Computers, Materials & Continua
DOI:10.32604/cmc.2022.021020
Article

Tech Science Press

PLC Protection System Based on Verification Separation

Xiaojun Pan[1], Haiying Li[2], Xiaoyi Li[1], Li Xu[1] and Yanbin Sun[1,*]

[1]Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou, 510000, China
[2]School of Science and Engineering, Laval University, Quebec, G1V0A6, Canada
*Corresponding Author: Yanbin Sun. Email: sunyanbin@gzhu.edu.cn
Received: 19 June 2021; Accepted: 29 September 2021

Abstract: Supervisory control and data acquisition systems (SCADAs) play an important role in supervising and controlling industrial production with the help of programmable logic controllers (PLCs) in industrial control systems (ICSs). A PLC receives the control information or program from a SCADA to control the production equipment and feeds the production data back to the SCADA. Once a SCADA is controlled by an attacker, it may threaten the safety of industrial production. The lack of security protection, such as identity authentication and encryption for industrial control protocols, increases the potential security risks. In this paper, we propose a PLC protection system combined with a monitor between a SCADA and a PLC and a physically separated monitoring station. By using the PLC protection system, identity verification and command verification are separated, and both the identity of the operator and the corresponding commands are recorded. Experiments show that even if the SCADA is controlled by an attacker, our system could still protect the PLC in the field and record the identity of the key command operator, which facilitates the tracing and forensics of malicious activities.

Keywords: ICS; SCADA; PLC security

1 Introduction

Industrial control systems (ICSs) are widely used in power, sewage, petrochemical, and other social infrastructure industrial facilities. Industrial control systems generally consist of programmable logic controllers, human-machine interfaces (HMIs), remote terminal units (RTUs), etc. With the development of information technology and internet technology, traditional industrial control systems that used to be physically isolated from the internet are being networked and becoming more intelligent [1]. To separate monitoring and control, traditional protocols in industrial systems are gradually adopting TCP from traditional networks. For example, the Modbus protocol is extended to be a Modbus TCP. However, the original industrial control protocols lack security measures such as authentication and data encryption. As these hidden dangers are gradually exposed, industrial systems connected to a public network or a corporate office network are becoming increasingly more vulnerable.

HMIs and engineering stations have a high level of control over local PLCs, which could lead to production accidents and financial losses if attackers gain control of the HMIs and engineering stations. For example, Stuxnet used the vulnerabilities of the WinCC software in HMI to control WinCC, which can intercept the PLC data and send malicious commands [2]. In 2011, the water supply SCADA in Illinois was hacked, causing damage to water pumps [3]. In 2013, Israel's transport sector was attacked by hackers, resulting in large-scale traffic congestion [4]. In 2014, the Havex virus invaded the SCADA of the European and American Ministry of Energy [5]. In 2015, in the Ukrainian blackout, an attacker took control of an engineering station and remotely controlled the PLC through the engineering station, causing grid failure [6]. At the Black Hat Conference, hacker groups demonstrated a worm residing in a PLC. Once the worm infects a PLC, the worm can automatically seek out other PLCs on the LAN and replace the programs running in them, causing a massive infection [7]. In 2019, the Norsk Hydro aluminum plant was attacked by hackers, resulting in production interruption, the closure of several factories, and a 1.2% rise in the global aluminum price [8].

Fig. 1 shows the data of China's National Bureau of Statistics. The global industrial system is under increasingly more attacks. Industrial systems are widely used in water treatment, petrochemicals and other infrastructure. Industrial security is related to national security and people's livelihood. Increasingly more countries have realized the importance of industrial system security.

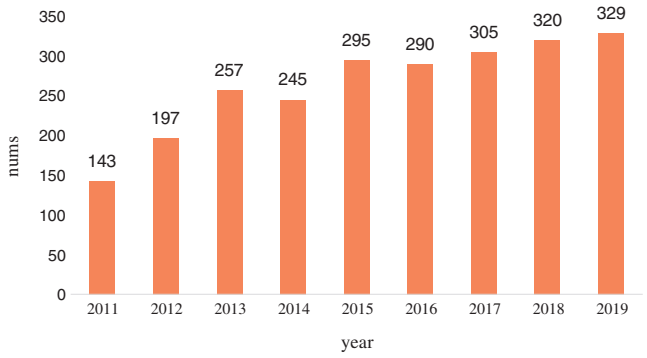

Figure 1: Attack trend of global industrial events

Currently, in industrial control systems, there are many security threats to monitoring systems and PLCs. The main problems are as follows.

(1) HMIs and engineering stations run on Windows or Linux operating systems with various vulnerabilities. Furthermore, the monitoring and configuration software running on them also has security vulnerabilities. Obviously, HMIs and engineering stations run in an unreliable environment. They are at risk of being controlled by attackers.
(2) HMIs and engineering stations lack identity management and records of the command type and the command time, making it difficult to trace related operations [9].
(3) The lack of authentication, data encryption, and other methods in industrial control system protocols makes communication traffic susceptible to eavesdropping and forging [10]. There is no way to verify the source of commands and their legitimacy.
(4) PLCs lack authentication and other security features. Their weak processing ability, firmware closure, lack of security control in industrial protocols and other reasons make them vulnerable.

To solve the problems above, we investigate a PLC protection system based on verification separation. The system consists of a monitoring station and a monitor. The monitoring station is

physically isolated from the industrial control network and the internet. It is used to monitor and intercept the data sent by the HMI, engineering station, or another component. Furthermore, the system uses data classification, traffic encryption, permission classification and other methods to ensure the safety of industrial production equipment when the HMI or engineering station is controlled by attackers. The key commands sent to the PLC are recorded, which is convenient for tracing the source of attack commands and traffic.

The remainder of this paper is organized as follows. Section 2 introduces the related work on PLC security, Section 3 describes the system architecture studied and the related methods, Section 4 presents our experimental results and evaluations, and Section 5 outlines our summary and future research.

2 Related Work

This work seeks to solve the problem of engineering stations or HMIs being maliciously controlled to send malicious codes and commands to PLCs. Malchow et al. [11] designed a PLC guard that decodes the MC 7 code of all Siemens PLC programs and compares it with previous versions by adding a guard between the PLCs and engineering stations. An engineer approves or rejects the code upload by physically interacting with the PLC guard. However, this method is not used to detect the relevant data sent to the PLC and is only used to detect the PLC code, and there is no ability to block malicious data injection. Zonouz et al. [12] proposed a method based on the symbolic execution of PLC code to detect PLC malicious programs. The method first reverses the security requirements and generates the corresponding unsafe requirements (UR). Then, it finds the path P that satisfies the conditions, where P is the Cartesian product of TEG and UR. If there is no path that satisfies the conditions, the code meets the security requirements and can be executed safely. The method determines the malicious code automatically. There is a path explosion problem during the path solving process. The detection efficiency of the method is relatively low. Due to automatic judgment, there is a possibility of misjudgment. Clark et al. [13] proposed a new defense framework that uses a set of randomized encryption keys to authenticate the control commands sent by a system operator to a PLC. The framework uses cryptographic analysis, control theory, and game theory methods to quantify the impact of malicious control instructions and to judge the relevant control instructions. This type of automatic judgment also has a certain false alarm rate. The false alarms may be a serious threat to site production safety. Lin et al. [14], based on the in-depth analysis of the Modbus protocol in industrial protocols, proposed a malicious intrusion detection method based on automatic learning. The method also has the same problem that it cannot intercept the relevant commands and gives false positives. Ponomarev et al. [15] proposed a method for detecting the ICS of an intruding network by measuring and verifying the data transmitted over the network. The intrusion detection system was able to achieve 94.3% accuracy in detecting attackers and engineering stations on the same network and 99.5% accuracy in detecting attackers and engineering stations on different networks. This automated judgment also has some problems with false alarm rates. Yau et al. [16] proposed using semisupervised machine learning to detect anomalous PLC behavior based on captured PLC memory address values. Halas et al. [17] proposed using encryption algorithms to encrypt data on PLCs to achieve the goal of data integrity. This approach has compatibility issues with existing protocols in use.

There is no effective way to solve the security problems of field equipment when an engineering station or HMI is controlled by an attacker. Bestak et al. [18] proposed an encryption algorithm for PLCs to encrypt data. This method has compatibility problems with the existing protocols and does not prevent a host computer from attacking a PLC after being controlled by hackers. Wardak et al. [19] believe that attacks on PLCs are all exploited to access PLCs without authorization vulnerability.

They propose that data security modules between PLCs and other equipment can solve this problem. However, the attacker can still use the host computer to attack the on-site devices. Zhang et al. [20] designed a state-based no-depth network deep packet inspection (DPI) system that can detect the payload of malicious network packets. This system cannot prevent attacks on field devices when the host computer is controlled. Figueroa-Lorenzo et al. [21] proposed a new role-based access control model (RBAC). The model uses the method of message authorization for roles and unit IDs to ensure the legitimacy of access. A unit ID is a unique identifier used to authorize the Modbus frame. This method can only prevent the external equipment from illegally operating the field equipment and cannot guarantee the security of the host computer under the control of the attacker. Lin et al. [22] proposed a malicious intrusion detection method based on automatic learning. They believed that in order to penetrate an industrial network, the ICS network topology must first be determined. There must be some abnormal traffic when an attacker launches an attack. However, this method cannot avoid attacks on field equipment after the host computer is controlled. Yong et al. [23] analyzed the interactive behavior of industry control protocols and used machine learning methods to collect physical fingerprint information of devices to model PLCs and physical devices. Then, the method uses this information to discover the abnormal behavior of the protocol and PLC.

3 PLC Protection System Based on Verification Separation

3.1 Industrial System Security Issues

A typical industrial control system architecture today, which includes an HMI, engineering stations, historical data servers, office networks, switches, firewalls, PLCs, and field devices, is shown in Fig. 2 [24]. An HMI is a device that allows an operator to monitor and control a production process. An engineering station is a workstation for engineers to use to configure, program, and modify a computer system [25]. A historical data server is a database server that records the history of the status of the process control system. The office network is connected to the production network through a firewall. A PLC, which can receive control commands from the HMI using industrial communication protocols, is a field device that can be connected directly to sensors, actuators, or other field devices [26].

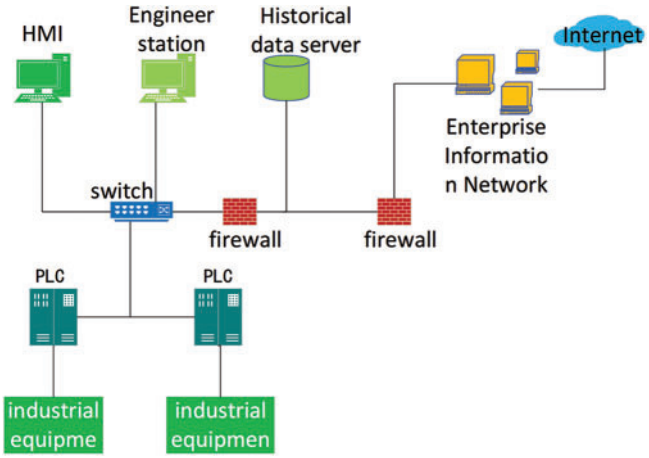

Figure 2: Industrial control system architecture

An HMI and engineering stations can control PLCs [27]. However, in industrial control systems, enterprise information networks and field control networks only use network firewalls for isolation.

Attackers can penetrate enterprise information networks into industrial control networks to attack a PLC. APT attacks are also a persistent high-threat attack: the attackers infiltrate the field control networks through a range of means and then further control an HMI or engineering station to take control of the field devices. Once an HMI or engineering station is controlled by an attacker, the attacker can intercept and tamper with normal data from employees' operations to attack field devices. This type of data tampering comes from an HMI or engineering station, making it difficult to intercept. The general attack path is shown in Fig. 3. Attackers use the vulnerabilities of the office network to attack the office network through the internet. The office network is then used to attack monitoring and collection systems, such as HMIs, engineering stations, or historical data servers. After controlling these devices, they use these devices to attack PLCs, such as through program tampering and data tampering.

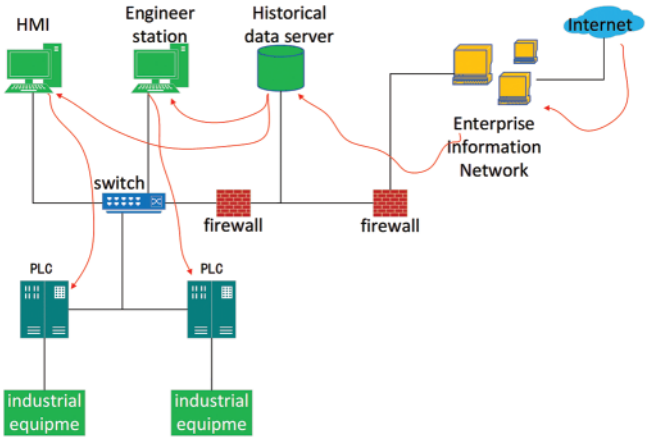

Figure 3: Attack path

Fig. 4 shows a simulation of an attack on a Ukrainian power plant. The attacker used the CVE-2014-4114 vulnerability in the office computer to attack the office computer. Then, the office computer was used to control the SCADA computer. This occurs because the SCADA computer is connected to the PLC. Access to the PLC does not require authentication, and the instructions are all in plain text. The attacker used the SCADA computer to send a stop command to the PLC to stop the field equipment, which caused a large-scale power outage.

The current protection methods based on traffic analysis, access control, and device monitoring cannot prevent a host computer from attacking a PLC after being controlled by a hacker. We need a new protection strategy and method to prevent hackers from using a host computer to attack field equipment. If we can authenticate the commands sent by a PLC on the host computer, it will greatly reduce the occurrence of such incidents. We design a PLC protection system based on verification separation. While protecting the verification server, the system verifies the legality of the instructions sent to the PLC without affecting the existing architecture.

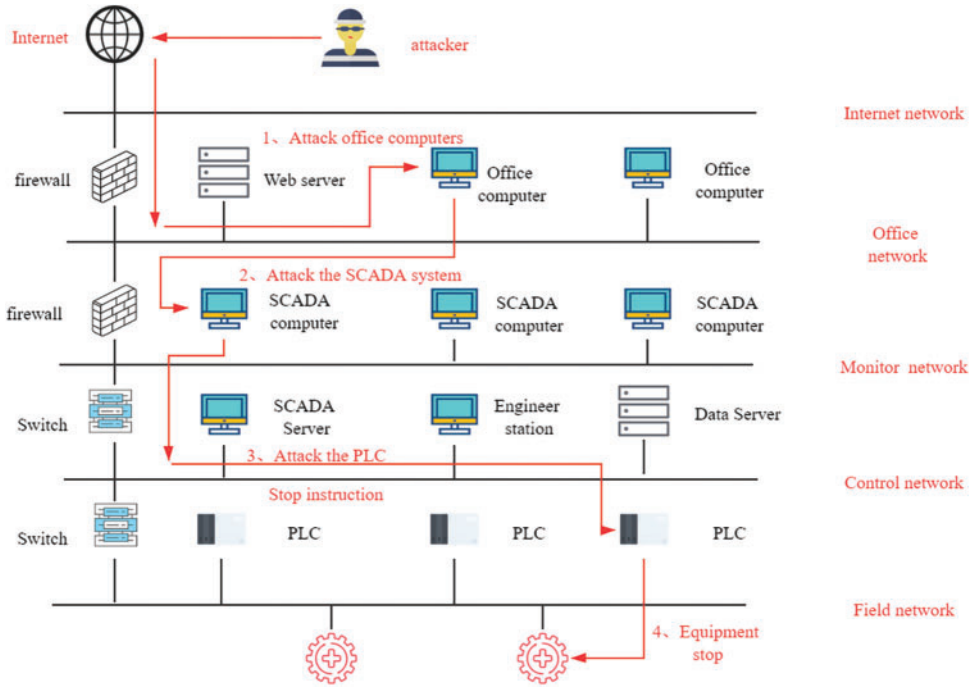

Figure 4: Ukrainian power outage

3.2 System Architecture

In order to solve the problems above, considering compatibility with existing industrial control systems, we designed a system that separates authentication from existing data transmission. Its architecture is shown in Fig. 5.

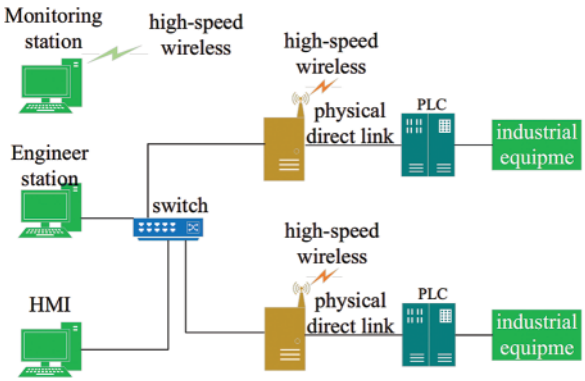

Figure 5: Validating the separated PLC system architecture

The system consists of a monitor, monitoring station and high-speed wireless network. The monitor is physically connected directly with the PLC while it is connected to the monitoring station using an independent high-speed wireless network. The monitor intercepts the commands transmitted to the PLC, encrypts the commands and transmits them to the monitoring station through the high-speed wireless network. The relevant commands are recorded for subsequent queries. The monitoring

station determines the legitimacy of the commands and authenticates the identity and privileges of the person who verifies the command. The high-speed wireless network uses a low latency network for communication between the monitoring station and the monitor. The high-speed wireless network is not connected to the existing industrial network to ensure physical isolation from the industrial network.

Its workflow is shown in Fig. 6. After the monitor receives the command from the HMI or the engineering station, it determines the type of command. If the command is a memory operation or a stop/start operation, the data will be encrypted and sent to the monitoring station. Then, the staff confirms the security of the data and sends an accept or reject command to the monitor. The monitor receives the command from the monitoring station and decides whether to discard the packet or forward it to the PLC device.

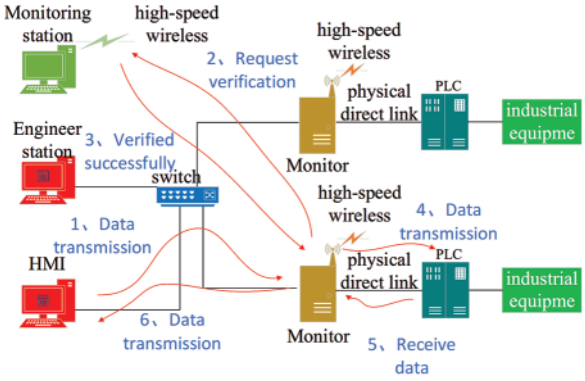

Figure 6: System workflow

The monitoring station is physically isolated from the industrial network, and unauthorized access to external devices is prohibited to ensure the credibility of the monitor's operating environment. The monitoring station and the monitor use encrypted communication methods to ensure the reliability of communication. The monitor is able to record the commands to ensure their traceability. The monitor will not forward data without the permission of the monitoring station, ensuring that external attacks cannot control the PLC.

3.3 PLC Protection System Model Based on Verification Separation

The data transmitted in industrial communication networks are divided into two types: real-time data and non-real-time data [28]. Non-real-time data include user program data, configuration data, and partial system state monitoring data. These data are not harsh regarding their real-time requirements and allow relatively long time delays [29]. Process monitoring and control application packet loss and jitter are less sensitive, and they can tolerate second-class transmission delays [30]. Therefore, we intercept the data transmitted from the HMI or engineering station to the PLC and analyze the commands. If the command is a memory operation command, such as uploading a data block, deleting a data block, writing memory, shutdown, or startup, we will send the encrypted data to the monitoring station through a high-speed wireless network. Considering that machine learning or deep learning methods have a certain false alarm rate, the accuracy of the model built for program changes or data changes will be drastically reduced for such data; therefore, we adopt the staff method to verify whether the data have been maliciously altered to ensure data security. We classify our staff members into four levels, as shown in Tab. 1 below.

Table 1: Employee privilege levels

Employee status	Rating	Competence
Super administrator	1	Add and delete administrators and not allowed to accept commands
Keeper	2	Add and delete general employees and engineers and accept all commands
Engineers	3	Accept all orders.
General staff	4	Only accept memory writes and stop and restart commands are allowed.

We also record the identities of the people in charge of the checks to ensure the traceability of such dangerous operations, thus providing some protection against malicious actions by internal employees. To ensure the uniqueness of the identity and the security of the key, we use a two-key method. These two types of keys are shared keys and private keys. The monitor transmits encrypted data to the monitoring station using a shared key that can be changed. Each staff member has his own unique private key. After the staff member reviews the data uploaded by the monitor, they encrypt the commands sent to the monitor with their own private key. The advantage is that even if the shared key is cracked or leaked, the data uploaded by the monitor may be tampered with, and the commands issued by the staff can still be guaranteed to have not been tampered with. In the case where the private key of a staff member is leaked, since everyone has their own unique private key and permission restrictions, the risk of the system being under complete control can also be reduced.

In order to reduce the security risk of the database, we separate the databases. The monitoring station and the monitor each have a database. The database of the monitoring station is used to store staff information, including permission information, communication keys, ID information, creators, creation information and the key index of the monitoring station. The key index stored by the monitoring station is the index of the staff keys in the monitor, which can be used to reduce table lookup time. The database in the monitor stores staff IDs, staff keys, creators, and permission information and records the relevant commands and times.

The model of the system is shown in Fig. 7.

The monitor consists of an encryption module, a decryption module, a control module, an authentication module, a database, and network card devices. The encryption module is responsible for encrypting the data from engineering stations or HMIs. The decryption module is responsible for decrypting the data from the monitoring station. The database is used to record information such as legal identity, authority level, private key, etc. The authentication module is responsible for classifying the data from engineering stations or HMIs. The network card is responsible for forwarding the data.

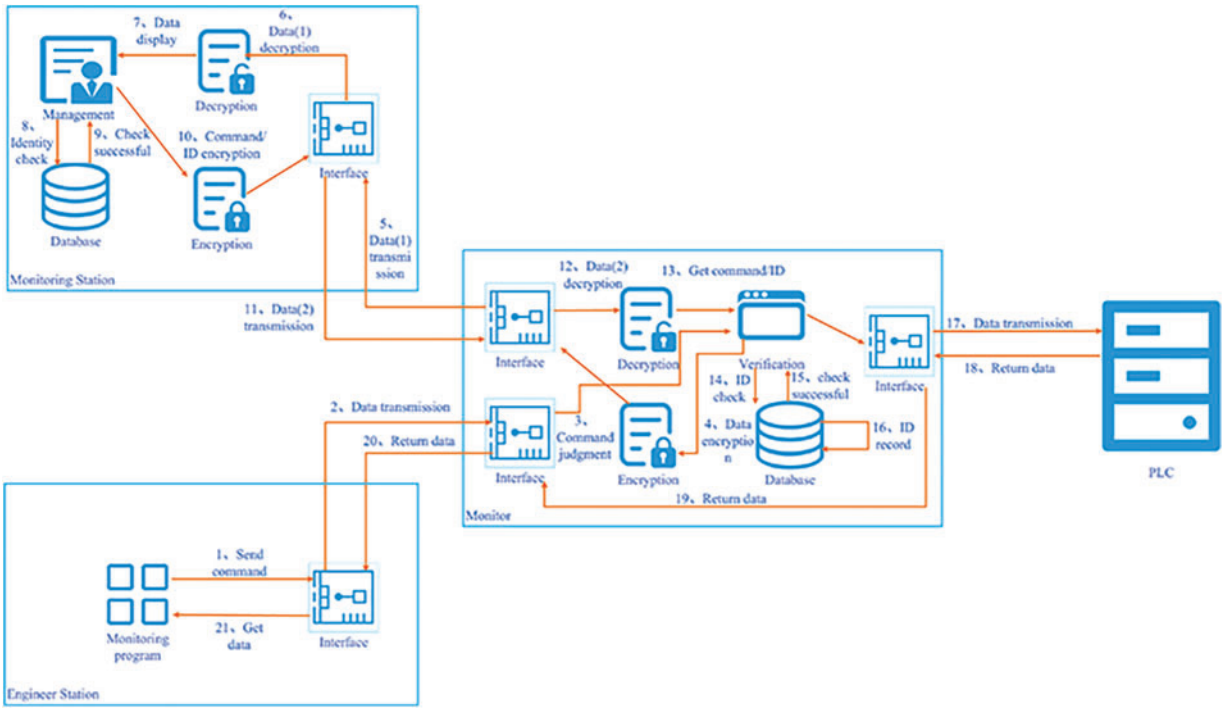

Figure 7: System model

The decryption module of the monitoring station is responsible for decrypting the data from the monitor. The encryption module is responsible for encrypting the data sent by staff to the monitor, such as commands, identities, and times. The client module is responsible for displaying the data sent by the monitor and verifying the identity of the staff. The database is used to store the staff's identity, the staff's private key, the private key index in the monitor and other data.

The engineering station and HMI are responsible for sending relevant commands or monitoring the PLC in the field. They consist of a control or monitoring program and a network card.

The engineering station sends the data to the monitor. The monitor encrypts the data and sends it to the monitoring station. The monitoring station performs command display, identity verification and command verification. Then the monitoring station encrypts the data and sends it to the monitor. The monitor confirms the identity based on the data and performs corresponding actions.

3.4 System Workflow

To ensure secure communication between the monitor and the monitoring station, we use an encryption method. Mainstream encryption algorithms are divided into symmetric and asymmetric encryption algorithms. An asymmetric encryption algorithm requires high computing resources and is generally only used for digital signatures. Therefore, we adopt symmetric encryption for encryption. The characteristics of the mainstream encryption methods are shown in Tab. 2 [31]. The AES algorithm has advantages in running speed, security, and resource consumption. Therefore, we adopt a 128-bit AES algorithm for encryption.

Table 2: Comparison of commonly used symmetric algorithms [32]

Encryption algorithm	Calculating speed	Security	Resource consumption
DES	Faster	Low	Medium
3DES	Slow	Medium	High
AES	Fast	High	Low

As shown in Fig. 8, first, the engineering station or HMI sends data to monitor [33]. The monitor receives the data and fetches the command to determine whether it is a memory operation, stop or start command. If the command is one of these commands, the monitor will encrypt the monitor's mac address, timestamp and data using PKr, a key shared with the monitoring station, to form the message {PKr (data, mac, Ts)}. Then, the monitor will send the message to the monitoring station. If this does not occur, the data will be forwarded directly to the PLC. Furthermore, the time monitoring will be started. After 30 s, if the monitoring station does not give a command, then the data will be discarded.

After receiving the data from the monitor, the monitoring station decrypts the data using PKr. Then, it verifies the timestamp Ts and mac to verify whether a message is a replay attack. Additionally, time monitoring is started. If there is no operation after 30 s, the message will be ignored. After an employee accepts or rejects command R, the monitoring station queries its own database to verify the identity ID and obtains the employee's private key PK_{ID} and the key's index in the monitor. Then, the monitoring station uses PK_{ID} to encrypt the command R, the employee's identity ID and the timestamp to form a message (PK_{ID} {ID, R, Ts}, index) with the index to send to the monitor.

The monitor takes out the index among the messages obtained from the monitoring station and queries the database with the index to obtain the employee's private key PK_{ID}, which is used later to decrypt the employee's ID, R, and Ts. Then, the monitor verifies Ts to prevent replay attacks and verifies the ID to ensure that the identity is legitimate. If R is a receiving command, it will record the employee's ID, data and Ts to the file and send the data to the PLC. If R is a rejecting command, the employee's ID, data and Ts are recorded in the file, and the data are discarded.

When the monitor receives the data sent by the PLC, the data are forwarded directly to the HMI or engineering station.

4 Experimental Evaluation

4.1 System Verification

We used a MacBook Pro as the monitor and simulated an HMI and engineering station being controlled to send data to a PLC. The network topology is shown in Fig. 9. The monitoring station and the monitor are on the same LAN. They communicate wirelessly. The HMI and the monitor are on the same LAN, and the monitor and the PLC are on the same LAN.

In this experiment, we intercepted the commands 0×05 (write), 0×29 (stop PLC), and 0×28 (start PLC) of the Siemens S7 protocol. The experiment showed that no host (including HMI and engineering stations) has access to make changes to the PLC memory without personnel verification, which can protect the industrial equipment in the field well. Fig. 10 is our experimental equipment.

We sent a write command to the PLC, as shown in Fig. 11. The command is written (0×05). The data length is 3 bytes, and the data are 0×00000000.

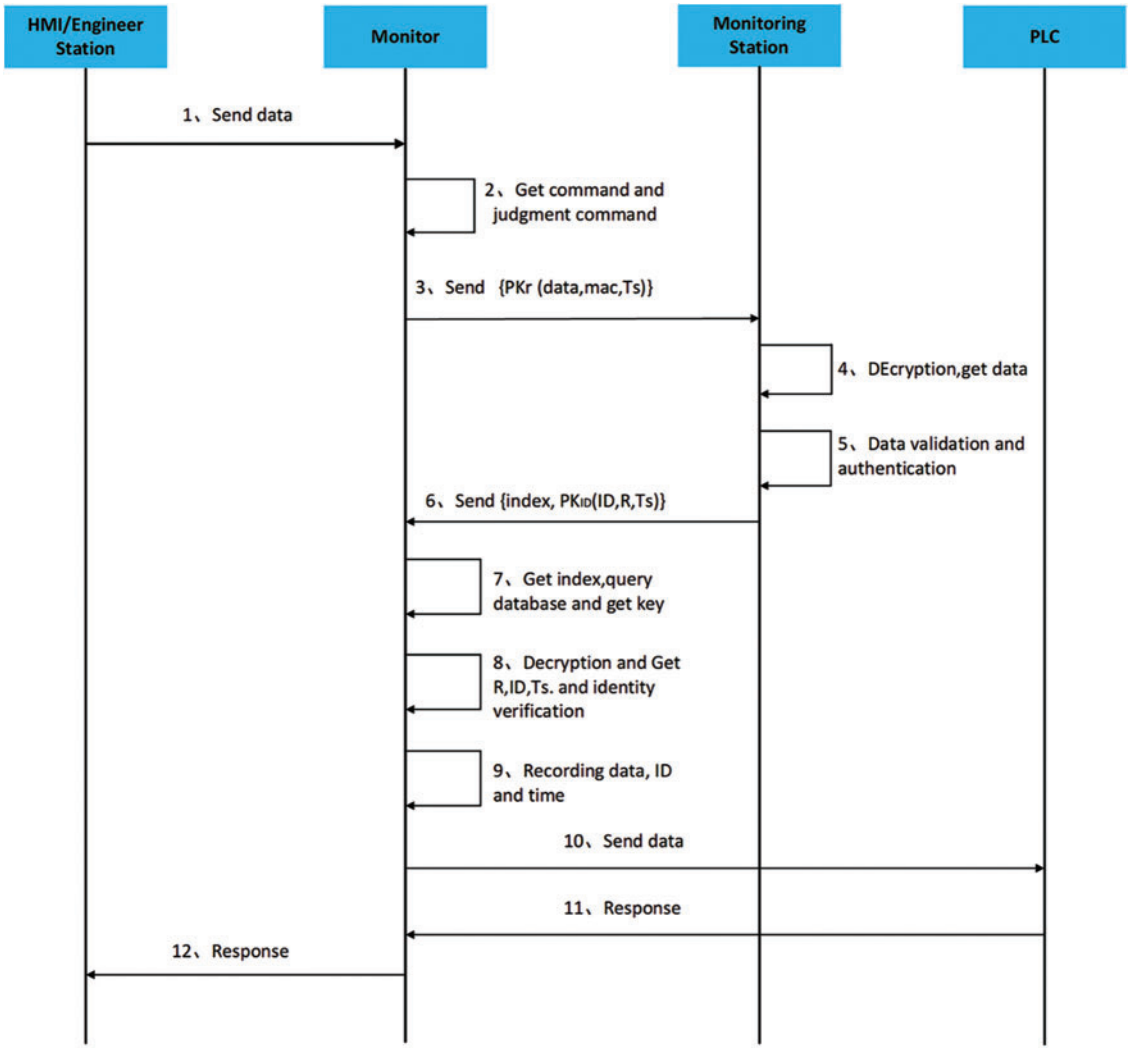

Figure 8: Sequence of communication between the HMI/engineering station and the monitoring station

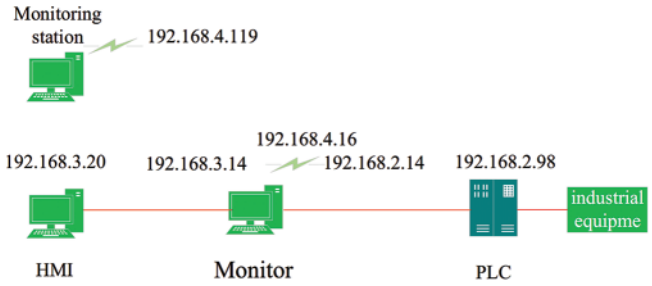

Figure 9: Network topology

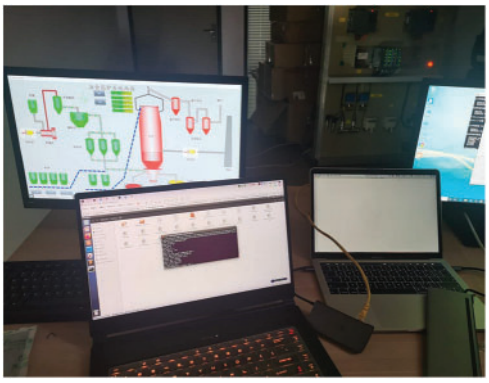

Figure 10: Experimentalequipment

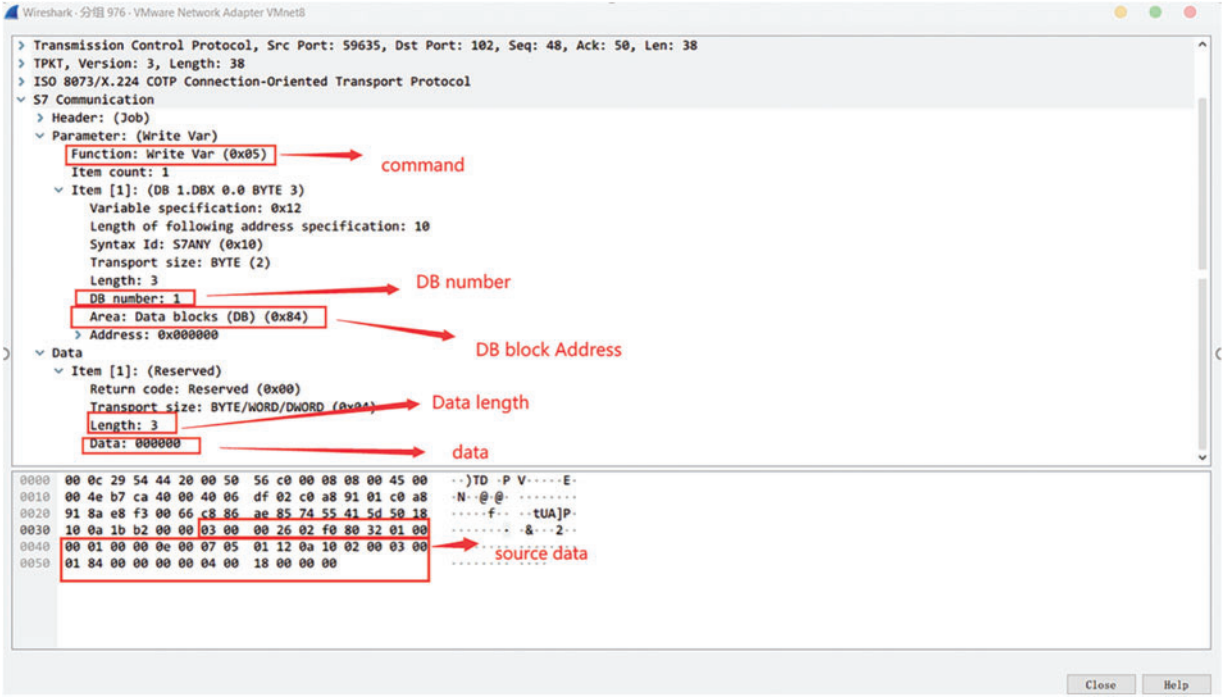

Figure 11: Data sent by a simulated attack

Fig. 12 shows that the monitoring station receives data from the monitor. The received data are encrypted binary data. After decryption, the data content is restored. The operating command is written. The data length is 3 bytes. The data address block is 1, and the data are 00000000.

Fig. 13 shows the ID of the employee, the time and the accepted data recorded by the monitor after receiving the command. The accepted data are recorded as the raw data sent by the HMI.

Figure 12: Monitoring station data

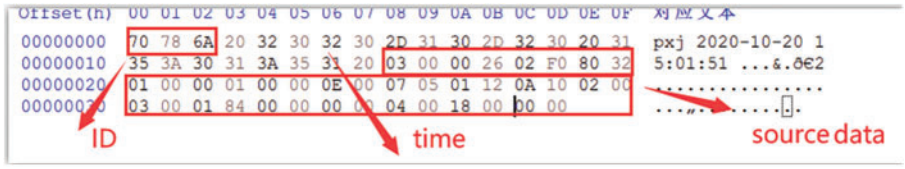

Figure 13: Employee behavior data

Since we are intercepting various HMI commands that operate on PLC memory and this type of command is more affected by human behaviors, the time delay measurement of such commands is of little significance. However, some programs, such as monitoring programs and database programs, are constantly querying PLC data. In our system, we need to intercept the data sent by the HMI to determine the command. If a command is a memory operation command, then it will be encrypted and sent to the monitoring station. If a command is a query command, then it will be directly forwarded to the PLC. Therefore, the process adds a certain time delay. Hence, we performed a time delay test on the query command. We performed 200 tests for each query data length and then averaged the results. The time delay is shown in Fig. 14. The horizontal axis represents the length of our query data. The vertical axis represents the time delay. The yellow column is the time delay without the query data in our system. The blue column is the time delay after the query data were added to our system. The increase in the time delay after query data join our system is below 6%, which could be ignored. The variances are shown in Fig. 15. The variance increases after adding our system, which means that the network fluctuation increases. However, the increase is very small, which means that the network fluctuation tends to be stable. This shows that the addition of our system has a relatively small impact on monitoring functions such as queries.

4.2 Protection Verification

As shown in Fig. 16, we simulated a scenario where a SCADA was attacked by APT. We designed an Excel file that contains an attack command, which can shut down the on-site PLC. If we open this Excel file, it will automatically send a stop command to the PLC. When the Excel file is opened, the on-site equipment will stop running. After joining our equipment without our protection system, the on-site equipment was operating normally, and information such as the time when the command was sent was recorded. Fig. 17 is our experimental equipment.

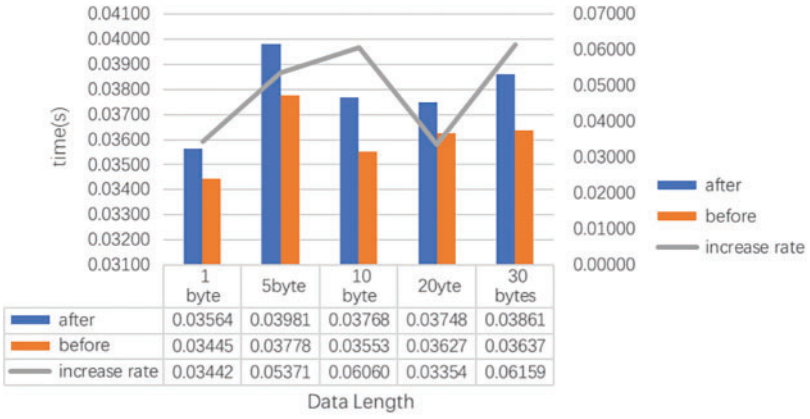

Figure 14: Time delay

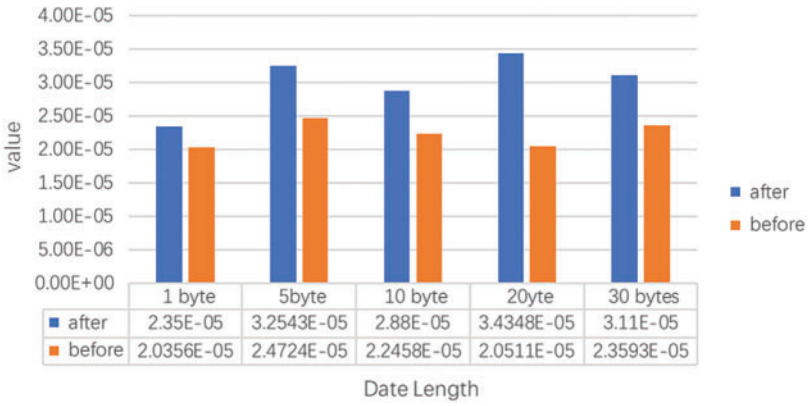

Figure 15: Variance in time delay

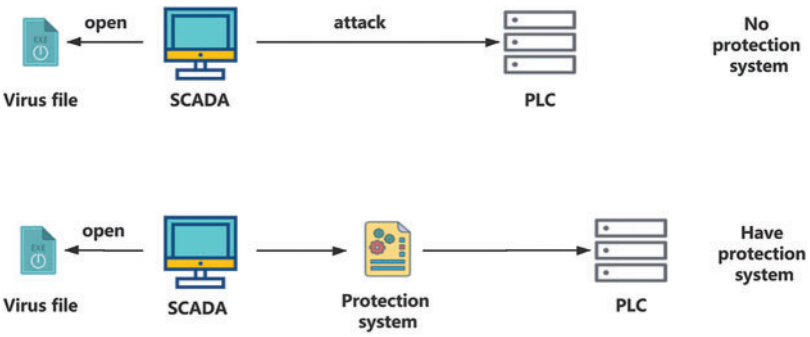

Figure 16: Simulated attack

Figure 17: Experimental equipment

5 Summary and Future Work

We designed a PLC protection system based on verification separation. The system will not affect the operations of the original system. In addition, the increased time delay is less than 6%. Different from other protection systems, this system does not encrypt the original protocol for compatibility. Because of the existence of the monitor, we can intercept some of the more important commands and send them to another server that is isolated from the industrial control external network through encryption. Some unimportant instructions, such as read instructions, are not processed. This greatly reduces the time delay. In addition, we also recorded the sending time of each critical command and confirmed the identity of the operator. This is of great help to the location and source tracing of some attacks. We can use this information to quickly locate the relevant attack time and attack. Because the system can intercept and reproduce the commands sent by the host computer, it can intercept some command substitutions and attacks where the host computer is controlled. This is something that other protection methods based on identity authentication and traffic identification cannot do.

The system architecture also has some shortcomings. For example, PLC-to-PLC communication cannot be verified manually due to its high requirements for latency and its large data communication. Considering that monitoring devices and databases are reading PLC data in real time, we do not detect or intercept the reading-data action, which may cause privacy leakage. In the future, we will implement the automated judgment of key commands in PLC-to-PLC communication. Due to the high data flow and the peculiarities of the production site, the automated judgment process does not allow false alarms, which is a challenge to the reliability and accuracy of the system.

Funding Statement: This work is funded by the National Key Research and Development Plan (Grant No. 2020YFB2009503), the National Natural Science Foundation of China (No. 62072130, 61702223, 61702220, 61871140, 61872420), the Guangdong Province Key Area R&D Program of China (No. 2019B010137004), the Guangdong Basic and Applied Basic Research Foundation (Nos. 2020A1515010450, 2021A1515012307), Guangdong Province Universities and Colleges Pearl River Scholar Funded Scheme (2019), and Guangdong Higher Education Innovation Group (No. 2020KCXTD007), Guangzhou Basic and Applied Basic Research Foundation (No. 202102020867, 202102021207) and Guangzhou Higher Education Innovation Group (No. 202032854), Industrial Internet innovation and development project of MIIT NO. TC200H01 V.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. Lee, H. Choi, J. H. Kim, J. W. Kim and J. T. Seo, "Identifying and verifying vulnerabilities through PLC network protocol and memory structure analysis," *Computers, Materials & Continua*, vol. 65, no. 1, pp. 53–67, 2020.

[2] D. Kushner, "The real story of stuxnet," *IEEE Spectrum*, vol. 50, no. 3, pp. 48–53, 2013.

[3] G. Tzokatziou, L. Maglaras and H. Janicke, "Insecure by design: using human interface devices to exploit SCADA systems," in *Proc. of the 3rd Int. Symp. Conf. on ICS & SCADA Cyber Security Research*, Ingolstadt, Bavaria, Germany, pp. 103–106, 2015.

[4] Z. Deng, X. Lun, R. Yu, W. Li and L. Jin, "Data security transmission mechanism in industrial networked control systems against deception attack," *International Journal of Security and its Applications*, vol. 10, no. 4, pp. 391–404, 2016.

[5] X. Y. Xu, "An investigation of haxex, the next generation exploitation to industrial control network," in *Proc. of the 7th Conf. on Vulnerability Analysisi and Risk Assessment*, Changsha, Hunan, China, pp. 594–609, 2014.

[6] R. Spenneberg, M. Brüggemann and H. Schwartke, "PLC-Blaster: a worm living solely in the PLC," in *Proc. of 2016 Black Hat*, Las Vegas, Nevada, USA, pp. 1–16, 2016.

[7] G. Liang, S. R. Weller, J. Zhao, F. Luo and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2015.

[8] A. Shlomo, M. Kalech and R. Moskovitch, "Temporal pattern-based malicious activity detection in SCADA systems," *Computers & Security*, vol. 102, no. 11, pp. 102153–102168, 2021.

[9] V. S. Sheng and J. Zhang, "Machine learning with crowdsourcing: a brief summary of the past research and future directions," in *Proc. of the AAAI Conf. on Artificial Intelligence*, Palo Alto, California, USA, pp. 9837–9843, 2019.

[10] A. Maamar and K. Benahmed, "A hybrid model for anomalies detection in ami system combining k-means clustering and deep neural network," *Computers, Materials & Continua*, vol. 60, no. 1, pp. 15–40, 2019.

[11] J. O. Malchow, D. Marzin, J. Klick, R. Kovac and V. Roth, "PLC guard: a practical defense against attacks on cyber-physical systems," in *Proc. of 2015 IEEE Conf. on Communications & Network Security*, Florence, Tuscany, Italy, pp. 326–334, 2015.

[12] S. Zonouz, J. Rrushi and S. Mclaughlin, "Detecting industrial control malware using automated PLC code analytics," *IEEE Security & Privacy*, vol. 12, no. 3, pp. 40–47, 2015.

[13] A. Clark, Q. Zhu, R. Poovendran and T. Basar, "An impact-aware defense against stuxnet," in *Proc. of 2013 IEEE Conf. on American Control Conf. (ACC)*, Washington, USA, pp. 4140–4147, 2013.

[14] C. T. Lin, S. L. Wu and M. L. Lee, "Cyber attack and defense on industry control systems," in *Proc. of 2017 IEEE Conf. on Dependable & Secure Computing*, Taipei, Taiwan, China, pp. 524–526, 2017.

[15] S. Ponomarev and T. Atkison, "Industrial control system network intrusion detection by telemetry analysis," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 2, pp. 252–260, 2016.

[16] K. Yau, K. P. Chow, S. M. Yiu and C. F. Chan, "Detecting anomalous behavior of PLC using semi-supervised machine learning," in *Proc. of 2017 IEEE Conf. on Communications and Network Security (CNS)*, Las Vegas, Nevada, USA, pp. 580–585, 2017.

[17] M. Halas, I. Bestak, M. Orgon and A. Kovac, "Performance measurement of encryption algorithms and their effect on real running in PLC networks," in *Proc. of 2012 IEEE Int. Conf. on Telecommunications & Signal Processing*, Ostrava, South Moravian Region, Czech, pp. 161–164, 2012.

[18] I. Bestak and M. Orgon, "Performance measurement of encryption algorithms used in PLC devices," *Interna-tional Journal of Research and Reviews in Computer Science*, vol. 2, no. 5, pp. 1218–1221, 2011.

[19] H. Wardak, S. Zhioua and A. Almulhem, "PLC access control: a security analysis," in *Proc. of 2016 World Congress Conf. on Industrial Control Systems Security*, London, UK, pp. 1–6, 2016.

[20] W. Zhang, Y. Jiao and D. Wu, "Armor PLC: A platform for cyber security threats assessments for PLCs," *Procedia Manufacturing*, vol. 39, no. 2019, pp. 270–278, 2019.
[21] S. Figueroa-Lorenzo, J. Añorga and S. Arrizabalaga, "A role-based access control model in modbus SCADA systems. A centralized model approach," *Sensors*, vol. 19, no. 20, pp. 4455–4479, 2019.
[22] C. T. Lin, S. L. Wu and M. L. Lee, "Cyber attack and defense on industry control systems," in *Proc. of 2017 IEEE Conf. on Dependable and Secure Computing*, Taibei, Taiwan, China, pp. 524–526, 2017.
[23] P. Yong, X. Chong, Z. Miao, D. Chen, H. H. Gao *et al.*, "Scenario fingerprint of an industrial control system and abnormally detection," *Journal of Tsinghua University*, vol. 56, no. 1, pp. 14–21, 2016.
[24] X. U. Zhen, X. J. Zhou, L. M. Wang, Z. Chen, K. Chen *et al.*, "Recent advances in PLC attack and protection technology," *Journal of Cyber Security*, vol. 4, no. 3, pp. 1–48, 2019.
[25] Y. Liu, Y. Zhao, K. Li, S. Yu and S. Li, "Design and application research of a digitized intelligent factory in a discrete manufacturing industry," *Intelligent Automation & Soft Computing*, vol. 26, no. 5, pp. 1081–1096, 2020.
[26] Y. Sun, M. Li, S. Su and M. Guizani, "Honeypot identification in softwarized industrial cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5542–5551, 2021.
[27] K. Yakine, M. Menaa, K. Tehrani and M. Boudour, "Optimal tuning for load frequency control using ant lion algorithm in multi-area interconnected power system," *Intelligent Automation & Soft Computing*, vol. 25, no. 2, pp. 279–294, 2019.
[28] M. B. Nejad, "Parametric evaluation of routing algorithms in network on chip architecture," *Computer Systems Science and Engineering*, vol. 35, no. 5, pp. 367–375, 2020.
[29] J. Dong, "Analysis of the real-time problem in industrial communication network," *Agriculture Network Information*, vol. 1, no. 1, pp. 113–115, 2009.
[30] E. Sisinni, A. Saifullah, S. Han, U. Jennehag and M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, 2018.
[31] Z. Tian, M. Li, M. Qiu and S. Su, "Block-dEF: A secure digital evidence framework using blockchain," *Information Sciences*, vol. 491, no. 3, pp. 151–165, 2019.
[32] J. H. Zhang, X. B. Guo and X. Fu, "AES encryption algorithm analysis and the application in information security," *Netinfo Security*, vol. 1, no. 5, pp. 31–33, 2011.
[33] Q. Wang and X. Wang, "Parameters optimization of the heating furnace control systems based on BP neural network improved by genetic algorithm," *Journal of Internet of Things*, vol. 2, no. 2, pp. 75–80, 2020.