Hindawi
Journal of Sensors
Volume 2023, Article ID 4619556, 12 pages
https://doi.org/10.1155/2023/4619556

Research Article

Ethernet Information Security Protocols Based on Industrial Control Wireless Sensor Networks

Xiaobo Yin, Shunxiang Zhang, Li Feng, and Guangyu Xu

Anhui University of Science and Technology, Huainan, China 232001

Correspondence should be addressed to Xiaobo Yin; xbyin@aust.edu.cn

Received 2 September 2022; Revised 5 December 2022; Accepted 4 April 2023; Published 30 April 2023

Academic Editor: Gengxin Sun

Copyright © 2023 Xiaobo Yin et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This paper provides an in-depth study and analysis of information security protocols for industrial Ethernet using wireless sensor networks. The optimal number of cluster heads for nonuniform subclustering is derived based on the sensor energy consumption model, and then, the EEUC contention radius formula is optimized to select candidate cluster heads with random values and energy as weights. A multihop approach based on the shortest offset is also proposed for intercluster information transmission. Experimental results show that the EEUC-based improved cluster routing protocol proposed in this paper balances the node energy consumption and extends the network lifetime. In response to the problem that the coarsened hop value and average hop distance of the DV-Hop localization algorithm cannot reflect the network topology, the improved DV-Hop algorithm based on multicommunication radius and hop distance correction is proposed. Simulation experiments show that the improved algorithm based on multiple communication radius and hop count correction can significantly reduce the localization error and improve the accuracy of the algorithm. Aiming at the shortcomings of MRP with excessive risk concentration and transmission medium limitation, this paper proposes a fast self-healing mechanism of industrial Ethernet with a multiexpert strategy. The PCP-AP common platform architecture for openSAFETY sites is designed on the base sleeve of the implementation of the industrial Ethernet protocol Ethernet POWERLINK; the main communication part of POWERLINK is implemented through an FPGA hardware solution, and the openSAFETY site is implemented using AM335X high-performance processor to implement openSAFETY security application functions. Finally, the article conducts field tests on the wireless signal information transmission, WSN data transmission, network connection, and power supply system in the system and compares and analyzes the data collected by the system with the monitoring data of the national control site. The data obtained by the system has real reliability. The communication module used is inexpensive, lightweight, and easy to operate. It can realize the collection of multiple pollution sources, and compared with traditional monitoring equipment, it avoids the difficulties of complicated wiring, difficult positioning of pollution sources, and restricted monitoring areas and largely reduces the investment in human and material resources.

1. Introduction

Wireless sensor networks (WSNs) have gradually come into the limelight with the rapid development of embedded computer technology, Internet of Things technology, and wireless communication technology. WSNs deploy various types of sensors at different locations in different ways for different information collection targets and therefore can collect a variety of data information, for example, temperature, smoke, humidity, and other environmental information around the node [1]. In practical applications, such as environmental awareness, fire prevention, and other application scenarios, the distribution of sensor nodes in the network is irregular; if the staff cannot obtain the location of the sensor, then, the sensor collects other information also loses its relevance and use value; only the information collected by the sensor and the sensor's location information is known before it can be practically applied to life. The wireless sensor network is a network technology based on the development of self-organizing networks, it has a fundamental difference in the purpose of use and other communication networks; its primary task is responsible for monitoring the

environmental factors in the region, such as wind speed, and humidity. Sensor technology was first adopted by the military; in the Vietnam War, the U.S. military first used a similar sensor technology, the "tropical tree" sensor, which can listen to the surrounding sound and vibration. Thanks to the "tropical tree" technology, the U.S. Army was able to destroy tens of thousands of North Vietnamese vehicles in combat, making a big difference. After the war, the U.S. began researching sensor technology, and through cooperation with universities, the U.S. has made great breakthroughs in all aspects of wireless sensors. The successful application of wireless sensor technology in various industries has made wireless sensor networks an irreplaceable technology in the information age, which is widely used in many fields such as biomedical, environmental monitoring, and military reconnaissance [2]. Many tiny sensor nodes form a network of data sharing through self-organization, i.e., wireless sensor networks. To ensure that all areas of the network can be monitored, the nodes are generally distributed evenly. Each sensor node has storage, communication, and computational capabilities, but there are energy limitations. Therefore, research into more energy-efficient and efficient network protocols has become a top priority in sensor technology. The way of data transmission in sensor networks determines whether the energy consumption between nodes is relatively balanced, and to better meet the data collection requirements of users, the most realistic data collection methods should be designed in different scenarios. At present, there are three main types of data collection methods, which are traditional data collection methods, mobile sink-based data collection methods, and intelligent algorithm-based mobile sink data collection methods.

As network communication technology and automation control technology continue to grow, the most popular industrial control network systems are fieldbus control systems (FCS) and industrial Ethernet control systems. Ethernet technology occupies a large market in the field of commercial network communication because of its high communication rate, good compatibility, interconnection performance, and expansion performance. Industrial Ethernet technology is based on general Ethernet technology, which is derived from and different from the latter. Although Ethernet control network technology has many advantages, at the technical level, industrial Ethernet and commercial Ethernet can be connected seamlessly [3]. However, industrial Ethernet is used in harsh environments such as industrial automation sites and transportation engineering, which require more real-time and reliability, and the data transmission methods are different for different transmission media. Unlike the information security threats faced by traditional Ethernet, functional security events of industrial control systems often lead to more serious accidents, which can cause huge losses of property and equipment and endanger the lives of staff. Nowadays, industrial Ethernet technology is advancing rapidly with the development of fieldbus and programmable control systems, and the demand for safety-related devices in industrial automatic control systems is expanding, and the overall requirements for information security and functional safety performance are also increasing, so the traditional industrial safety protocol technology is no longer applicable to the complex real-time industrial Ethernet communication environment. Industrial Ethernet technology is widely used in the industrial automation control field and transportation industry because of its high communication rate, good compatibility, and scalability [4]. However, in industrial sites, the harsh environment can distort data transmission. To ensure the reliability and real-time performance of industrial applications, network self-healing technology has been widely researched and applied in recent years.

At present, the mainstream trend of global manufacturing upgrading is intelligent automation, in which the automation production line of industrial control system field equipment communication often includes HMI, PLC, divisional I/O, and all kinds of instruments. The connection of these components has gradually changed from the traditional closed fieldbus to open industrial Ethernet, which shows that the system of efficient and standardized integration will become the modern industrial automation [5]. This indicates that efficient and standardized system integration will become the development direction of modern industrial automation system and control system. Industrial Ethernet can solve many problems such as effectiveness, openness, trustworthiness, and anti-interference of industrial sites, especially in information determination and prioritization, and its development has gradually risen to the level of national information strategy [6]. At the same time, with the frequent occurrence of network security events such as virus infection, hacker illegal invasion, and illegal operation, information security and virus protection for industrial control networks have also begun to attract the attention of the industry. Most of the security problems are network attacks and malicious control by using the current vulnerabilities of industrial Ethernet, so network management and security system can be used for internal and external isolation of the network, or network security management by using security mechanisms such as permission control and data encryption to prevent attackers from using protocol permissions to maliciously tamper or listen in. In this paper, it is important to study Ethernet security protocols based on industrial control wireless sensor networks.

2. Related Works

Ethernet technology is the most rapidly developing network technology in recent years. Nowadays, Ethernet technology has become the most dominant network communication technology in the industrial field as well as in the rail transportation industry. To improve the demand for industrial Ethernet for data communication network reliability and reduce the economic loss caused by sudden network failure, some major network equipment manufacturers have continuously released their network redundancy self-healing methods. Many schools as well as major enterprises and research institutes have started to put more effort into the research of network redundancy self-healing technology [7]. The DPR protocol is defined in the EPA standard for real-time communication and control of Ethernet in

industry, which was agreed upon by many research institutions. For ring communication and control networks, an active parallel fault detection method is used, which allows the risk of failure to be distributed and makes the recovery time after a failure in a ring network topology much shorter [8]. From the introduction of the industrial Internet to the rapid development in recent years, industrial control systems are more closely linked with Internet technology, and the security issues of industrial control systems that have been leaked out along with the development of technology are also very worthy subjects of research. With the frequent occurrence of industrial Internet security accidents at the same time, the field of information security has attracted the high attention of developed countries in Europe. The United States, as the leading country in the field of high-tech information for the industrial control field of information security from the last century, has begun research. Some European countries are relatively late to research information security. Siemens and Schneider Electric are the world's largest operators of industrial control equipment, and they also have research on information security of industrial control systems [9]. For example, Siemens proposes the longitudinal protection on process control information security, which is to conduct a risk assessment on ICS against the background of ensuring the security of hardware equipment and to provide security protection for the whole system. For the security defense of industrial Internet systems, Symantec Industrial Controllers introduces two kinds of security protection: one is to protect the device security of industrial Internet systems, and the other is the product security of Internet providers [10]. Wang and Jiang analyze the types of vectors against ICS attacks and their applications in controllers and construct mathematical models using the interference situation generated by the attacks to achieve the prevention of possible anomalous behavior [11]. Nechibvute and Mudzingwa proposed a method that allows real-time anomaly detection control systems in industrial processes, first learning the normal behavior at work, and when each time anomalous behavior is detected, the system generates an alarm and adds it to the learning algorithm model, but this method may cause the consumption of system resources depending on the continuous accuracy of the algorithm model [12]. Gadze implemented the login authentication of public key certificates by deploying the security system architecture for Internet information transmission and access and analyzed the encryption method during transmission to control the access of resources at the gateway deployed to the Internet [13].

The concept of wireless sensors was first proposed by the United States in the 1970s; in the following decades, the technology was mainly used in the field of military defense. In addition, the United States also has WSN-related technologies officially in the scope of the international conference on mobile computing and networking in the scope of discussion, and that WSN will greatly promote the development of future technological life. To promote the overall progress of science and technology, countries have for WSNs to carry out in-depth research [14]. Wireless sensor network technology also gradually matured with the development of sensor technology, communication technology, and microprocessor technology. With the dramatic development of big data and artificial intelligence technology in recent years, coupled with the growing maturity of traditional embedded and IoT technologies, the integration of terminals and networks continues to tighten; whether in monitoring, coordination, and automation, the development of emerging technologies are accelerating in the direction of intelligence and networking [15]. Some national projects and research programs include wireless sensor networks technology research, such as science and technology support, science and technology major special projects, the National Science Foundation, and other major national tasks. Many universities have also set up laboratories with corresponding topics to further promote the development of technology in this field. Zhou et al. proposed the idea of dual cluster heads, i.e., two nodes are selected as cluster heads in a cluster at the same time, and the two cluster heads share each other's energy consumption to prevent the energy exhaustion of a single cluster head from disrupting the communication within the whole cluster [16]. Cossu et al. proposed a new election strategy, in which each round of cluster head election effectively reduces the number of cluster head elections and reduces part of the election energy consumption [17]. Thanks to the strong development of artificial intelligence, scholars have applied artificial intelligence algorithms to sensor technology and the results show that artificial intelligence algorithms improve the performance of traditional routing protocols. In applying BP (Back Propagation) to information aggregation, simulation experiments by Naraliyev and Samal show that BP neural networks greatly improve the performance of data fusion [18].

The application scenarios of wireless sensor networks are intricate and complex, especially in some harsher environments and even in places that are difficult for humans to reach. Once the energy of the sensor nodes arranged in these areas is depleted, it is not possible to replenish it. In addition, when all the nodes in a certain area are depleted, the environmental changes in the area are no longer known. Therefore, given the limited energy of the nodes themselves, how to maximize the use of this energy, maximize the full coverage of the monitoring area, and maximize the life cycle of the entire network have become the most important concern of many scholars. A series of malicious attacks implemented against industrial control systems have caused significant harm to industrial sites, and these typical security events have sounded the alarm for industrial production control systems. The information security protection of industrial control systems must be paid great attention to it. And with the exponential growth of the data volume of industrial control systems, directly transferring all the data that needs to be processed to the cloud service center will generate additional bandwidth and time delay. Therefore, there will be an edge server in the middle of the industrial control site and cloud services to provide low-latency proximity services. Security protection at the edge can protect the industrial site and the communication system in the cloud, thus achieving stronger security measures.

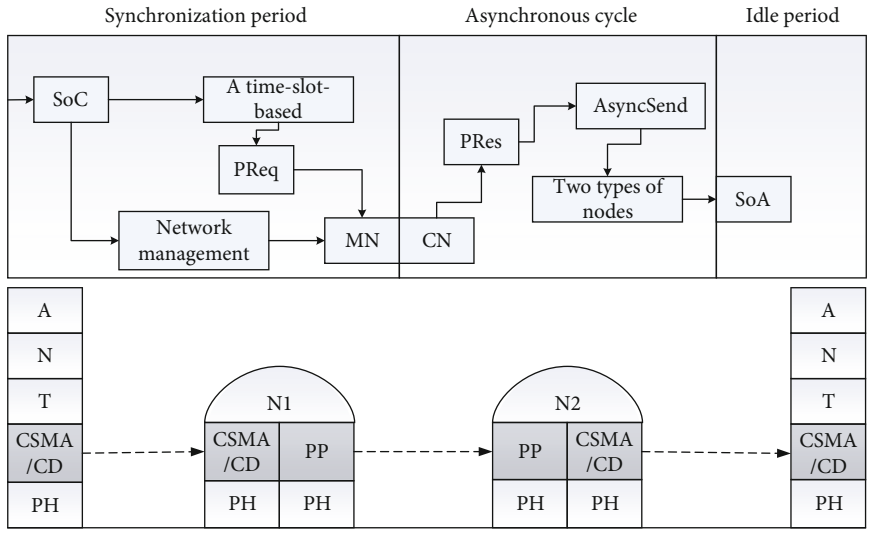

Figure 1: Schematic diagram of the data link layer communication cycle.

3. Exploring Ethernet Information Security Issues

In the beginning, industrial Ethernet was designed to be used in closed network environments, and its control protocols and strategies were less concerned with security. However, with the development of network technology and the increasing complexity of industrial systems, industrial Ethernet needs to be applied in open environments, which exposes the information network security of existing industrial Ethernet protocols. The idea of functional security assurance of intelligent industrial control systems is to analyze the security requirements of the system from the level of the system and convert the relevant security issues into problems of controlling the risk objectives within an acceptable range [19]. The object of this research is intelligent industrial control systems with comprehensive relevant safety. Such systems are usually difficult to predict possible situations due to strong uncertainties in operation, which also makes it difficult to determine each failure mode in practice. The way to achieve functional safety of intelligent industrial control systems is to use the appropriate disciplinary techniques to complete the optimization and modeling of the system and to analyze and study the system by combining qualitative and quantitative analysis. The data information that can be collected by wireless sensor networks is also diverse, such as temperature, smoke, humidity, and other environmental information around the nodes. With the continuous promotion of industrialization and information reform in the new era, the performance complexity and scale of intelligent industrial control systems are increasing, which makes the possibility of system failure also increase, so the system's functional safety is facing a great challenge. The functional safety of industrial control system is the embodiment of the ability of the control system to perform the correct function on the one hand, and the basis for the system to maintain effective and stable operation on the other. The theoretical system of functional safety standards involves the interpenetration of knowledge from many disciplines, including knowledge of system theory, control theory, computer technology theory, and safety management theory [20]. The guarantee of system functional safety requires the comprehensive use of the above theoretical knowledge and technology, and the combination of qualitative and quantitative analysis methods to model and optimize the system, to achieve the purpose of guaranteeing system functional safety. The assurance of system functional safety is mainly reflected in two aspects: failure identification and safety integrity level assessment.

With the continuous development of industrial society, all fields are approaching the direction of intelligence and automation, and to realize industrial production automation, it is inseparable from the communication system to meet the demand of business development. With the full coverage of 4G networks of operators and the imminent commercialization of 5G networks, wireless base station-based networks of public operators are widely used in the industrial sector, such as urban intelligent traffic monitoring and command systems, urban gas transmission control systems, and urban intelligent water supply systems. At the data link layer, POWERLINK replaces the CSMA/CD mechanism of Ethernet with a time-slot-based communication network management mechanism to solve the problem of network data conflict preemption and to ensure that only one communication device can get access to transmit data in the same cycle. In this mechanism, there are two types of nodes in the entire network: an expert managed node MN (ManageNode) and several controlled nodes CN (ControlledNode). The communication cycle of the POWERLINK data link layer is shown in Figure 1.

The entire POWERLINK communication cycle is divided into 3 phases: synchronous, asynchronous, and idle. The synchronous phase starts with the MN sending SoC detects to each 0 for isochronous synchronization. After that, the bandit sends a PReq device to a specific CN requesting its periodic data interaction, and the CN replies with a

PRes data device. This process continues sequentially until the MN polls all the CNs in the network when the synchronous cycle ends and the network enters the asynchronous cycle. The MN sends SoA to open the asynchronous communication, and only the CN at the top of the asynchronous queue can upload nonperiodic data and configuration data via data pa. At the end of the asynchronous phase, the network enters the idle phase. The idle phase is the remaining time interval between the end of the asynchronous phase and the start of the next cycle. Since the length of the asynchronous phase may vary with the size of the asynchronous data in each cycle, the idle phase exists to provide a buffer for the asynchronous phase.

Many data frames are constantly being forwarded in the network message operation, and the switch must ensure that these data frames are handled accurately, while also handling the MRP's set of algorithms. However, the CPU has a limited resource allocation to handle the millions of forwarding events per second on average, and the MRP is running at the same time, making it inevitable that the protocol will experience significant latency. If MRP processing is delayed, the recovery speed of network communication will be reduced. The execution efficiency of the protocol processing is improved by executing the events forwarded by the CPU and the MRP tasks separately while ensuring that the hardware platform meets the actual requirements. Although there are many data frames in the network that need to be forwarded, the task of forwarding data frames is simple and does not involve a lot of logical operations. In terms of hardware selection, a professional switching chip is used to process the data frame forwarding events. The switch chip handles the task of a data frame forwarding only, and there is no other logical operation. The data frame is forwarded directly without CPU processing, which greatly improves the efficiency of data frame forwarding in this way. At the same time, the switch chip directly forwards data frames to remove many frames that are not MRP frames, so the CPU does not need to process other frames and only uses them to process MRP frames, which increases the CPU processing speed.

4. Industrial Wireless Sensor Networks Based on the Construction of Ethernet Information Security Prevention System

Industrial Wireless Sensor Networks (IWSNs) usually include sensor nodes, gateway nodes, and control centers, which form industrial wireless sensor networks in the modern sense with the collaboration of many distributed sensor nodes. The sensor nodes are generally deployed in a certain detection area and form a self-organized information transmission network through a wireless network for monitoring, collecting, and processing various information about the monitored objects [21]. The data monitored by the sensor nodes are transmitted and processed by other nodes through the wireless network with multiple hops to reach the gateway node, and finally, the data is sent to the control center by the gateway node. Modeling industrial information physical systems based on control theory helps to deal with uncertainty, fault diagnosis, and attack detection of complex models. The basic framework required for modeling industrial information-physical systems mainly includes physical processes, industrial wireless sensor networks, and information systems.

Under normal conditions, the sensor measures the controlled object to get the measured value y_κ and transmits the measured value y_κ through the wireless communication network to the estimator for optimal state estimation, and the estimator estimates the optimal state $\widehat{x}_\kappa$. The controller receives the state estimation and gives the control signal $\widehat{x}_\kappa$ u_κ and then transmits the control signal u_κ to the actuator through the wireless communication network to drive the controlled object to the desired state. The initial state $x_0 \in N(0, P_0)$ and for all $\kappa \geq 0$ are independent of w_κ and v_κ.

$$y_\kappa = A\widehat{x}_\kappa + w_\kappa v_\kappa \tag{1}$$

The model knowledge in the three-dimensional attack space model refers to the attacker's priori model knowledge of the control system. If the attacker has a large amount of model knowledge, he can construct more complex and difficult-to-detect attacks, which can cause more serious consequences to the system. Disclosure resources are sensitive information about the system obtained by the attacker before the attack, such as sensor and actuator node data, but disclosure resources by themselves cannot disrupt system operations and can be combined with disruption resources to form a disruptive attack, such as the common replay attack. Disruption resources are information that the attacker develops an attack strategy to disrupt the system based on the knowledge of the model and disclosure resources, such as DoS attacks that disrupt the integrity or availability of data. Based on the attack principles of the three attacks, further analysis of the impact of the three attacks on the system shows that the DoS attack will cause the sensor measurements to not reach the corresponding receiving node, thus making the measurements unavailable [22]. The replay attack will cause the receiving node to receive delayed measurements affecting the real-time performance of the system; the false data injection attack will covertly change the measurements sent by the sensor, causing the receiving node to receive. The false data injection attack will covertly change the measurement values sent by the sensor, resulting in the receiving node receiving the tampered measurement values, thus affecting the stability of the system. If the location of the sensor is not available to the staff, then the other information collected by the sensor loses its relevance and use.

The Simulink/TrueTime simulation software is used to simulate the ICPS under DoS attack, add an event trigger with caching effect after the sensor, and write the MATLAB code corresponding to the event trigger, Kalman filter, and tracking controller. The initial position of the ball is assumed to be 0 m (the leftmost end of the rail), and the control objective (target output value) is to stop the ball at 0.2 m in the middle of the rail, and the ballbar networked control

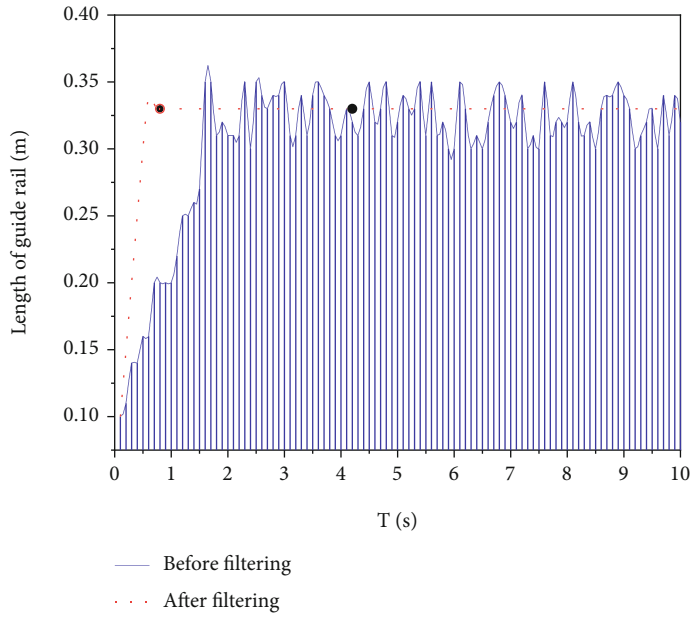

Figure 2: Position of the blob before and after the filter.

system is simulated based on a discrete linear time-invariant system. The simulation of the system under normal conditions with ambient noise interference and after filtering by the Kalman filter is shown in Figure 2. By comparing the waveforms before and after filtering in Figure 2, the system before filtering is affected by noise and will oscillate back and forth at 0.2 m with a large amplitude, which affects the stability of the system. After filtering, the system no longer oscillates and reaches a stable state soon, so the Kalman filter can effectively filter out the noise.

5. Ethernet Information Security Preparedness System Construction

In industrial control systems, the first consideration is the secure communication between the upper and lower computers, where the Ethernet Modbus TCP is commonly used for communication transmission. However, most of the ICS protocols are not designed with security in mind, and these protocols work in a closed environment and industrial control networks, which are physically isolated from the outside Internet. Due to the characteristics of the ICS itself, only the practicality, transmission efficiency, and authenticity of the ICS communication protocols were required, and no research was done on the protection of information security. However, with the close integration of Internet technology and ICS, ICS faces an Internet environment that has not existed before, which also reveals the vulnerability of many industrial control protocols themselves [23]. Modbus TCP communication protocol itself has security vulnerabilities, but some security risks only become known in the process of implementing a specific industrial control system. For example, some hackers or miscreants can break into the Modbus network and tamper with the function codes of the Modbus TCP, which can adversely affect field devices. There is also a risk of data buffer overflow, where the data stored in the buffer is larger than its capacity, causing it to overflow and overwrite the original data. There is also the potential danger of Modbus TCP function codes, which could be exploited by malicious attackers if they penetrate the network. Finally, the Modbus protocol running on TCP/IP also has the same security vulnerabilities that appear in the TCP/IP protocol itself running on the Internet, such as denial-of-service attacks, man-in-the-middle attacks, and tampering can appear in industrial control systems. Once an attacker invades any industrial control machine in the industrial control system, he can launch an attack, which may seriously jeopardize the normal operation of the whole industrial control system.

In the distribution automation communication system, the maximum number of messages for a single information interaction between the dispatching expert station and the distribution terminal does not exceed 1518 bytes, and the congestion control of the equipment restricts the network load rate in one direction to not more than 50% under the ring formation condition, and the minimum network bandwidth of the network equipment port is 100 Mbit/s. To ensure reliability and real-time signal transmission, the number of relay signal nodes is required to be no more than 50.

$$T_{\max} = \sum_{i=1}^{n} \left(t_i + \mathrm{t}_{SQ} + t_{ST}\right). \tag{2}$$

The time required for the propagation of information in the medium depends on the physical length L of the communication network between the field devices, which is equal to the ratio of the channel length and the propagation rate C of the electromagnetic wave on the channel, while the transmission speed of data in the fiber optic line is 2/3 of the speed of light in the fiber optic transmission

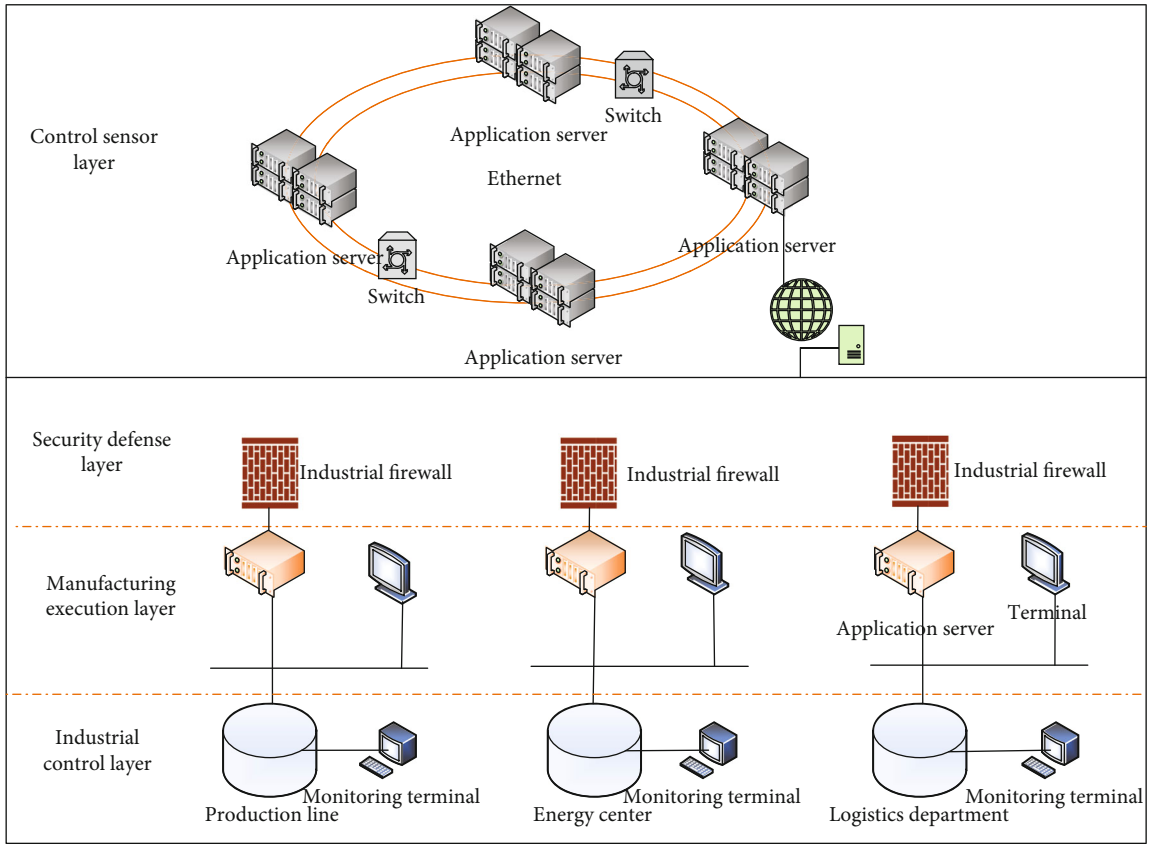

Figure 3: Ethernet information security preparedness system structure.

medium. In urban distribution network automation projects, the length of optical fiber from the communication terminal to the dispatching expert station or substation does not exceed 100 km.

$$T_{\min} = \frac{L_{\max} - T_L}{c - T_w}. \quad (3)$$

Comprehensive and holistic principle: from the perspective of system engineering, the security protection level of the network should be analyzed comprehensively by adopting an integrated strategy and adhering to the principle of balancing demand, risk, and cost. Multiprotection principle: there are various technical means to protect the network security of distribution data network based on industrial Ethernet technology, but a single network security measure cannot ensure the absolute security of the network, and there is a possibility of a breakthrough. In actual engineering, the principle of combining multiple measures should be adopted to establish a solid and reliable communication network security system, and each layer of protection should be independent of the others.

An intelligent industrial control system is a multilayered system that includes an enterprise interaction layer, a supervisory aggregation layer, a control sensing layer, and a device layer. Because each different layer has a different functional task division and each different layer is also using a different communication network and protocol [24], therefore, each layer faces different system information security threats, and its needs for each layer of information security preparedness are required to take different means of preparedness. Only by combining the structural characteristics and risk requirements of each level of the system can the structural system of multilevel defense applicable to the intelligent industrial control system be designed. The multilayer defense system blocks malicious intrusion attacks layer by layer and finally guarantees the normal and stable operation of the intelligent industrial control system from intrusion attacks. Based on the structural characteristics of the intelligent industrial control system and the actual needs of each level, a multilayer longitudinal defense structure system is designed to ensure the information security of the system by adopting the method of isolation and boundary defense hierarchically and the structure system is shown in Figure 3.

Information security policy decision link is mainly based on the hazard assessment and based on the assessment results of the system under threat posture for a comprehensive analysis; from the information security policy service set, the decision applies to the current threat under the security policy for system recovery. As the intelligent industrial control system is not an unlimited resource cost, if the damage caused by this intrusion attack to the system is small compared to the cost of system resources consumed by the intrusion response, in this case, whether to take relevant response measures again needs to be carefully considered.

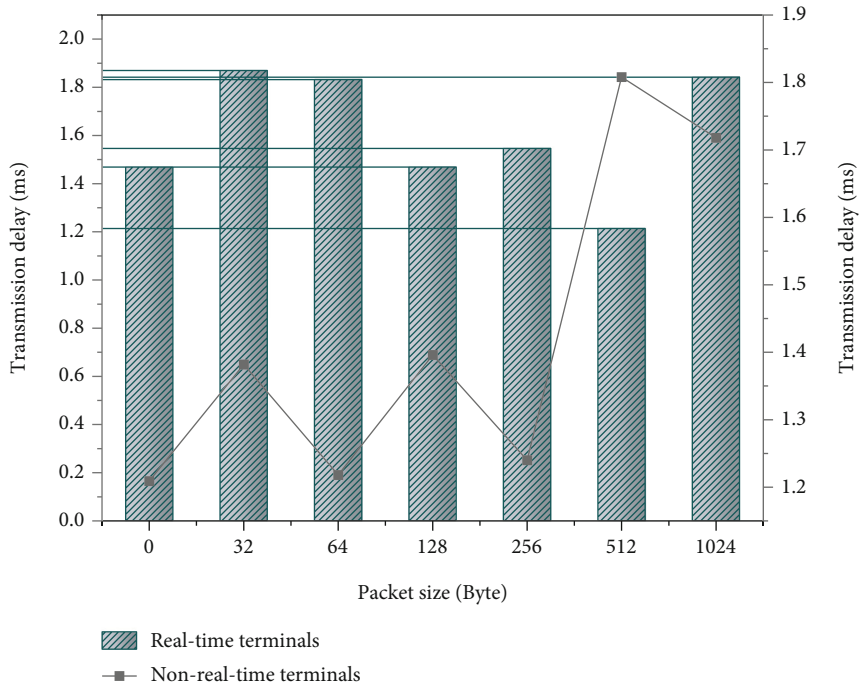

Figure 4: Normal operation simulation data.

Information intrusion attacks may make the generally normal and stable operation of the system gradually deviate from the expected state, or even into a nonsecure state. Therefore, the information security preparedness of the system needs to be considered in conjunction with the current state of the system, and the system is brought back to the expected state from the deviated state through the appropriate information security policy, and the appropriate security policy is a security policy decision-making process that considers the balance of system cost, state optimization, and risk security and other aspects.

6. Simulation Experiments and Result Analysis

Simulate the fault-free normal operation state of the whole network to verify the size of packets on the communication delay of real-time terminals, non-real-time terminals, and the corresponding expert server. The experimental results are shown in Figure 4, where the horizontal coordinates indicate the packet size and the vertical coordinates indicate the transmission delay.

Under the normal operation of the whole network without failure, the time delay of the real-time and non-real-time networks is within the range of 1.174 ms-1.182 ms, which meets the requirement of less than 100 ms network delay for intelligent distributed three remote terminals. Therefore, the packet size of ICMP messages in the subsequent experiments is set to a 1518-byte value to facilitate the control variables. A simulation model of the industrial Ethernet-based distribution automation imitation communication system is built by NSP simulation software to verify the feasibility of the networking configuration scheme discussed in the previous section. The simulation model construction and protocol configuration process are introduced in detail in the paper, and several failure scenarios, such as network fiber optic cable failure, access layer device failure, and backbone layer device failure, which commonly occur in the actual network are designed [25]. The analysis of the failure test data shows that the industrial Ethernet-based distribution automation communication system has high reliability and the time delay can meet the network requirements.

To realize the compensation control of ICPS under DoS attack, a compensator is added between the state estimator and the controller, and a multistep state prediction compensation strategy is designed to decide whether to trigger the compensator based on the detection result of the detector and to prevent the estimator from transmitting the abnormal state estimate obtained based on the abnormal detection value to the controller while making state prediction based on the state estimate of the previous normal moment. Thus, the impact of the attack on the system stability is reduced to a certain extent in cooperation with the detector before the relevant staff makes attack resistance measures. To simulate the missing real value, based on the predictive control idea, a multistep state prediction is considered to simulate the change of the real value and then combined with the LQG controller to compensate for the control of the system.

Through many simulation experimental tests, the statistical results show that the attack efficiency is below 50% for attack durations below 0.1 s and reaches 100% for durations above 0.8 s. The attack duration with high attack efficiency was not selected, and the attack duration was set every 0.1 s between 0.1~0.8 s. Many tests were conducted for each duration of the attack, and the attack efficiency under different attack durations was obtained as shown in Figure 5.

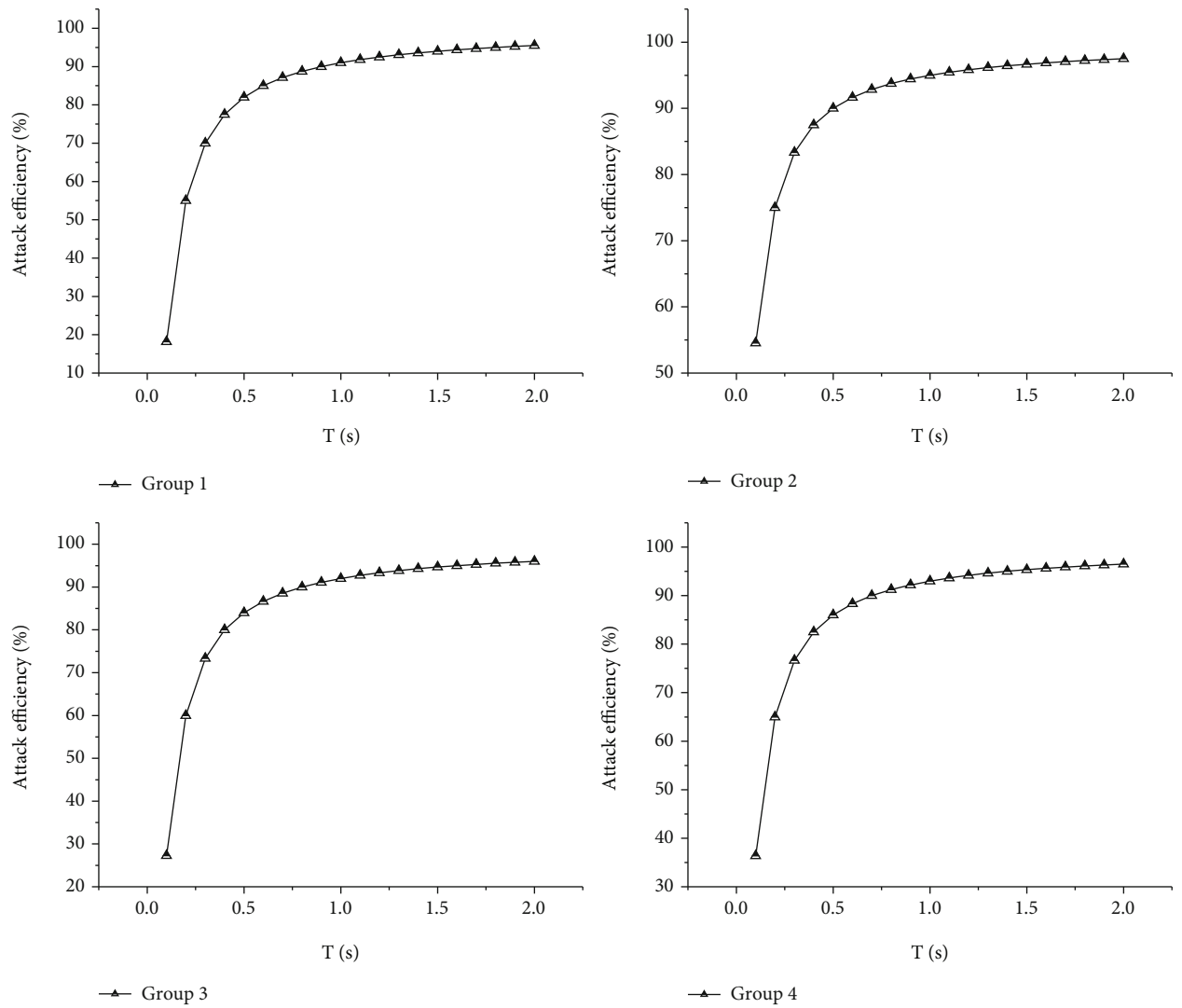

Figure 5: Attack efficiency change curve.

When the attack duration reaches 0.2 s, the attack efficiency is greatly improved compared to 0.1 s and increases with the attack duration, and the detection rate is very close to 100% when the attack duration is higher than 0.6 s. Combining the attacker's attack resources and ensuring a high attack efficiency, the attack efficiency is 94.8% assuming an attack duration of 0.5 s.

To verify the effectiveness and superiority of the cardinality detector in the detection scheme, the Euclidean detector is used as a comparison experiment to verify the false alarm rate, missed alarm rate, detection rate, and accuracy of the two detectors under DoS attack by statistically analyzing the detection values of the two detectors under DoS attack. To better reflect the effectiveness of the improved algorithm in this chapter in locating the coordinates of unknown nodes, the traditional DV-Hop algorithm, the improved algorithm in Chapter 4, and the improved algorithm in this chapter are compared together in this chapter. And the experimental simulation and analysis are carried out by using MATLAB 2018 software with anchor node density, node communication radius, and node density as variables, respectively, through the control variable method. As shown in Figure 6, when the number of anchor nodes increases from 5 to 30, the error of each algorithm decreases, and the error of all three algorithms decreases gradually. When the number of anchor nodes is increased from 5 to 20, the error folding rate of the improved algorithm in this chapter is larger and the decrease is more obvious. In summary, the improved algorithm proposed in this chapter can effectively reduce the algorithm error when the density of anchor nodes is the variable, and the algorithm performance is more stable and has an obvious optimization effect.

The total value of the large cluster BC_i is the sum of the values of all its subnodes. As shown in Figure 7, the DBSCAN algorithm and MinPts parameters have a large impact on the clustering results, so it is necessary to choose the appropriate parameters according to the specific dataset to get more suitable clustering results. Through comparative analysis, the data set used in this chapter is better in the DBSCAN algorithm when is 10 and MinPts is 3. At this

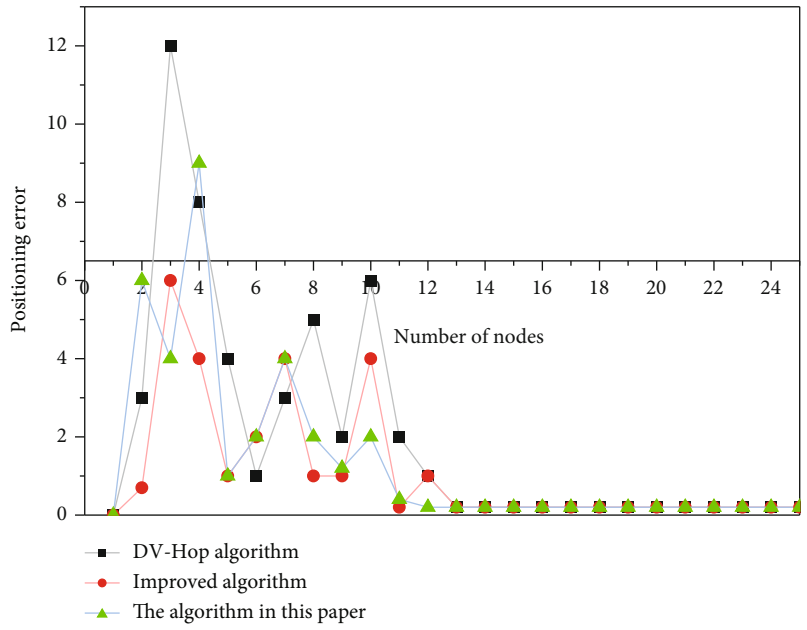

Figure 6: Effect of node density on wireless sensor performance.

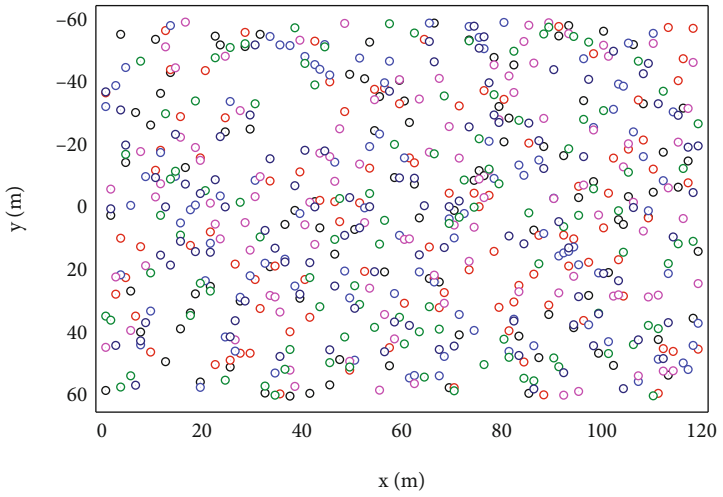

Figure 7: Ethernet security system simulation results.

time, the number of noisy nodes is 12, which is divided into 10 clusters. From the classification results of nodes, although K-means does not have noisy nodes and fully covers the network, the nodes at each distance of the K-means algorithm are scattered, which is not conducive to data collection; the K-value of the K-means algorithm is difficult to determine, and the classification results are greatly influenced by the K-value. However, the DBSCAN algorithm does not need to determine the K-value in advance and divides the area according to the neighborhood and MinPts parameters.

Considering the data collection latency problem caused by the mobile sink, inspired by the pheromone in the ant colony algorithm, the data value of the data is used to describe the data collection priority. If the value of data decays gradually with time, the exponentially decreasing formula is used to model the value of data, considering that the decay rate of data value is from high to low where α represents the initial value at a certain moment, and for the convenience of the study, we set the initial value as a constant. The constant β represents the rate of decay of data value, the more important the data, the faster the decay of data value. With different initial values and different decay rates, the decay curves of values are not the same at all.

7. Conclusion

In this paper, an Ethernet information security prevention system is constructed based on industrial wireless sensor networks. An improvement method is proposed to address the shortcomings of EEUC by optimizing the EEUC

competition radius formula to select candidate cluster heads with random values and energy as weights. The next large cluster is selected as the moving target of the moving sink by calculating the priority of each large cluster among large clusters, and the priority formula considers the value of data as well as the distance factor. The experimental results show that the length of the data collection trajectory of the mobile sink formed by the algorithm is reduced, which reduces the time delay of data collection and considers the value of the data. The node location-related calculation method in the traditional DV-Hop localization algorithm is improved, and the node location problem is changed into the problem of solving the optimal value by first using the PSO algorithm to perform a wide-range search at the beginning of the algorithm execution and taking its location result as the initial value and then using the DFP algorithm to perform a local search for the optimal solution. Through MATLAB experimental simulation, the final improved algorithm in this paper has a good localization effect. An experimental test platform is built for protocol stack communication testing. Combined with the specific experimental test data, it is proved that the PCP-AP structured division of labor design provides good Ethernet real-time performance and efficient data load capacity, and confirms that the POWERLINK-based openSAFETY implementation works well and has great performance improvement space. This study provides a certain theoretical basis for industrial Ethernet security. In the future, in the repeated game of network attacks and information security, industrial control systems may still be "counter-controlled" outbreak. Therefore, in future research, the prevention strategy for the new attack invasion means can be from the security isolation gateway, intrusion detection system, access control, and other technologies as a starting point, to build a network-wide multiprotection system.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was financially supported by the National Natural Science Foundation of China (nos. 62076006 and 61471004), the Anhui Provincial Department of Education Project (2016gkk006), and the Teaching Demonstration Course Project of Anhui Quality Engineering (no. 842).

References

[1] M. Abdulkarem, K. Samsudin, F. Z. Rokhani, and M. F. A Rasid, "Wireless sensor network for structural health monitoring: a contemporary review of technologies, challenges, and future direction," *Structural Health Monitoring*, vol. 19, no. 3, pp. 693–735, 2020.

[2] F. Wan, X. Miao, B. Ravelo et al., "Design of Multi-Scale Negative Group Delay Circuit for Sensors Signal Time-Delay Cancellation," *IEEE Sensors Journal*, vol. 19, no. 19, pp. 8951–8962, 2019.

[3] O. I. Khalaf, G. M. Abdulsahib, and B. M. Sabbar, "Optimization of wireless sensor network coverage using the bee algorithm," *Journal of Information Science and Engineering*, vol. 36, no. 2, pp. 377–386, 2020.

[4] D. Zhang, H. Wu, P. Zhao et al., "New approach of multipath reliable transmission for marginal wireless sensor network," *Wireless Networks*, vol. 26, no. 2, pp. 1503–1517, 2020.

[5] J. Liu, Z. Zhao, J. Ji, and M. Hu, "Research and application of wireless sensor network technology in power transmission and distribution system," *Intelligent and Converged Networks*, vol. 1, no. 2, pp. 199–220, 2020.

[6] B. Cao, J. Zhao, Y. Gu, S. Fan, and P. Yang, "Security-aware industrial wireless sensor network deployment optimization," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5309–5316, 2020.

[7] S. Liu, M. Chen, M. Lei, M. Lu, and Z. Wang, "Electromagnetic and structural analysis on vacuum vessel for CFETR during plasma major disruption," *Journal of Fusion Energy*, vol. 33, pp. 713–719, 2014.

[8] D. Fan, G. P. Jiang, Y. R. Song, Y. W. Li, and G. Chen, "Novel epidemic models on PSO-based networks," *Journal of Theoretical Biology*, vol. 477, pp. 36–43, 2019.

[9] J. Åkerberg, M. Gidlund, T. Lennvall, J. Neander, and M. Björkman, "Efficient integration of secure and safety critical industrial wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, Article ID 100, 13 pages, 2011.

[10] M. Raza, N. Aslam, H. Le-Minh, S. Hussain, Y. Cao, and N. M. Khan, "A critical analysis of research potential, challenges, and future directives in industrial wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 39–95, 2018.

[11] Q. Wang and J. Jiang, "Comparative examination on architecture and protocol of industrial wireless sensor network standards," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2197–2219, 2016.

[12] A. Nechibvute and C. Mudzingwa, "Wireless sensor networks for scada and industrial control systems," *International Journal of Engineering and Technology*, vol. 3, no. 12, pp. 1025–1035, 2013.

[13] J. Gadze, "Control-aware wireless sensor network platform for the smart electric grid," *IJCSNS International Journal of Computer Science and Network Security*, vol. 9, no. 1, pp. 16–26, 2009.

[14] S. Vitturi, C. Zunino, and T. Sauter, "Industrial communication systems and their future challenges: next-generation Ethernet, IIoT, and 5G," *Proceedings of the IEEE*, vol. 107, no. 6, pp. 944–961, 2019.

[15] R. Maaloul, R. Taktak, L. Chaari, and B. Cousin, "Energy-aware routing in carrier-grade Ethernet using SDN approach," *IEEE Transactions on Green Communications and Networking*, vol. 2, no. 3, pp. 844–858, 2018.

[16] Z. Zhou, J. Lee, M. S. Berger, S. Park, and Y. Yan, "Simulating TSN traffic scheduling and shaping for future automotive

Ethernet," *Journal of Communications and Networks*, vol. 23, no. 1, pp. 53–62, 2021.

[17] G. Cossu, A. Sturniolo, A. Messa et al., "Sea-trial of optical Ethernet modems for underwater wireless communications," *Journal of Lightwave Technology*, vol. 36, no. 23, pp. 5371–5380, 2018.

[18] N. A. Naraliyev and D. I. Samal, "Review and analysis of standards and protocols in the field of Internet of Things. Modern testing methods and problems of information security IoT," *International Journal of Open Information Technologies*, vol. 7, no. 8, pp. 94–104, 2019.

[19] N. Miloslavskaya and A. Tolstoy, "Internet of Things: information security challenges and solutions," *Cluster Computing*, vol. 22, no. 1, pp. 103–119, 2019.

[20] R. Mahieu, N. J. van Eck, D. van Putten, and J. van den Hoven, "From dignity to security protocols: a scientometric analysis of digital ethics," *Ethics and Information Technology*, vol. 20, no. 3, pp. 175–187, 2018.

[21] S. Szymoniak and Department of Computer Science, Czestochowa University of Technology, Dabrowskiego 69, 42-201 Czestochowa, Poland, "Security protocols analysis including various time parameters," *Mathematical Biosciences and Engineering*, vol. 18, no. 2, pp. 1136–1153, 2021.

[22] J. Andréasson and U. Pischel, "Molecules for security measures: from keypad locks to advanced communication protocols," *Chemical Society Reviews*, vol. 47, no. 7, pp. 2266–2279, 2018.

[23] Y. Zhang, Y. Liang, J. Chen, and H. Chen, "Effect of lime loading on the performance of simultaneous lime treatment and dry anaerobic digestion of smooth cordgrass," *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects*, vol. 38, no. 20, pp. 3048–3054, 2016.

[24] X. L. Zhang, T. Wu, Y. Shao, and J. Song, "Structure optimization of wheel force transducer based on natural frequency and comprehensive sensitivity," *Chinese Journal of Mechanical Engineering*, vol. 30, no. 4, pp. 973–981, 2017.

[25] Y. Lu, Y. F. Cheng, X. P. He, X. N. Guo, and B. R. Zhang, "Improvement of robustness and ethanol production of ethanologenicSaccharomyces cerevisiaeunder co-stress of heat and inhibitors," *Journal of Industrial Microbiology and Biotechnology*, vol. 39, no. 1, pp. 73–80, 2012.