Hindawi
Complexity
Volume 2021, Article ID 9924291, 12 pages
https://doi.org/10.1155/2021/9924291

Research Article

Topology Control and Medium Access Control (MAC) Protocol for Wireless Sensor Networks (WSNs) in Cyber-Physical System

Ang Li,[1,2] **Chen Zhang**,[1] **Baoyu Zheng**,[2] **and Lei Li**[2]

[1]*Institute of Electronic Engineering and Optoelectronic Technology, Nanjing University of Science and Technology Zijin College, Nanjing 210023, China*
[2]*College of Telecommunications & Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210023, China*

Correspondence should be addressed to Ang Li; 2015010215@njupt.edu.cn

Received 2 April 2021; Accepted 23 April 2021; Published 3 May 2021

Academic Editor: Wei Wang

The system reachability set is calculated by covering all possible behaviours of the system through a finite number of simulation steps to ensure that the system trajectory stays within a set safety region. In this paper, the theory of the game method is applied to the design of the controller, a very small controller is designed, and good control results are obtained by simulation. The system gradually shows a divergent trend and cannot achieve stable control. A multihop channel reservation Medium Access Control (MAC) protocol based on a parallel mechanism is proposed. The multihop channel reservation mechanism is proposed based on periodic node sleep, and the node uses the reservation frame to make the reservation of the channel and transmits the data according to the reservation information; the parallel mechanism is used to make the reservation information and data transmission simultaneously.

1. Introduction

Cyber-physical system (CPS) is a high-efficiency cybernetically networked intelligent information system that integrates computation, network, and physical entities based on environment sensing and integrates the 3Cs (computation, communication, and physical information) [1]. The technology of the large-scale engineering system can be integrated and collaborated in depth to realize real-time sensing, dynamic control, and later information service [2]. The essence of this is to enable the network to monitor physical processes through embedded computers, while physical processes influence computational processes through feedback, ultimately completing the interaction between physical and computational processes [3]. The recovered soft information of the UE's lost packet is combined with the local undecodable soft information of the same packet to form a distributed turbo code [4]. Integration does not imply a simple fusion of the physical world and cyberspace, but rather a deep interaction of physical and cyber components, and the analysis and design of CPS are a synthesis of physical dynamic processes, computers, software, and networks [5]. In the future, CPS will be widely used in critical infrastructure monitoring and control, defense weapon systems, environmental monitoring, smart home, and life support, aerospace and space systems, health care, intelligent highways, etc. The emergence of CPS will change the way people interact with the physical world and controllers, as well as controlled systems and wireless communication components [6]. Sensors collect information about the physical operation of the system and transmit this information in real time to computers and embedded systems for intelligent control [7]. The information-acquisition part of the process is often subject to hardware constraints, imperfect communication constraints, and time-varying transmission environments [8]. Actuators can receive control commands and exert control over controlled objects [9]. The controller has some computational capabilities and can obtain data from the sensors over the network to derive the control quantity to be passed to the actuator based on a written control algorithm [10].

CPS Week is the most important event on information-physical fusion systems, with five leading conferences from all over the world covering all aspects of CPS, bringing together academics from all over the world to discuss technical developments [11]. Several prestigious universities and research institutes have also conducted a series of studies on CPS, with some innovative and representative results [12]. Representative examples include Mobile Integrated Terminal (MIT)'s Distributed Intelligent Robot Garden, the Pennsylvania School of Engineering's car navigation software Groove Net, and Carnegie Mellon University's Smart Grid [13]. The literature provides an overview of the various types of attacks that can be expected in an information-physical converged system [14]. Problems in existing information security and network control systems to secure information-physical converged systems are discussed, as well as new directions and challenges for improving security [15]. The literature develops a framework for detecting and identifying measurement errors caused by adversaries in a network [16]. The authors of the literature studied the impact of attacks on data communication in network control systems [17]. In this literature dedicated to the design of feedback controllers that minimize the control objective function, only packet loss is considered and no latency is considered [18]. The design of predictive controllers under delay and packet loss is proposed, but the disorder is not explicitly considered [19]. Sahoo et al. studied the application of Kalman filtering under measurement loss using the Bernoulli process and proposed a threshold condition for the packet loss probability for the optimal estimation and gave a threshold function [20]. The condition for studying the control or packet loss probability is that the control system can tolerate and still maintain the reliability of the system [21]. The Bernoulli model is commonly used to model packet loss in control systems, and Bernoulli has been widely studied in recent years due to its generality and ease of handling [22]. However, the Bernoulli process only gives a discrete probability distribution model for packet loss, without considering the delay and observation noise [23]. The network is the core of the CPS, where the components of the system exchange and transfer information, and the information system structure in the CPS is complex and heterogeneous, and the system has become more complex and open as it has evolved, making it extremely vulnerable to external interference and even malicious attacks [24]. Under the threat of malicious attacks, how to design a defense control strategy to control and recover from failures promptly so that the system can correct errors in a short period and prevent them from spreading without affecting the normal working state of the system is the focus of CPS security research [25].

CPS is a network with control properties, but it is different from the existing control systems. Information-physical converged systems are prone to failures, such as attacks on their physical infrastructure, as well as attacks on the data management and communication layers. Concerns about the security of control systems are not nascent, as there is much literature on system failure detection, isolation, and recovery. For some of the deficiencies that exist in CPS that do not affect the control system, appropriate detection and identification techniques need to be developed. The reliance on communication networks and standard communication protocols to transmit measurement and control packets increases the likelihood of attacks on physical systems. Information security methods, such as authentication, access control, and message integrity, do not appear to be sufficiently effective in protecting information physically fused systems. These security methods do not take advantage of measurements on controlled systems under physical processes or control mechanisms, and they are ineffective against attacks on physical systems. Information-physical fusion systems consist of deeply integrated, tightly coupled computational and physical components with communication capabilities. These systems are highly complex and span multiple scientific and technical domains. As a result, they also pose many challenges, and they are extremely important for the progress and security of society. PS is becoming more complex, open, and vulnerable to security threats, making security an important issue to consider when designing CPS.

2. Topological Control and MAC Protocol Analysis of WSNs in CPS

2.1. Information-Physical System Design. CPS shares some common features with popular Information and Communication Technology (ICT) systems, such as embedded systems, Networked Control Systems (NCSs), the Internet of Things (IoT), and the Internet of the Future [26]. Here is an overview of the relationship between CPS and other emerging technologies. CPS is also not the Internet of Things, although they are sometimes used interchangeably. The Internet of Things typically corresponds to a hierarchical communications infrastructure with application-driven ways of sensing, processing, and transmitting the information.

On the other hand, it emphasizes dynamic interaction between physical processes and networks. IoT is more like a platform for implementing several applications. In other words, it is an extension of the Internet. In contrast to the Internet of Things, CPS is a way to go about realizing and designing the real world. The coming Industrial Internet refers to the integration of global industrial ecosystems, pervasive sensing, advanced computing, and pan-network connectivity to the increasing benefits of the world economy. Thus, its technological foundation is CPS. Wireless sensor networks (WSNs) are one of the main ways of information access in CPS [27]. The development of wireless sensor network technology will help the realization of CPS, and the construction of the existing wireless network environment will provide a good platform for the development of CPS. However, WSN technology has certain limitations; sensor nodes in space are static configuration, belonging to an open-loop monitoring mode. Wireless sensor network in CPS is characterized by rapid changes in the network topology, and CPS not only contains sensors but also contains actuator nodes, and monitoring needs to ensure closed-loop interaction control and nodes with autonomy, as shown in Figure 1.

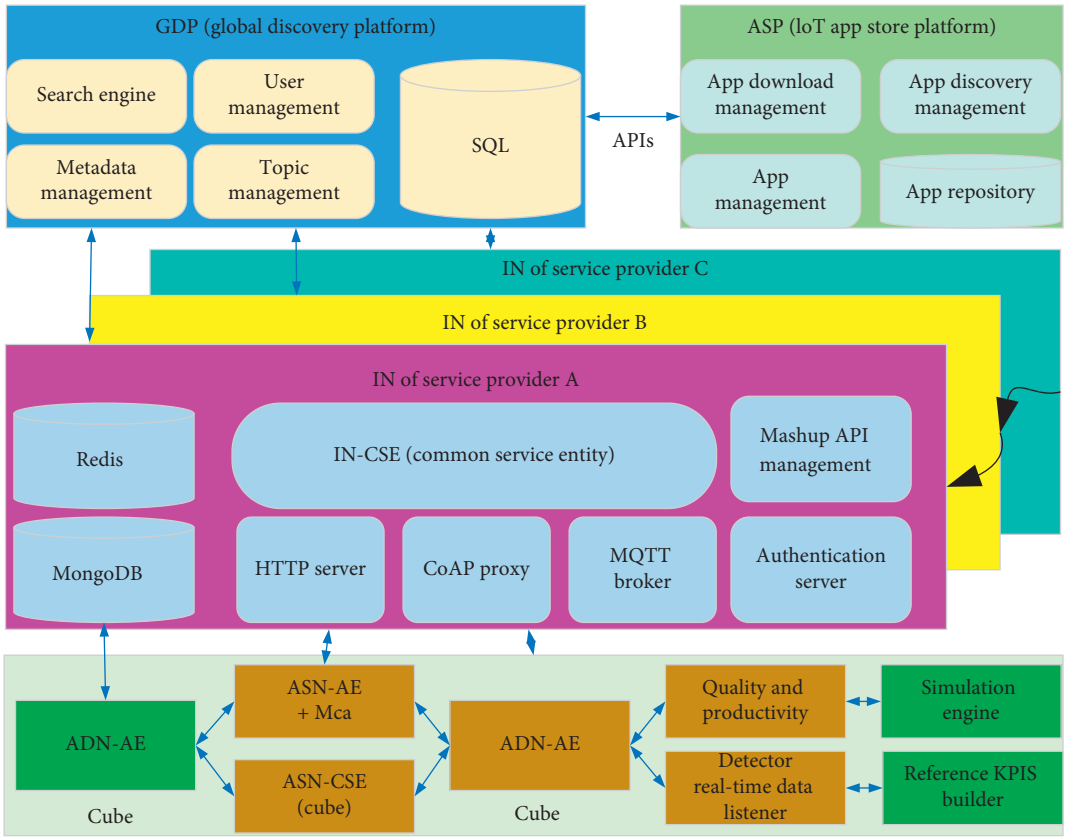

Figure 1: CPS framework.

Rapid advances have been made, but there will still be significant challenges in designing a CPS using existing underlying theory and techniques. The goal of a CPS is to achieve a real-time, efficient interaction between computational and physical processes. This close interaction, while having many advantages, also poses many risks. New types of risks include adverse effects of the information system on the physical environment as well as adverse effects of the physical environment on the information system. Therefore, security, reliability, defensiveness, confidentiality, and adaptiveness, which are less important features of traditional computing systems, are the focus of CPS. Research in related security areas has focused on the development of tools and techniques to address known security issues. Important security tools, such as antivirus software and intrusion detection systems (IDS), are important. This approach to security is effective in responding to attacks using off-the-shelf tools and popular techniques. However, the response measures to new attack vectors and methods are inadequate. This continues to push the security frontier and stimulate the need for proactive security approaches. An important feature of CPS is the seamless and complex interaction between the computing unit and the physical environment. CPS should be designed and implemented with strict security, which requires a safety verification of failures. In the field of safety-critical systems, safety verification of the system model using formal verification theories and techniques that can prove the correctness of the system model is extremely important and has been a major concern in recent times.

Safety in CPS can be divided into fault safety and active safety. Failure safety refers to the prevention of system failures caused by unintentional actions in normal operation and is the avoidance of occasional failures, while active safety prevents the loss of system functions caused by intentional damage by operators and focuses on the active prevention of malicious attacks. For the safety design of the CPS system, the main concern is how to prevent accidents, so safety research should be divided into the following two aspects: for the absence of an attacker, to ensure fault safety, the system's reach should be calculated and verified; for the presence of a malicious attacker, to ensure active safety, the system should be resilient and have robust control. The safety test is to verify that, from the given initial conditions, the system will operate in violation of the statute or is unsafe. Due to the continuous advances in technology and the increasing complexity of technical systems, strong verification methods already exist for purely discrete systems that can prove the safe operation of quite complex systems, and for hybrid systems with discrete and continuous dynamic combinations, safety assessment is a common problem for many classes of systems. A simple way to check the safe operation of mixed systems is to apply Monte Carlo simulation. Monte Carlo simulation focuses on calculating the probability of system failure, and there are methods for generating test cases in such a way that makes it possible to maximize test coverage to detect unsafe executions [28]. However, its disadvantage is that it does not prove the safety of the system.

2.2. WSN Topology Control Analysis Design. Data fusion is a multilevel processing process that automatically detects, estimates, federates, correlates, and combines data from multiple sources. The working environment and node characteristics of WSNs determine the necessity of data fusion. Firstly, WSN nodes are energy-intensive and need to minimize the amount of data transmission to save energy. Sensor nodes are battery-powered, and most of them are manually scattered in random areas, making it difficult to replenish energy by replacing batteries. Once the network runs out of energy, the data transmission capabilities of the WSN will be lost. The main energy-consuming modules of the node are the wireless transmission module, sensor module, and processor module; with the support of advanced circuit technology, the energy consumption of the processor and sensor is very low, and the main energy consumption comes from the wireless AC module. Therefore, to extend the node life, it is highly necessary to fuse the data to reduce the wireless transmission capacity. Second, the data in WSNs is often redundant and needs to be fused to obtain more accurate information. Compared to transmitting aggregated data, transmitting raw data does not bring more information to users and may lead to data conflicts, and the retransmission mechanism in WSNs will further increase network energy consumption and reduce information collection efficiency [29]. Therefore, it is necessary to fuse the redundant raw data to reduce data conflicts and improve information collection efficiency. Thirdly, WSN nodes often collect inaccurate data and require fusion algorithms to remove the effects of such data. On the one hand, WSN nodes are often deployed in environments with extreme variations in pressure, temperature, radiation, or electromagnetic noise, which make it difficult to achieve high accuracy of measurement data; on the other hand, there may also be anomalous nodes that send false data. If these inaccurate data are sent directly to the base station, the user will get biased results. Therefore, data fusion techniques are needed to process all the perceived data in the area to be monitored to obtain more accurate information. In summary, to improve the efficiency of information collection, increase the utilization of network broadband, and extend the life cycle of the network, it is necessary to perform data fusion, as shown in Figure 2.

Among them, the probabilistic model-based algorithm is suitable for situations where the user needs to know not only the monitoring results but also all the information of each node, and the data transmission volume is huge; this type of algorithm does not contain an anomalous data processing module and the data within the tolerance range is not transmitted, so the accuracy is the lowest; moreover, the energy-saving of this type of algorithm depends on the specific setting of the model and tolerance level. Neural network algorithms have good energy savings and very low information transfer, but not high accuracy. The Kalman filtering algorithm reduces the effect of white Gaussian noise and thus has higher data accuracy than other algorithms; and it has good energy savings and very low data transmission and is widely applicable to many agricultural IoT monitoring systems.

Scale-free networks consider two important characteristics of real networks: the size of the network is not fixed, but is constantly expanding. New nodes joining the network are more likely to be connected to nodes of larger size [30]. For these two network characteristics, two mechanisms are introduced in the construction of the scale-free network model: a growth mechanism and a preferential connection mechanism. Growth mechanism: The initial network consists of nodes. Only one node is added to the network at a time, connecting to the existing nodes. When a new node joins the network, it gives preference to the larger nodes in the network. The probability that a new node connects to an existing node P_{m} is

$$P_m = \frac{K_m}{\sum_i^M \sum_M^M K_m + K_j - K_i}. \tag{1}$$

The algorithm calculates the edge capacity based on the remaining energy of the nodes and periodically invokes the maximum flow algorithm to calculate the broadening path and traffic flow to maximize the network load traffic [31]. The edge capacity is calculated as follows: assuming that the energy consumption of a node is P_m, the energy consumption of a node receiving a packet is E_i, the energy consumption of a node sending a packet is K_m, and the number/capacity of packets that a node can forward is defined as C_i.

$$C_i = \frac{E_i + E_j}{K_m + P_m},$$

$$C\left(n_i, n_j, n_m\right) \begin{cases} \delta_{i,j,m} * C_i, \ n_i \neq n_j, \\ C_j, n_i = n_j, \text{and } n_i = n_m, \\ C_m, \text{others}. \end{cases} \tag{2}$$

The edge capacity on the virtual source and virtual destination nodes and their neighbour nodes is determined by the ability of their neighbour nodes to forward packets. This is because the virtual source node and virtual destination node have infinite energy and the edge capacity is determined by their neighbour nodes with finite energy.

$$\delta_{i,j,m} = \begin{cases} \dfrac{E_i + E_j}{\sum_i^M \sum_j^M \sum_m^m K_m + K_j - K_i}, & \text{if } N_i \neq 0, \\ \dfrac{E_i - E_j}{\sum_i^M \sum_j^M \sum_m^m K_m + K_j - K_i}, & \text{others}. \end{cases} \tag{3}$$

Preference is given to a node to send packets to its lower-level neighbour nodes for the sake of a minimum number of hops; a node is considered to send packets to its fellow neighbour nodes only if it does not have a lower-level neighbour node. The scale factor is the meaning of the percentage of the energy of the neighbour node R in the sum of the energy of all neighbour nodes. The average energy collected by the node in a second is R, and all nodes have the same energy collection rate.

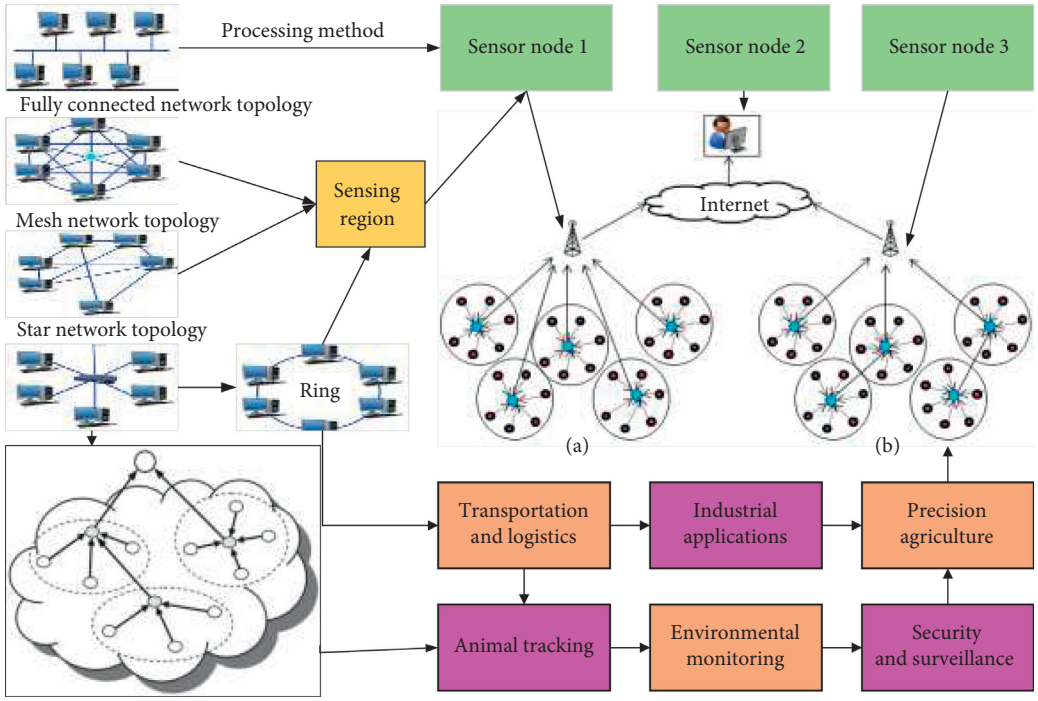

Figure 2: WSNs data topology control model.

$$R_{\chi} = \left\{r_{t+1}, r_{t+3}, r_{t+5}, \ldots, r_{t+2\chi+1}\right\}. \tag{4}$$

The elements of R can be identical; "identical" means that the path of the packet is the same twice, and the packet will necessarily choose a broadened path calculated by the maximum flow algorithm as the transmission path. Flag denotes the containment relationship between a node and the route g_i.

$$\text{flag}_i = \begin{cases} 0, & \text{if } n_i = n_m, \\ 1, & if\ n_i \neq n_m. \end{cases} \tag{5}$$

For the Pierre Mendes France (PMFR) algorithm, if the source node sends packets at time t, the set of periods for periodic invocations of the maximum flow algorithm can be represented as

$$H = \left\{H_{t+1}, H_{t+3}, H_{t+5}, \ldots, H_{t+2\chi+1}\right\}. \tag{6}$$

Similarly, it is possible to calculate the edge capacity now of C according to the following equations:

$$C\left(n_i, n_j, n_m\right) \begin{cases} \delta_{i,j,m} * C_i, & n_i = n_j, \\ C_j, n_i = n_j, & \text{and } n_i \neq n_m, \\ C_i, & \text{others.} \end{cases} \tag{7}$$

$$\delta_{i,j,m} = \begin{cases} \dfrac{E_i + E_j}{\sum_i^N \sum_j^M \sum_m^N K_m + K_j - K_i}, & \text{if } N_i \neq 0, \\ \dfrac{E_i - E_j}{\sum_i^N \sum_j^M \sum_m^N K_m + K_j - K_i}, & \text{others.} \end{cases} \tag{8}$$

If it is the first packet transmission, there is no need to update the remaining energy of the node because the node has not started collecting energy; if it is not the first packet transmission, there is a need to update the remaining energy of the node [32]. Determine whether the edge capacity needs to be updated according to (9); if the edge capacity is updated, calculate all edge flows and the maximum flow according to the maximum flow algorithm.

$$f_{r\left(n_i, n_j\right)}\left(t_m\right) = f_{r\left(n_m, n_j\right)}\left(t_i\right) - p * \left(t - t_m\right) + p * \left(t_i - t_j\right). \tag{9}$$

2.3. MAC Protocol Design Analysis. When designing a MAC protocol, the actual requirements and overall performance of the network should be taken into consideration. Nodes receive and process unnecessary data from neighboring nodes. The crosstalk phenomenon causes the wireless transceiver and processing modules of nodes to consume more energy because of the design of the MAC protocol. In the specific application of wireless sensor networks, the number of sensor nodes and their distribution density in the network are subject to change. The death of old nodes as well as the addition of new nodes must require good dynamics of the network topology. Wireless sensor networks, as a distributed self-organizing network, require MAC protocols that are adaptable and scalable to cope with changes in network load and topology.

If there are too many control messages, the sensor network will also consume more energy to execute the control messages. However, there are specific applications where energy efficiency is less important than the packet-

to-packet ratio and low latency, where high transmission rates can be achieved at the expense of energy efficiency. Communication protocols generally prioritize energy efficiency and are designed to tolerate latency and other issues. However, when it comes to specific application requirements, energy efficiency is less important than packet-to-packet ratios and low latency, and communication protocols should be responsive. The protocol must also be able to prioritize packets carrying critical data, as they often contain important sense data and require efficient transmission. Also, the protocol must support fairness to the source of the packet. Fairness is important when there is a hazard, and an aggregating node can receive complete information from all sensor nodes to monitor the propagation of the hazard.

The parent node responds to an acknowledgment (ACK) message to its children to confirm that each child node is added to its list of children. If a node does not receive an acknowledgment message after a specific period broadcast, the message is replayed. A node keeps broadcasting the construction tree information until it receives an acknowledgment message or exceeds the maximum value to retransmit. If a node updates its Parentnode_id and its Hop, it also needs to notify its old parent node after reestablishing the build tree information, and the old parent node responds to the node with an acknowledgment message informing the node that it has been removed from the list of child nodes. If the node does not receive the old parent's acknowledgment message, it will rebroadcast the build tree information, and the old parent's acknowledgment message will help the child node list the most recent information. If the list of child nodes is not updated, the old parent node may try to receive some packets from the child node, thus wasting energy on idle listening. The node will keep broadcasting the tree building information until it receives an acknowledgment or exceeds the maximum number of retransmissions. During the tree network building phase, the node may crosstalk to hear transmissions from other nodes within its transmission range. The node records the sender of the message as one of the nodes in its list of single-hop neighbour nodes. At the end of this phase, all nodes in the network have received the tree building message. When this phase is over, each node knows the number of hops that reached the convergence node, its parent, the list of children, and the list of single-hop neighbours' nodes.

During this phase, nodes perform slot allocation and exchange scheduling plans, making sure that no node shares a slot between two hops, as their transmissions may collide if nodes have the same slot within two hops. At the end of the slot allocation phase, each node ensures that its scheduling plan is different from that of its single-hop and two-hop neighbours to avoid conflicts. Time slot allocation follows a bottom-up approach, starting with a leaf node (with no children), and the purpose of the time slot allocation job is to ensure that the transmission plan from the leaf node can support the flow of messages to the aggregating node. During the time slot allocation phase, all communications are scheduled for conflict-free periods using CSMA/CA.

3. Analysis of Results

3.1. Simulation and Analysis of WSN Energy Consumption with Different Number of Cluster Heads. In the LEACH algorithm, the setting of the number of cluster headers is an important factor that affects the energy consumption of WSN. If the number of cluster headers is too few, some nodes in the network are too far away from the cluster head locations, resulting in higher energy consumption for transmission between the nodes and the cluster headers; if the number of cluster headers is too high, the energy consumption for communication between the cluster headers and the base station is too high. Therefore, there should exist an optimal number of cluster heads that minimize the total energy consumption of the entire network. Figure 3 simulates the variation of WSN energy consumption as a proportion of the number of cluster heads. The figure shows that as the ratio of the number of cluster heads increases, the network energy consumption first decreases and then increases. In this experiment, the overall energy consumption of the WSN is minimal when the number of cluster headers is about 4% of the total number of nodes. Also, it can be seen in Figure 4 that the LEACH algorithm reduces energy consumption by a factor of 7 compared to the direct communication protocol when the optimal number of cluster heads is selected. The energy savings of the LEACH algorithm come from the combination of data routing and lossy compression. There is a trade-off to be made between the output quality of the data and the compression ratio. In this case, despite some data loss, the energy consumption of the entire system is significantly reduced.

The energy consumption for node data transmission is closely related to the transmission distance, so the difference in network diameter will have an important impact on the energy consumption of the WSN. Figure 5 simulates the relationship between the total WSN energy consumption and the network diameter for the LEACH algorithm and two reference algorithms when the cluster header ratio is 5%. The results show that the LEACH algorithm reduces the energy consumption by a factor of 7 to 8 compared to Direct, while the LEACH algorithm reduces the energy consumption by a factor of 4 to 8 compared to the MTE protocol.

Figure 6 compares the total energy consumption of the system under the Low Energy Adaptive Clustering Hierarchy (LEACH) algorithm with the total energy consumption of the system under the two reference algorithms when the network diameter and the initial energy of the nodes are varied. The results show that the LEACH algorithm has a significant energy-saving effect for most of the parameter values. The main significance of the node energy balance is that it can balance the energy consumption among nodes and prevent individual nodes from consuming energy too fast. The variance is a mathematical quantity used to describe the fluctuation of the sample data: the larger the variance, the larger the difference between the sample and the mean. The greater the variance in the simulation of node energy balance, the greater the difference between the remaining energy of each node, reflecting that the individual node energy

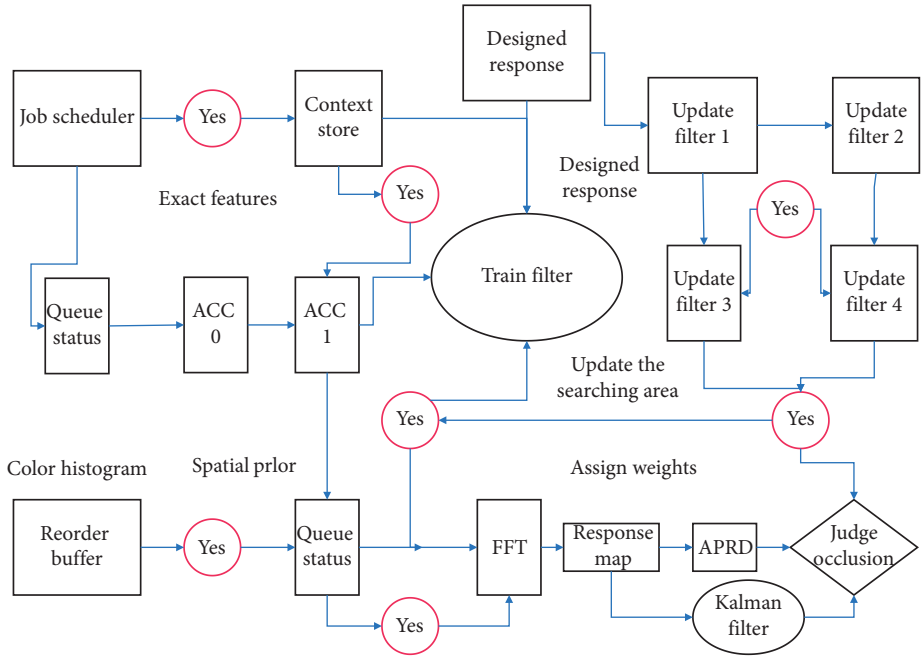

Figure 3: MAC protocol design.

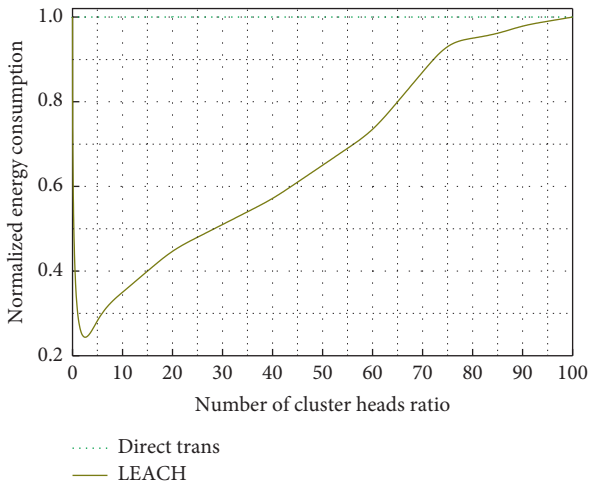

Figure 4: Relationship between system energy consumption and percentage of cluster headers.

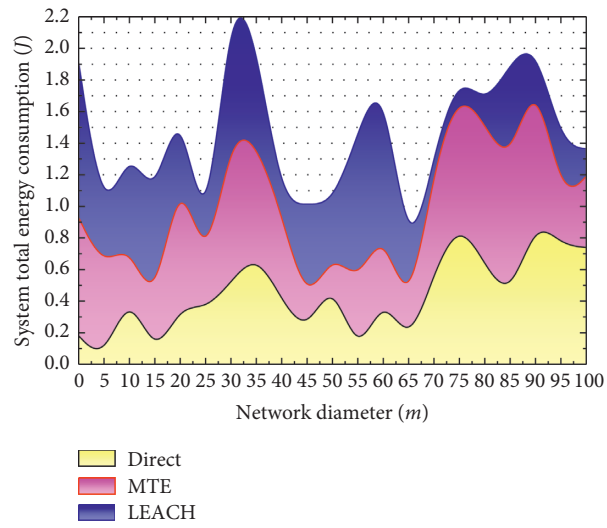

Figure 5: Total system energy consumption versus network diameter.

consumption is too fast; and the smaller the variance, the smaller the difference between the remaining energy of each node, reflecting the node to share the energy consumption.

The trend of energy consumed as the packets sent varies from 2 bits to 4096 bits. The Genomics Education and Training Center (GETC) and Coastal Transit Bill Container (CTBC) algorithm are better than the transmission energy consumed by the maximum transmission power, and the GETC algorithm consumes less energy. When the packet size is 4096 bits, the energy consumed by GETC is 440 MJ, which is only 56% of the energy consumed by the maximum transmitting power. Figure 6 shows the simulation of carrying out node energy balance, Link-2 is not using node energy balance, and the data is transmitted over a fixed link. Link1-1 and Link1-2 alternate data transmission between two different links according to the adaptation function after node energy balance is adopted. The analysis of 6 reveals that the energy consumed by transmitting on the link is spread over two links. It is found that the energy consumption of both links is smaller than that of Link-2, but the sum of energy consumption of both links is the same as that of Link-2, which does not increase the energy consumption because of the energy balance.

3.2. MAC Protocol Performance Analysis. Figure 7 shows the average latency of the simulated high-priority packets. ER-MAC's high-priority packets have lower latency than

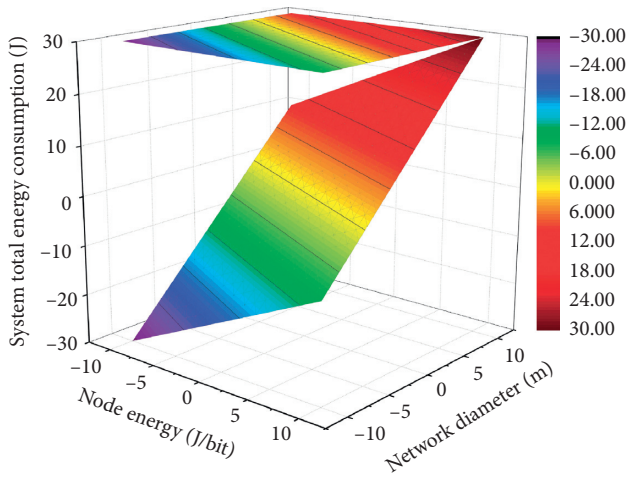

Figure 6: Comparison of energy consumption when network diameter and node energy change.

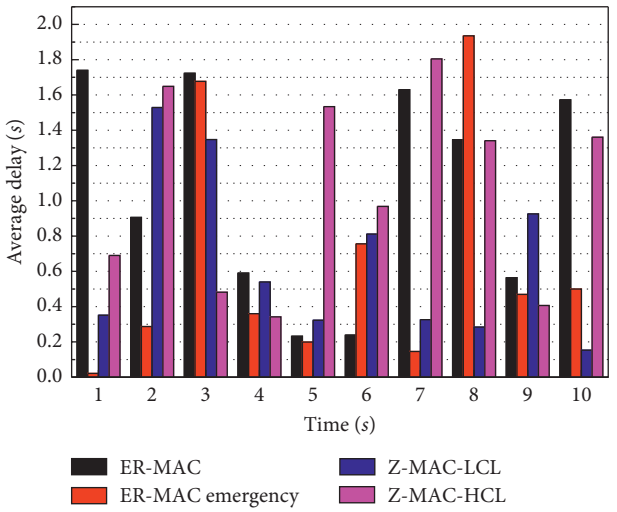

Figure 7: Comparison of the average latency of high-priority packets under different loads.

Z-MAC's high-priority packets. This is because ER-MAC maintains two priority queues that separate the high-priority packets from the low-priority packets, and the high-priority packets always transmit transmissions first until the queue is empty. On the other hand, Z-MAC uses only one queue to send high- and low-priority packets one after the other, so the latency of Z-MAC's high- and low-priority packets is almost identical. In the event of an emergency, nodes can propagate data faster by competing for some unused time slots, and the latency of high-priority packets is reduced.

Another simulation scenario is shown in Figure 7, in which the network load profile is changed over a range of 500 s. The network traffic changes every 100 seconds, from 5 packets per node per minute to 25 packets per node per minute, and then drops to 5 packets per node per minute. The network load is varied to simulate the changing network environment from normal monitoring to emergency monitoring. As a node generates more traffic, it changes the behaviour of the MAC from normal to emergency mode and

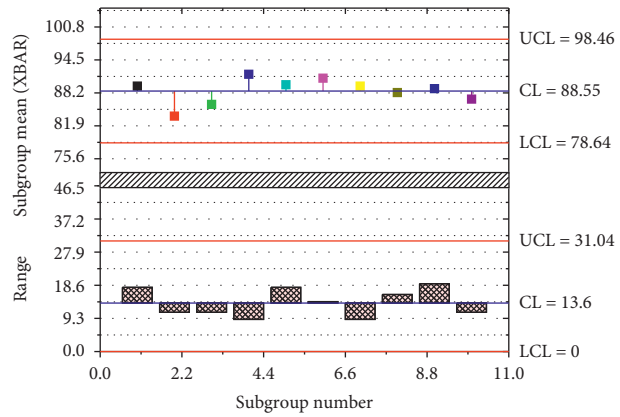

Figure 8: Transmission rate of high- and low-priority packets for MAC protocol in emergency and HCL situations.

back to normal mode as it reduces traffic. Based on this, a comparison between ER-MAC and Z-MAC was made. Over time, changes are found in the average delay of each node. In general, ER-MAC is better than Z-MAC because of the high-priority queues and it has lower latency than Z-MAC for high-priority packets. Z-MAC uses only one queue and sends it. High- and low-priority packets must be sent one after the other.

To compare the delivery rates of high- and low-priority packets, you can force the source node to generate both types of packets at the same time. Figure 8 shows that ER-MAC's high-priority packets are delivered better than Z-MAC's packets and ER-MAC's low-priority packets. In Figure 8, the curves for Z-MAC's high-priority packets and low-priority packets are the same because Z-MAC has no priority, so the percentage of packets delivered is the same for both types of packets. Z-MAC running in HCL mode achieves a higher delivery than ER-MAC when the traffic is very low because the packet is lost when the data is retransmitted and the sender does not receive an acknowledgment message. On the other hand, ER-MAC does not acknowledge each packet, so it does not retransmit lost data. Even when traffic increases, the ER-MAC's delivery rate for high-priority packets decreases, but the decrease is minimal. This is caused by contention in the TDMA time slot, which prioritizes the propagation of high-priority packets in emergencies, as shown in Figure 8.

Figure 9 shows the average energy consumption per node in the simulation experiments. ER-MAC in normal and emergencies consumes less energy than Z-MAC in LCL and HCL modes. This is because, in ER-MAC, the owner of a time slot does not need to compete for access to a channel if it has a message to send. However, in Z-MAC, the time slot owner must compete for the channel before sending data, despite having priority access. The data also shows that, during emergencies, ER-MAC nodes consume more energy than normally monitored because they wake up to contend in every time slot. Energy consumption of ER-MAC nodes is high during emergencies and when the network load is low because more nodes compete for access instead of using their transmission slots to send data if neighboring nodes do not

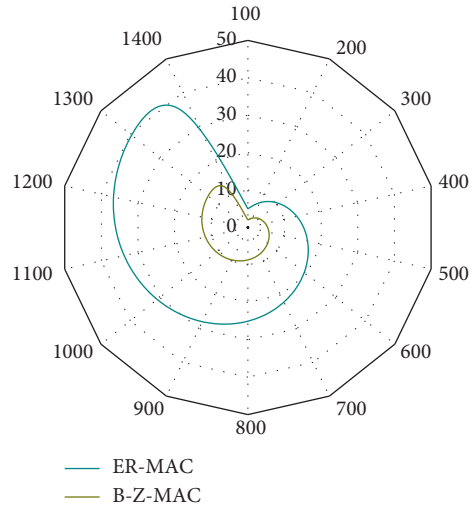

Figure 9: Comparison of energy consumption under load over time.

have data to send. In other words, the lower the load on the network is, the more competition the network may have in an emergency.

Figure 9 shows the variation of average energy consumption per node for ER-MAC and Z-MAC as the load varies over time. Overall ER-MAC performs better than Z-MAC because it has higher energy efficiency; higher priority packets also have better transmission rates and lower latency. The overhead for time slot contention becomes larger. The protocol performance is analysed and evaluated in terms of node delivery rate, packet delivery latency, and energy effectiveness using NS2 and the simulation experiments on ER-MAC. The simulation experiments confirm the scalability of the protocol and achieve higher delivery rates, with lower latency and lower energy consumption.

The sender of a scheduling message receives a conflicting message, depending on the source of its conflicting message, its single-hop neighbour node or its two-hop neighbour node updates the conflicting message and then redistributes the scheduling and broadcasts a new scheduling message to its two-hop inner neighbour node. However, channel conflicts are possible during random storage, and conflicting information may be lost during transmission. If their scheduling messages do not conflict, the neighboring node receiving the scheduling message sends a nonconflicting message to the sender of the scheduling message. To reduce more conflicts, the sender of the scheduling message keeps a list of neighbour nodes; it receives the nonconflicting messages and adds the information from this list to the scheduling message. A neighbour node that does not send a nonconflicting message, if it is in the list, does not receive more nonconflicting messages from its two-hop neighbour node after broadcasting the scheduling message several times, and the sender of the scheduling message conveniently assumes that its scheduling schedule does not conflict with the scheduling schedule of its two-hop neighbour node, and then the node sends the scheduling message directly to the parent node into a notification message (INFORM), and the parent node receives this message and replies Confirmation message, as shown in Figure 10.

In microgrid monitoring, the network nodes require high accuracy to collect information, and it is necessary to avoid blind spots due to the death of individual nodes; therefore, it is necessary not only to compare the network survival time under each algorithm, but also to compare the time of the first dead node in the network and the distribution of dead nodes in the network. The relationship between the surviving nodes and the survival period of the three algorithms in Figure 11 shows that the Batch Update Clustering Algorithm (REBUCA) significantly increases the network survival time and the time for the first dead node to appear compared to the LEACH and EEUC algorithms. In the basic clustering of the network, the REBUCA uses nonuniform clustering to avoid the problem that the cluster headers near the convergence point do not have enough energy to forward the other clusters due to the large cluster size. The EEOC nodes need to interact with each other to negotiate the final cluster head node. The REBUCA considers the distance and energy factors for both the radius of competition and the waiting time and takes more reasonable values to better balance the network energy consumption. Also, the REBUCA sets the rotation weights to avoid reclustering every time, which reduces the number of clusters and leaves more energy for data monitoring rather than network construction.

A multihop channel reservation MAC protocol based on a parallel mechanism is proposed, which rationalizes the data transmission and reduces unnecessary idle listening through the channel reservation mechanism. By using the parallel mechanism, the transmission of reservation information and data is carried out simultaneously, saving energy consumption. To a certain extent, it reduces the energy consumption of nodes in WSN, reduces the delay in multihop transmission, and improves the life cycle of the network. The effectiveness of the PCR-MAC protocol is verified by comparing different MAC protocols through the OPNET network simulation tool.

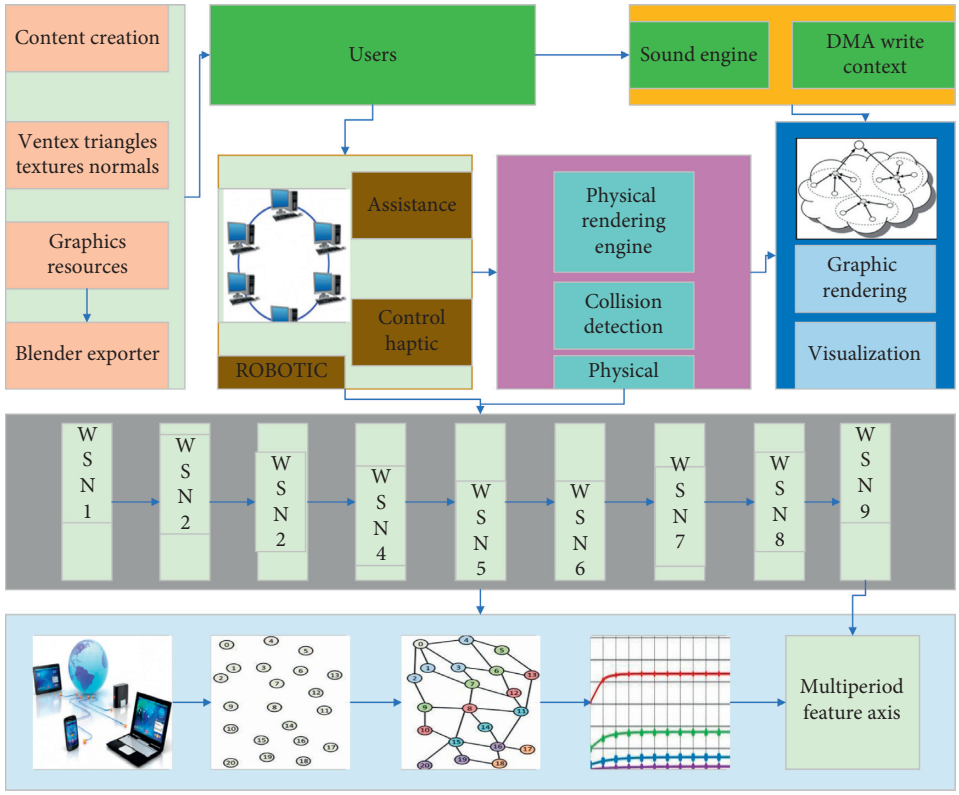

Figure 10: WSN control and MAC protocol performance in cyber-physical system.

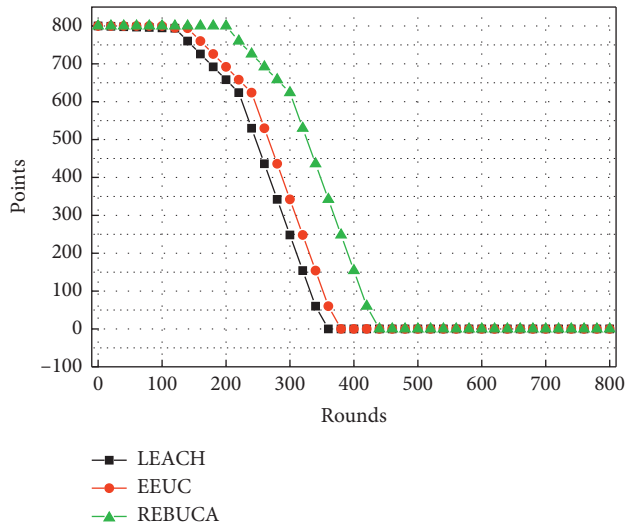

Figure 11: Surviving nodes vs. surviving cycles.

4. Conclusion

In this paper, based on the analysis of the WSN topology control algorithm, an energy balance topology control algorithm based on a geometric structure is proposed. First of all, we established constraints to ensure network connectivity, under the premise of meeting the constraints, by controlling the transmission power to establish an effective transmission link and reduce unnecessary connections; secondly, based on ensuring network connectivity, the use of planar geometry to draw auxiliary lines, and geometric cutting, the location of the node is divided into different regions, for different regions of the topology of the link. Determine and add some links to enhance the reliability and overall energy optimization of the network; then apply the node energy balancing mechanism to balance the energy consumption of each node and prevent individual nodes from dying due to excessive energy consumption, thus improving the performance of the entire network. A very small controller is designed for the characteristics of the information-physical convergence system. For a large information-physical converged system composed of wireless sensor communication nodes, due to network instability, or suffer from external attacks, it is easy to cause packet loss, out of order, etc., which has a serious impact on the control of physical devices; therefore, this paper defines the attack type as a packet timing attack. Under the interference of this attack, the controller can compensate for the delayed data formation and play a certain inhibitory role in the interference, using the double water tank as the control model, and the simulation results show that it can meet the requirements of stability and robustness of the control. In contrast, the LQG controller clearly cannot play a stable control role in this situation. To improve the energy efficiency and topology robustness of network topology control algorithm. An energy balance topology control algorithm based on geometric cut is proposed. The algorithm firstly performs power control and proposes that the angle between any two neighboring nodes should be less than or equal to $2\pi/3$ as the constraint to ensure the network connectivity,

and the nodes use lower transmitting power to send data under the premise of the above constraint to simplify the topological connection of the network; secondly, we consider the characteristic that the energy consumption of sensor nodes is proportional to the square of the transmission distance and the plane geometric characteristics of triangle. Secondly, according to the characteristic that energy consumption of sensor nodes is proportional to the square of transmission distance and the plane geometry of triangle, the node distribution area is cut into three parts by drawing auxiliary lines, and different topologies are established by different methods for different areas. The closer areas are connected directly and the more distant areas are connected by multihop method to form an optimized topological connection. Finally, according to the remaining energy of neighboring nodes and the power of sending data, an adaptation function is established, and different neighboring nodes are selected for data transmission by the adaptation function so that the energy consumption of each node is shared to optimize the energy efficiency.

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 research has been financed by the NSFC: research on high efficient video transmission technology based on sparse and low rank decomposition (No. 61671253); general project of Natural Science Research in Universities of Jiangsu Province: research on video transmission technology based on foreground background separation and simultaneous interpreting of information and energy (No. 18kjd510004); Jiangsu Province Education Information Research Project: new interactive education cloud platform design based on the Internet of things, and research on the teaching method of Information turnover in the classroom (No. 20172088); and Jiangsu Province General University Academic Degree Postgraduate scientific research innovation plan project: research on video processing technology based on sparse low rank decomposition and significance detection (No. KYLX16_0661).

References

[1] Z. Liu, T. Tsuda, H. Watanabe, S. Ryuo, and N. Iwasawa, "Data driven cyber-physical system for landslide detection," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 991–1002, 2019.

[2] S. Cai and V. K. N. Lau, "Zero MAC latency sensor networking for cyber-physical systems," *IEEE Transactions on Signal Processing*, vol. 66, no. 14, pp. 3814–3823, 2018.

[3] H. P. Sultana and P. V. Krishna, "Two-level medium access control in cyber physical system-based smart wireless networks," *International Journal of Critical Computer-Based Systems*, vol. 6, no. 3, pp. 191–203, 2016.

[4] K. Xu, W. Ma, L. Zhu et al., "NTC-HARQ: network–turbo-coding based HARQ protocol for wireless broadcasting system," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 10, pp. 4633–4644, 2014.

[5] Y. Liu, Y. Peng, B. Wang, S. Yao, and Z. Liu, "Review on cyber-physical systems," *IEEE/CAA Journal of Automatica Sinica*, vol. 4, no. 1, pp. 27–40, 2017.

[6] P. Padher and V. M. Rohokale, "A cyber-physical system for environmental monitoring," *International Journal Sensor Networks and Data Communications*, vol. 7, no. 2, pp. 154–158, 2018.

[7] H. Wang, H. Zhao, J. Zhang, D. Ma, J. Li, and J. Wei, "Survey on unmanned aerial vehicle networks: a cyber physical system perspective," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1027–1070, 2019.

[8] H. Wang, J. Li, H. Gao, and X. Zheng, "Gateway bandwidth arrangement of data transmission in cyber-physical system," *International Journal of Sensor Networks*, vol. 27, no. 1, pp. 14–25, 2018.

[9] A. Burg, A. Chattopadhyay, and K. Y. Lam, "Wireless communication and security issues for cyber–physical systems and the Internet-of-Things," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 38–60, 2017.

[10] W. W., X. Xia, M. Wozniak, X. Fan, R. Damaševičius, and Y. Li, "Multi-sink distributed power control algorithm for Cyber-physical-systems in coal mine tunnels," *Computer Networks*, vol. 161, pp. 210–219, 2019.

[11] O. Younis and N. Moayeri, "Employing cyber-physical systems: dynamic traffic light control at road intersections," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2286–2296, 2017.

[12] R. Atat, L. Liu, J. Ashdown, M. J. Medley, J. D. Matyjas, and Y. Yi, "A physical layer security scheme for mobile health cyber-physical systems," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 295–309, 2017.

[13] S. Siddiqui, S. Ghani, and A. A. A. D. P.-M. A. C. Khan, "An adaptive and dynamic polling-based MAC protocol for wireless sensor networks," *IEEE Sensors Journal*, vol. 18, no. 2, pp. 860–874, 2017.

[14] S. Bitam, S. Zeadally, and A. Mellouk, "Bio-inspired cybersecurity for wireless sensor networks," *IEEE Communications Magazine*, vol. 54, no. 6, pp. 68–74, 2016.

[15] B. Bordel, R. Alcarria, M. Á Manso-Callejo, and A. Jara, "Building enhanced environmental traceability solutions: from Thing-to-Thing communications to Generalized Cyber-Physical Systems," *Journal of Internet Services and Information Security*, vol. 7, no. 3, pp. 17–33, 2017.

[16] M. Zhan, J. Wu, H. Wen, and P. Zhang, "A novel error correction mechanism for energy-efficient cyber-physical systems in smart building," *IEEE Access*, vol. 6, pp. 39037–39045, 2018.

[17] F. R. Yazdi, M. Hosseinzadeh, and S. Jabbehdari, "A priority-based MAC protocol for energy consumption and delay guaranteed in Wireless Body Area Networks," *Wireless Personal Communications*, vol. 108, no. 3, pp. 1677–1696, 2019.

[18] S. A. Chaudhry, T. Shon, F. Al-Turjman, and M. H. Alsharif, "Correcting design flaws: an improved and cloud assisted key agreement scheme in cyber physical systems," *Computer Communications*, vol. 153, pp. 527–537, 2020.

[19] M. Z. A. Bhuiyan, J. Wu, G. Wang, J. Cao, W. Jiang, and M. Atiquzzaman, "Towards cyber-physical systems design for

structural health monitoring," *ACM Transactions on Cyber-Physical Systems*, vol. 1, no. 4, pp. 1–26, 2017.

[20] P. K. Sahoo and H. K. Thakkar, "TLS: traffic load based scheduling protocol for wireless sensor networks," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 30, no. 3, pp. 150–160, 2019.

[21] J. Zhang, J. Long, C. Zhang, and G. Zhao, "A delay-aware and reliable data aggregation for cyber-physical sensing," *Sensors*, vol. 17, no. 2, p. 395, 2017.

[22] X. Zheng, C. Julien, R. Podorozhny, F. Cassez, and T. Rakotoarivelo, "Efficient and scalable runtime monitoring for cyber–physical system," *IEEE Systems Journal*, vol. 12, no. 2, pp. 1667–1678, 2016.

[23] R. Shakeri, M. A. Al-Garadi, A. Badawy et al., "Design challenges of multi-UAV systems in cyber-physical applications: a comprehensive survey and future directions," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3340–3385, 2019.

[24] S. Liu, G. Huang, J. Gui, T. Wang, and X. Li, "Energy-aware MAC protocol for data differentiated services in sensor-cloud computing," *Journal of Cloud Computing*, vol. 9, no. 1, pp. 1–33, 2020.

[25] I. Henao-Hernández, E. L. Solano-Charris, A. Muñoz-Villamizar, J. Santos, and R. Henríquez-Machado, "Control and monitoring for sustainable manufacturing in the Industry 4.0: a literature review," *IFAC-PapersOnLine*, vol. 52, no. 10, pp. 195–200, 2019.

[26] G. Park and H. K. Park, "Design of QoS based MAC protocol considering data urgency for Energy harvesting wireless sensor networks," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 23, no. 8, pp. 1004–1010, 2019.

[27] S. Li, Q. Ni, Y. Sun, G. Min, and S. Al-Rubaye, "Energy-efficient resource allocation for industrial cyber-physical IoT systems in 5G era," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2618–2628, 2018.

[28] G. S. Dhunna and I. Al-Anbagi, "A low power WSNs attack detection and isolation mechanism for critical smart Grid applications," *IEEE Sensors Journal*, vol. 19, no. 13, pp. 5315–5324, 2019.

[29] M. L. Wymore and D. Qiao, "An opportunistic MAC protocol for energy-efficient wireless communication in a dynamic, cyclical channel," *IEEE Transactions on Green Communications and Networking*, vol. 2, no. 2, pp. 533–544, 2018.

[30] H. Wang, G. Zhou, L. Bhatia, Z. Zhu, W. Li, and J. A. McCann, "Energy-neutral and QoS-aware protocol in wireless sensor networks for health monitoring of hoisting systems," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5543–5553, 2020.

[31] S. Kartakis, A. Fu, M. Mazo, and J. A. McCann, "Communication schemes for centralized and decentralized event-triggered control systems," *IEEE Transactions on Control Systems Technology*, vol. 26, no. 6, pp. 2035–2048, 2017.

[32] L. Lyu, C. Chen, J. Yan, F. Lin, C. Hua, and X. Guan, "State estimation oriented wireless transmission for ubiquitous monitoring in industrial cyber-physical systems," *IEEE Transactions on Emerging Topics in Computing*, vol. 7, no. 1, pp. 187–201, 2016.