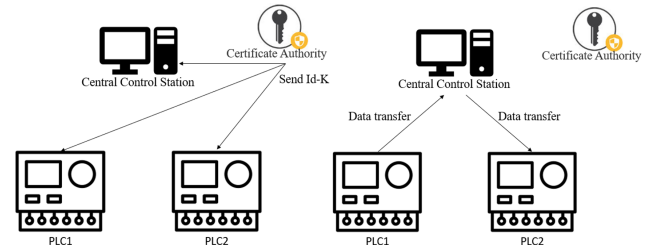


Figure 1. The two-step procedure of central control.

### B. Device to Device (D2D)

The device and device (D2D) authenticate to confirm that the other is a trusted device, as shown in Fig. 2. The advantage is that it can save resources and reduce delay, and the disadvantage is that each device needs to be authenticated. If there are  $n$  devices, then  $C_2^n$  authentications must perform, and there are still some security risks.

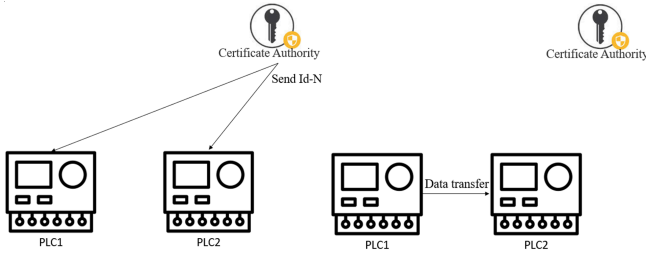


Figure 2. The two-step procedure of Device to Device (D2D).

### C. Hybrid

After the device is authenticated, the central control station informs the other devices that the device is credible, as shown in Fig. 3. The advantage is that it can avoid repeated authentication, and the disadvantage is that a central control device is required. The delay will increase due to waiting for the central control station to notify the remaining devices.

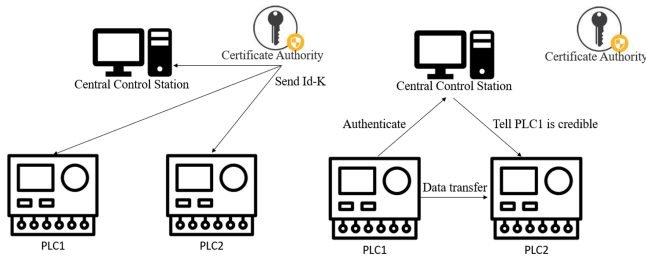


Figure 3. The two-step procedure of hybrid.

## III. CONTENT OF THE MECHANISM

### A. Central control

In the initialization, embed the same Identification Key (Id-K) in all devices through the Certificate Authority (CA).

- $Device_{send}$  uses the public key to encrypt the Id-K and transmit it to the central control station.
- The central control station decrypts with the private key.
- If the data obtained after decryption is equal to the Id-K issued by the CA, then  $Device_{send}$  is authenticated.
- The central control station asks  $Device_{send}$  for the data to be sent to  $Device_{receive}$ .
- The central control station updates the public key and private key, and broadcasts the public key to all devices.
- The central control station requires  $Device_{receive}$  to encrypt the Id-K with the public key and transmit it to the central control station.
- The central control station decrypts with the private key.
- If the data obtained after decryption is equal to the Id-K issued by the CA, then  $Device_{receive}$  is authenticated.

The central control station sends the data sent by  $Device_{send}$  to  $Device_{receive}$ .

### B. Device to Device (D2D)

In the initialization, the Identification Number (Id-N) embed in all devices through the CA, each Id-N in a device is different, and after any two Id-N are hashed, the same string can be obtained, and the string will also be stored on all devices.

- $Device_{send}$  request  $Device_{receive}$  to communicate.
- $Device_{receive}$  request  $Device_{send}$  send its  $Id-N_{send}$ .
- $Device_{receive}$  hashes  $Id-N_{send}$  and  $Id-N_{receive}$  to obtain a hash value.
- If the calculated hash value is equal to the string stored in the device,  $Device_{send}$  is authenticated by  $Device_{receive}$ .

- $Device_{receive}$  asks  $Device_{send}$  to send data.

The hash function is a one-way function, it can be a simple function, like A plus B and then take the remainder, but it will make the security drops.

### C. Hybrid

In the initialization, embed the same Identification Key (Id-K) in all devices through the CA.

- $Device_{send}$  uses the public key to encrypt the Id-K and transmit it to the central control station.
- The central control station decrypts with the private key.
- If the data obtained after decryption is equal to the Id-K issued by the CA, then central control tell  $Device_{receive}$  that  $Device_{send}$  is credible.
- $Device_{receive}$  asks  $Device_{send}$  to send data.

## IV. CONCLUSIONS

Based on cryptography, this paper proposes three verification methods (central control, D2D, and hybrid) to solve the problem that the original industrial control protocol lacks a verification mechanism. It can improve the lack of defense capabilities and ultimately improve the security of industrial control protocols.

## REFERENCES

- [1] T. S. Hugo, U. O. Claudio, K. M. John and O. Alvarado-Cando, "Hamming Code to Data Protection in a Modbus Industrial Communication: Experimental Results," Proceedings of the IEEE Third Ecuador Technical Chapters Meeting, pp. 1-5, 2018.
- [2] H.C. Chang, C.Y. Lin, D.J. Liao and T.M. Koo, "The Modbus Protocol Vulnerability Test in Industrial Control Systems," Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, pp. 375-378, 2020.
- [3] W. Jingran, L. Mingzhe, X. Aidong, H. Bo, H. Xiaojia and Z. Xiufang, "Research and Implementation of Secure Industrial Communication Protocols," Proceedings of the IEEE International Conference on Artificial Intelligence and Information Systems, pp. 314-317, 2020.
- [4] A. Ayub, H. Yoo and I. Ahmed, "Empirical Study of PLC Authentication Protocols in Industrial Control Systems," Proceedings of the IEEE Security and Privacy Workshops, pp. 383-397, 2021.
- [5] D. Xu, K. Yu and J.A. Ritcey, "Cross-Layer Device Authentication with Quantum Encryption for 5G Enabled IIoT in Industry 4.0," IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 6368-6378, 2022.
- [6] A. Esfahani, G. Mantas, R. Matischek, F.B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M.G. Tauber, C. Schmittner and J. Bastos, "A Lightweight Authentication Mechanism for M2M Communications in

Industrial IoT Environment," IEEE Internet Things Journal, vol. 6, no. 1, pp. 288-296, 2019.

- [7] A. Karati, S. H. Islam and M. Karuppiah, "Provably Secure and Lightweight Certificateless Signature Scheme for IIoT Environments," IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3701-3711, 2018.
- [8] L. Yang, W. Tong, Z. Li and Y. Wu, "Authentication Scheme for Distributed Industrial Control System Terminals," Proceedings of the International Conference on Electronic Information Technology and Computer Engineering, pp. 1005-1012, 2021.



**Chia-Wei Tsou** is a graduate student at National Taiwan University of Science and Technology. He received a bachelor's degree in Electrical Engineering from National Taiwan University of Science and Technology. His research interests include the industrial control system.



**Yi-Wei Ma** is an assistant professor in National Taiwan University of Science and Technology. His research interests include Internet of Things, Cloud Computing, and Future Network.



**Yi-Hao Tu** received his B.S. and M.S. degrees from the National Quemoy University, Kinmen Taiwan, in 2020 and 2022, respectively. He is currently a doctoral's student at electrical engineering at National Taiwan University of Science and Technology, Taipei, Taiwan. His current research interests include reinforcement learning, wireless networks and software defined networks.



**Jiann-Liang Chen** Prof. Chen was born in Taiwan on December 15, 1963. He received the Ph.D. degree in Electrical Engineering from National Taiwan University, Taipei, Taiwan in 1989. Since August 1997, he has been with the Department of Computer Science and Information Engineering of National Dong Hwa University, where he is a professor and Vice Dean of Science and Engineering College. Prof. Chen joins the Department of Electrical Engineering, National Taiwan University of Science and Technology, as a Distinguished professor and Dean now. His current research interests are directed at cellular mobility management, cybersecurity, personal communication systems and Internet of Things (IoT).