Eng Int Syst (2025) 5: 485–498

Engineering
Intelligent Systems

Remote Monitoring System Based on the Internet of Things and Monitoring Method for Design of Construction Machinery

Luyue Han[1]*, Liyan Gao[1], Songshan Feng[2], Fengzhen Qu[3] and Bowen Song[3]

[1] *Architectural Engineering Institute, Binzhou Polytechnic, Binzhou 256603, Shandong, China*
[2] *Department of Building Economic Management, Shandong Urban Construction Vocational College, Jinan 250103, Shandong, China*
[3] *Mechanical and Electrical Engineering Institute, Binzhou Polytechnic, Binzhou 256603, Shandong, China*

The monitoring of construction machinery is a major safety issue, and the prevention of accidents is something that concerns anyone responsible for the security of construction machinery. How to establish a safe, reliable, stable and scalable monitoring system for construction machinery is a crucial issue. In recent years, as the concept of the Internet of Things (IoT) has gradually been applied to remote monitoring technology, an increasing number of applications have emerged for the remote monitoring of construction machinery, making it a key research direction. Remote monitoring can be considered as either "monitoring" or "control". Of these, "monitoring" is remote monitoring, which can be the monitoring of the environment or the monitoring of the computer system and the network devices. To address the issue of construction machinery safety, this current study used the IoT positioning algorithm to determine the impact that remote monitoring systems have on safety in the construction of a large-scale building safety and, so that the relationship between remote monitoring and construction machinery design. Typically, the positioning algorithm uses various information sources, such as visible light sources, infrared sources, microwave sources, and landform fluctuations to produce images. Experimental results indicated that in normal environments, the parameters of payload, security processing, load density and transmission scheduling were improved. The RTT value of data transmission was tested and analyzed on UDP and SMS channels. Factors such as channel delay, security encapsulation, data compression, channel type and queue parameters were analyzed. The validity, reliability and safety of the remote monitoring system for large-scale building monitoring were verified, indicating that the remote monitoring system and monitoring method using the Internet of Things can be applied to, and improved, the design of construction machinery.

Keywords: construction machinery, Internet of Things (IoT), remote monitoring system, monitoring method, positioning algorithm

1. INTRODUCTION

With the continuous development of the world economy, the building industry is booming with the construction of new factories, warehouses, office buildings, etc. However, this has given rise to security issues. Traditional security measures involved manual inspections, consuming significant manpower and material resources while jeopardizing the safety of security personnel. These measures were not only inefficient and ineffective but also failed to provide comprehensive protection.

Nowadays, the rapid progress of technology has led to the emergence of advanced safety monitoring systems. These systems integrate network, sensing, image, and digital compression technologies, greatly improving the efficiency and accuracy of monitoring. On-site video and sound data are captured by multiple sensors and transmitted to the monitoring center, enabling real-time monitoring by security personnel. This provides an overview of the entire monitored area.

*Corresponding Author. Emails: HLY19880612@126.com, gaolunwen67075241@126.com, 705522978@qq.com, 83532851@qq.com, 810161874@qq.com

If any abnormal data is detected, it is promptly addressed to minimize monetary and property losses.

This study aimed to investigate the impact of a remote monitoring system on the safety of large-scale buildings. The relationship between the two was analyzed through field testing of the remote monitoring system operating on the Z bridge. The IoT positioning algorithm was used to verify the suitability of the remote monitoring system for large buildings and to demonstrate its potential to improve the design of construction machinery.

2. RELATED WORK

Wu et al. proposes Blockchain-assisted Cohesive Authentication using Attribute-Based Encryption Scheme (BCA-ABES) for dynamic control of access to big data stored in the cloud [1]. Zhang designed and implemented a remote monitoring system combined with the Internet of Things to monitor suppliers' papermaking equipment in different regions [2]. The remote monitoring system designed by Li could timely and effectively convey information about the direct current (DC) power supply system of a substation to the APP users [3]. To further develop greenhouse environmental monitoring technology, Cai designed and implemented a remote monitoring system for greenhouses with WinCE as the core component [4]. Wang and Ye design a set of cross-domain business management solutions, unified modeling, unified identification and unified representation, thus enhancing the scalability of applications [5]. Although these studies have contributed to theoretical knowledge, they have not been tested scientifically and empirically to determine the effectiveness of remote monitoring systems in other areas.

To construct a monitoring system based on the IoT, this current study utilized the IoT positioning algorithm, which has been widely applied in other researches. Wang proposed a novel 5G smart IoT for processing big data and optimizing communication channels [6]. Chen proposed an adaptive and scalable trust management approach to support service composition applications in SOA-based IoT systems [7]. Broring used five interoperability patterns to design a successful IoT-based ecosystem architecture that enabled cross-platform interoperability [8]. Gharbieh developed a traffic-aware spatiotemporal mathematical model to characterize the scalability of cellular up-links in an IoT network environment [9]. Farahani's research found the applicability of IoT in healthcare and medicine using the overall architecture of the IoT e-health ecosystem [10]. The aforementioned researches were all concerned with the application of IoT and provide the rationale for the application of the positioning algorithm of the IoT in the design of construction machinery.

3. CONSTRUCTION MACHINERY DESIGN AND INTERNET OF THINGS CONSTITUTION

3.1 Construction Machinery Design

The machinery construction industry provides technical equipment for various engineering projects. The construction industry plays a pivotal role in the development of the national economy and the construction of various infrastructures. As far as construction machinery is concerned, they have certain commonalities, which provide technical equipment for civil engineering, road and bridge, mining, and other engineering projects. In recent years, with the development of the market economy, the competitiveness of enterprises has accelerated the research and development of new products and the renewal of old products [11–12]. China's construction machinery has made great progress in terms of design, leading to the development and manufacture of a large number of cost-effective building materials. Each specific industry requires different types of machinery suitable for different applications. Also, with the continuous development of China's market economy and computer technology sector, construction machinery companies have gradually realized the importance of informatization [13].

3.2 IoT Algorithms

The "things" in the Internet of Things are very broad, and can be a mobile phone, a car, a ship, a deployed wireless sensor device, or even a person. The technologies used to obtain the location information of nodes in the Internet of Things are collectively referred to as "positioning technologies". Due to the large number of unknown nodes in the Internet of Things, it is not feasible to install a GPS on each node for positioning. Therefore, it is necessary to use a small number of nodes with known positions and some known metrics (such as distance, angle, etc.) to calculate and estimate the positions of unknown nodes through algorithms. These algorithms are called "localization algorithms", and nodes whose positions are known are called "anchor nodes". In this current study, the technology used to measure the distance between nodes and the commonly used positioning algorithm are examined [14].

(1) Performance evaluation standard of positioning algorithm

The performance of the IoT positioning algorithm needs to have certain evaluation indicators. The commonly used evaluation indicators are given below:

The ultimate goal of positioning accuracy (or positioning error) is precision. The goal of the positioning algorithm design is to achieve the highest positioning accuracy at the lowest possible cost [15]. The positioning accuracy is defined as the size of the error between the true value and the estimated value of the unknown node position. This is generally measured by metrics such as Root Mean Square Error (RMSE) or Mean Square Error (MSE).

1) Anchor node rate

   The anchor node rate is the ratio of the number of anchor nodes to the total number of nodes. The more anchor nodes in the IoT node location, the more precisely can the node be located. However, the location information of anchor nodes is generally obtained through two methods: one is manual deployment, which is a complicated procedure that is greatly affected by the environment; the other is to achieve positioning through GPS, which would greatly increase the cost. Therefore, the design goal of the algorithm is to achieve better positioning accuracy at the lowest anchor node rate [16].

2) Node density

In general, the higher the node density in IoT positioning, the higher the positioning accuracy. However, if the node density is increased blindly, the cost would increase and the amount of communication data between nodes would also increase, which could lead to network congestion. Therefore, in the application, the node density should not exceed the actual need [17].

3) Power consumption

In IoT positioning, nodes need to communicate, calculate, store, etc., which consumes a large amount of energy. The energy of the node is efficient but the service life would be reduced if there is high power consumption. Once a node fails due to energy exhaustion, the communication between nodes and the accuracy of positioning is affected. Therefore, it is necessary to reduce the power consumption as much as possible while ensuring the positioning accuracy [18].

4) Fault tolerance and adaptability

The application environment of the Internet of Things is complex and diverse, and the climate is changing. IoT nodes would fail in harsh environments, and it is difficult to repair or replace the failed nodes. Therefore, the localization algorithm needs to have good adaptability and fault tolerance [19].

(2) Classification of positioning algorithms

The positioning algorithms in the Internet of Things can be divided into the following categories according to different classification methods:

1) Absolute positioning and relative positioning

Absolute positioning obtains the physical position of a node without a reference object, while relative positioning generally selects several nodes as a reference, constructs a relative coordinate system, and calculates the relative coordinates of the nodes [20]. The advantage of absolute positioning is that it does not require nodes as references. The movement of the node has little influence on the positioning result, so it has a wide range of applications. However, relative positioning does not require anchor nodes, and some routing protocols such as geographic location-based routing can also be implemented in this way.

2) Distributed computing positioning and centralized computing positioning

Distributed computing is a positioning method that estimates the location of each node through information transfer between nodes; centralized computing transmits the required information to the sink node and calculates the node position in the sink node. The advantage of distributed computing positioning is that it reduces the communication overhead because the calculation of node location is done locally at the node without sending information to the sink node.In centralized computing and positioning, nodes near the sink node may experience higher energy consumption due to increased communication overhead. If the energy of these nodes is depleted and they fail, it could disrupt the communication between those nodes and the sink node, potentially affecting the overall positioning accuracy. However, centralized computing also has the advantage of being able to obtain more accurate node position estimation and can also exercise control macroscopically.

3) Positioning based on anchor nodes and positioning without anchor nodes

The anchor node-based positioning algorithm requires certain nodes to obtain their own location information through GPS or other methods. These anchor nodes then broadcast their location information to other unknown nodes within the communication range. As long as the unknown node obtains information about the position of three or more anchor nodes, the positioning algorithm can be used to locate the unknown node. The positioning accuracy of the anchor node-based localization algorithm depends on the number of anchor nodes, the anchor node rate and its distribution in the application environment. In addition, when the number of anchor nodes is large, information loss and network congestion may appear or increase, so the scalability of the anchor node-based positioning algorithm is poor. The positioning algorithm without anchor nodes only needs to know the relative positions of the nodes and modify the positioning results by means of coordinate transformation. However, when the nodes move, the relative positions between the nodes will change, which increases the amount of computation. Therefore, the positioning algorithm without an anchor node is not suitable when there is node movement.

4) Positioning based on ranging and without ranging technology

The use of range-based positioning requires measuring the absolute distance or angle between nodes. And according to the actual distance between the nodes, trilateration, trigonometry and other ranging-based positioning methods are used to determine the position of the nodes. Range-free technology locates unknown nodes by calculating the distance of nodes without measuring the angle and distance between nodes. Although the range-based positioning algorithm has high positioning accuracy, it imposes high requirements on the hardware of the node. Although the range-free positioning algorithm has low requirements on node hardware, its positioning accuracy also decreases.

(3) Ranging technology between nodes

The positioning algorithm based on ranging technology is used to measure the angle or distance information between nodes. The commonly-used ranging technologies are AOA, RSSI, TOA and TDOA.

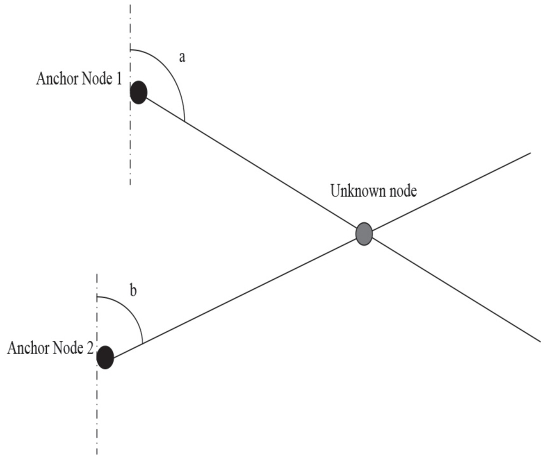


Figure 1 Schematic diagram of AOA positioning technology.

1) Ranging technology based on Angle of Arrival (AOA)

AOA ranging technology uses the angle of arrival to calculate the position of the unknown node. It is the arrival direction (incidence angle of radio wave) of the transmission path of the received signal from the unknown node to more than two anchor nodes measured by the receiver through the array antenna, and the position information of the unknown node is calculated based on this. AOA positioning technology can draw a line from the anchor node to the unknown node according to the measured signal direction angle between the unknown node and the anchor node, where the intersection of the two lines is the location of the unknown node. Therefore, the location of the unknown node can be obtained by the AOA measurement of the two anchor nodes. Usually, more than two anchor nodes are selected during positioning to prevent the unknown node's collinearity with the two anchor nodes, which leads to the AOA measurement being unable to determine the coordinates of the unknown node, as shown in Figure 1:

The coordinates of anchor node 1 are set to (m, n), and anchor node 2 is $(m_2,\ n_2)$; the direction angles of the signals they received are a and b, respectively. Then the coordinates (m, n) of the unknown node can be calculated with:

$$m = -\frac{(n_2 - m_2 \tan b) - (n_1 - m_1 \tan a)}{\tan b - \tan a}; \quad n = -\frac{(m_2 - n_2 \cot b) - (m_1 - n_1 \cot a)}{\cot b - \cot a} \tag{1}$$

The positioning accuracy of this method is affected by the anchor node location, non-line-of-sight, multipath propagation and other factors. When there is a great distance between the unknown node and the anchor node, the slight deviation of the signal direction angle causes a large positioning error. When in non-line-of-sight conditions, the positioning error increases due to reflection or scattering. Therefore, AOA technology is not suitable for the environment localization of non-line-of-sight paths.

2) Ranging technology based on Received Signal Strength Indicator (RSSI)

The RSSI ranging method is used to measure the power of the received signal. On the premise that the power of the transmitted signal is known, the propagation loss of the signal is converted into distance through the known signal fading model, and the coordinates of the unknown node are calculated according to the estimated distance between multiple nodes. The formula for the signal fading model is:

$$Q(f) = Q(f_0) - 10x \log\left(\frac{f}{f_0}\right) - \begin{cases} x_e \times E_{SG}, x_e < V \\ V \times E_{SG}, x_e \geq V \end{cases} \tag{2}$$

where Q(f) is the signal strength actually measured, and $Q(f_0)$ is the signal strength at the reference distance f_0. x is the decay index, which is related to the structure of the building and the materials used. The typical value is: general building $x = 2.766$, office building $x = 3.25$, shopping mall $x = 2.18$. x_e is the number of walls between the anchor node and the unknown node; V represents the threshold for the signal to pass through the wall; E_{SG} is the attenuation factor for the signal to pass through the wall or obstacle. The key to this method is to choose a signal attenuation model that is consistent with the actual environment. The complexity of the real environment raises certain difficulties in terms of modeling. There is a large distance measurement error, and the positioning accuracy is not high.

3) Ranging technology based on Time of Arrival (TOA)

The TOA ranging positioning method is a positioning technology based on signal transmission time, as shown in Figure 2:

As shown in the figure, it is assumed that the time when anchor node 1 sends the signal to the unknown node is t_1, and the time when the unknown node receives the signal is t_2, the time when the unknown node sends the signal back to the anchor node 1 after processing is t_3. The time when anchor node 1 receives the signal is t_4, then the distance between anchor node 1 and the unknown node is:

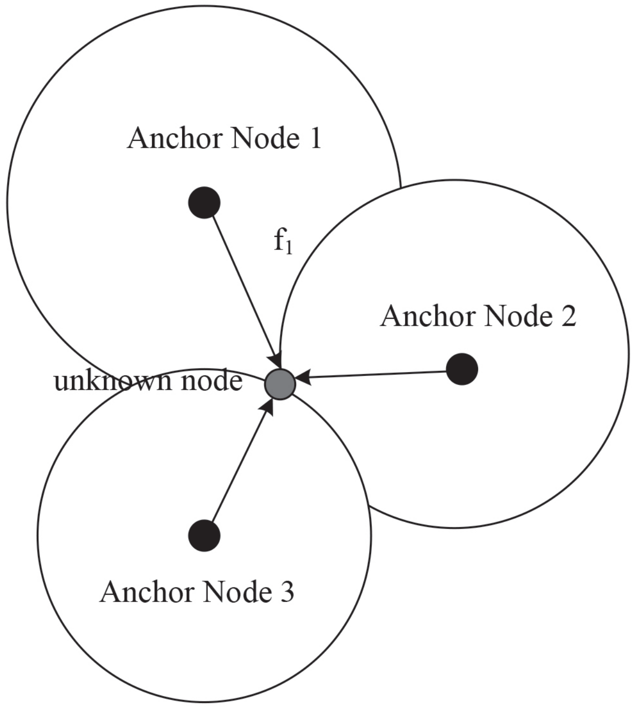


Figure 2 Schematic diagram of TOA positioning technology.

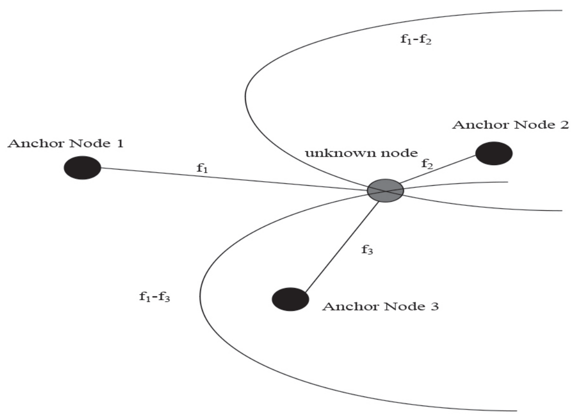


Figure 3 Schematic diagram of TDOA positioning technology.

$$f_1 = \frac{[(t_2 - t_1) + (t_4 - t_3)] \times e}{2} \tag{3}$$

where e is the propagation speed of the signal. TOA positioning technology has higher positioning accuracy and is generally better than AOA technology, but it requires time synchronization between unknown nodes and anchor nodes.

4) Ranging technology based on Time Difference of Arrival (TDOA)

TDOA ranging technology is a new positioning technology based on the time difference between signal transmissions from an unknown node to three anchor points, which gives the distance between each node. The existing localization algorithm is used for localization, as shown in Figure 3:

TDOA positioning technology can achieve higher positioning accuracy, but requires additional hardware such as acoustic wave transceivers on nodes, which increases the cost of nodes and is greatly affected by multipath interference.

(4) Typical positioning algorithm

In the Internet of Things, many localization algorithms have been proposed and widely used. This present study investigates several typical localization algorithms.

1) Trilateration method

Trilateration is a more commonly used ranging-based positioning algorithm. As long as the distance from the unknown node to the three anchor nodes is known and the mathematical formulas are established and solved, the coordinates of the unknown node can be obtained, as shown in Figure 4:

As shown in the figure, the coordinates of the unknown node are set to (m, n), and the coordinates of the

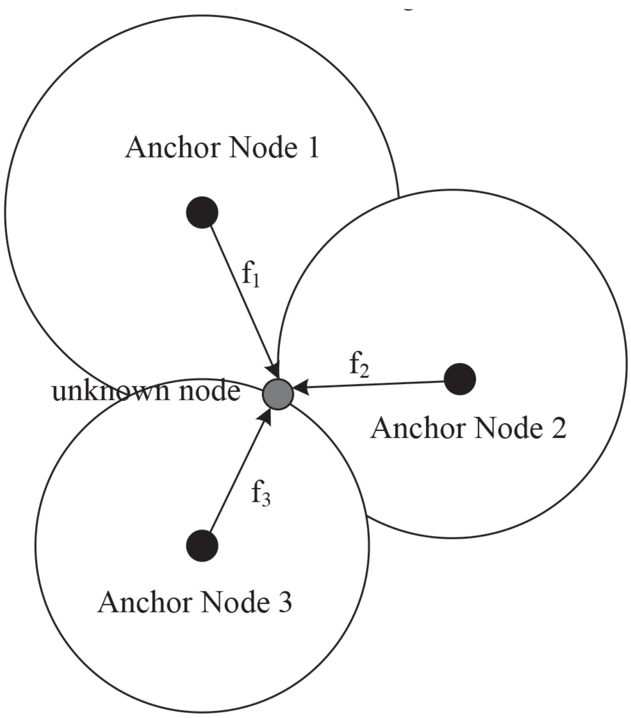


Figure 4 Schematic diagram of trilateration method positioning.

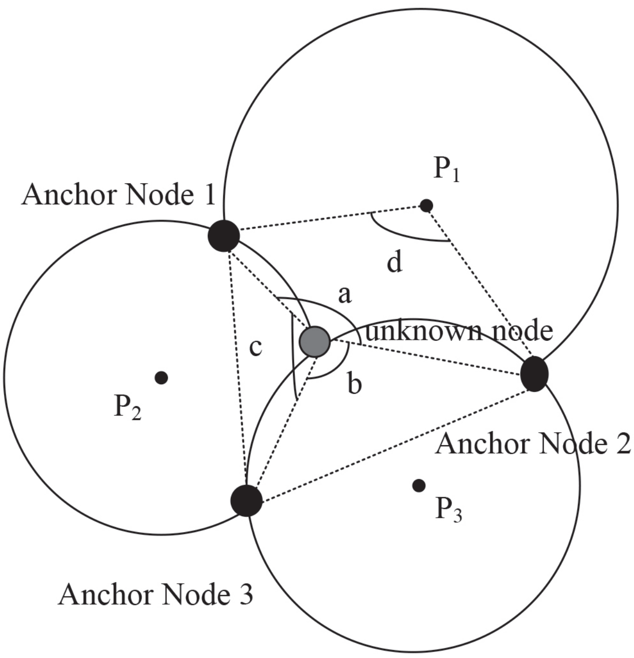


Figure 5 Schematic diagram of triangulation method positioning.

three anchor nodes are (m_1, n_1), (m_2, n_2), (m_3, n_3). f_1, f_2, and f_3 respectively represent the distance from the unknown node to the corresponding anchor node; the formulas are as follows:

$$f_1 = \sqrt{(m - m_1)^2 + (n - n_1)^2} \tag{4}$$

$$f_2 = \sqrt{(m - m_2)^2 + (n - n_2)^2} \tag{5}$$

$$f_3 = \sqrt{(m - m_3)^2 + (n - n_3)^2} \tag{6}$$

The coordinates of the unknown node can be obtained with:

$$\begin{bmatrix} m \\ n \end{bmatrix} = \begin{bmatrix} 2(m_1 - m_2)2(n_1 - n_2) \\ 2(m_2 - m_3)2(n_2 - n_3) \end{bmatrix}^{-1} \times \begin{bmatrix} f_2^2 - f_1^2 + m_1^2 + n_1^2 - m_2^2 - n_2^2 \\ f_3^3 - f_2^2 + m_2^2 + n_2^2 - m_3^2 - n_3^2 \end{bmatrix} \tag{7}$$

2) Triangulation

The triangulation method locates the unknown node according to the angle information between the unknown node and the three anchor nodes, as shown in Figure 5:

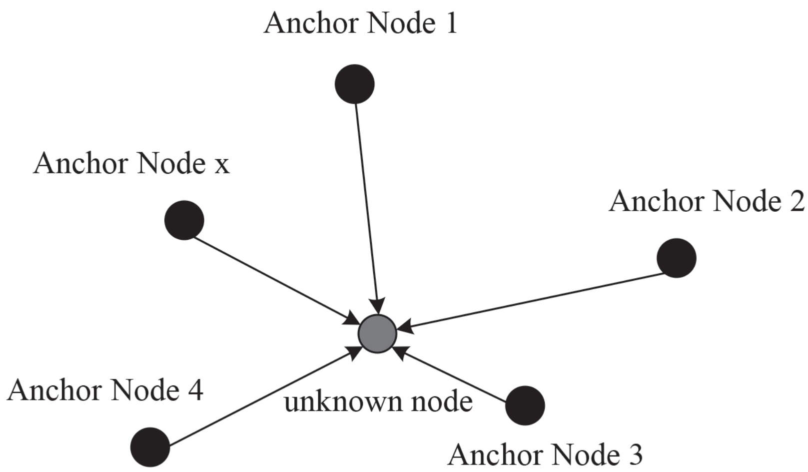


Figure 6 Schematic diagram of maximum likelihood estimation.

As shown in Figure 5, $(m_1,\ n_1)$, $(m_2,\ n_2)$, $(m_3,\ n_3)$ are the coordinates of the anchor nodes. The coordinates of the unknown node 1 is (m, n) and their angles are a, b, and c, respectively. If the arc formed by anchor node 1 and the unknown node as well as anchor node 2 is located in a triangle, then with three anchor nodes as vertices, a circle can be determined by a. The coordinates of the center P_1 is $(j_1,\ k_1)$ and the radius is r_1, then d $= 2\pi - 2$a and the formulas are:

$$r_1 = \sqrt{(m_1 - j_1)^2 + (n_1 - k_1)^2} \tag{8}$$

$$r_1 = \sqrt{(m_2 - j_2)^2 + (n_2 - k_2)^2} \tag{9}$$

$$(m_1 - m_2)^2 + (n_1 - n_2)^2 = 2r_1 - 2r_1^2 \cos d \tag{10}$$

The coordinates $(j_1,\ k_1)$ of the center P_1 and the radius r_1 can be obtained by solving. Similarly, according to b and c, the coordinates $(j_2,\ k_2)$, $(j_3,\ k_3)$ and the radii r_2, r_3 of the circle center P_2, P_3 can be obtained from the formulas, respectively. Finally, the coordinates of the unknown nodes can be solved.

3) Maximum likelihood estimation method

The location algorithm based on ranging needs to measure the distance between nodes, which can result in measurement errors. Therefore, when applying the trilateration method, the three circles do not intersect at one point, making the unknown node unable to be located. However, the maximum likelihood estimation method can solve this problem well, as shown in Figure 6:

As shown in Figure 6, $(m_1,\ n_1)$, $(m_2,\ n_2)$, $(m_3,\ n_3), \ldots, (m_x,\ n_x)$ represent the coordinates of x anchor nodes in turn. The coordinates of the unknown nodes are represented by $(m,\ n)$, and the distances between them are $f_1, f_2, f_3, \ldots, f_x$, respectively, then the formula system can be listed:

$$(m_1 - m)^2 + (n_1 - n)^2 = f_1^2 \tag{11}$$

$$(m_x - m)^2 + (n_x - n)^2 = f_x^2 \tag{12}$$

The first $x - 1$ term of the system of formulas are used to subtract the x-th term, and the following formulas are obtained:

$$m_1^2 - m_x^2 - 2(m_1 - m_x)\Big|m + n_1^2 - n_x^2 - 2(n_1 - n_x)n = f_1^2 - f_x^2 \tag{13}$$

$$m_{x-1}^2 - m_x^2 - 2(m_{x-1} - m_x)\Big|m + n_{x-1}^2 - n_x^2 - 2(n_{x-1} - n_x)n = f_{x-1}^2 - f_x^2 \tag{14}$$

It can be expressed as

$$SM = y \tag{15}$$

By using the least squares method, the coordinates of point D can be obtained as:

$$\hat{M} = (S^T S)^{-1} S^T y\circ \tag{16}$$

(5) Positioning algorithm without ranging

1) Centroid positioning algorithm

The centroid positioning algorithm (centroid) does not need ranging, it relies on the connectivity between the unknown node and the anchor node to regard the coordinates of the unknown node as the centroid of the polygon formed by all the anchor nodes connected to the unknown node, and the specific steps of the algorithm are:

$$t = (x + 1 - V) \times T \tag{17}$$

Among them, x is the number of signals to be sent within t time, T is the time interval of signal transmission, and V is a constant $(0 < V < 1)$. During the time t, the anchor node sends a broadcast signal containing its location information and Identity (ID) number to the unknown node every interval time T.

The percentage of successful communications between nodes is calculated, and the number of anchor node signals received by the unknown node is recorded, and the success rate of communication with each anchor node is calculated:

$$D = \frac{X_{recv}}{X_{sent}} \times 100\% \tag{18}$$

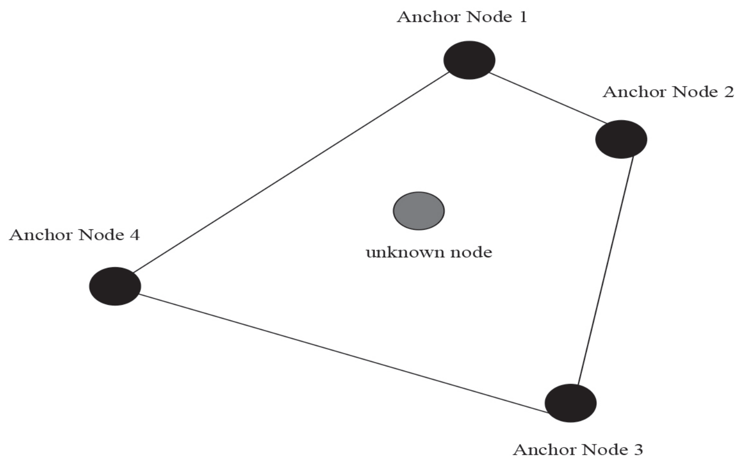


Figure 7 Schematic diagram of centroid algorithm.

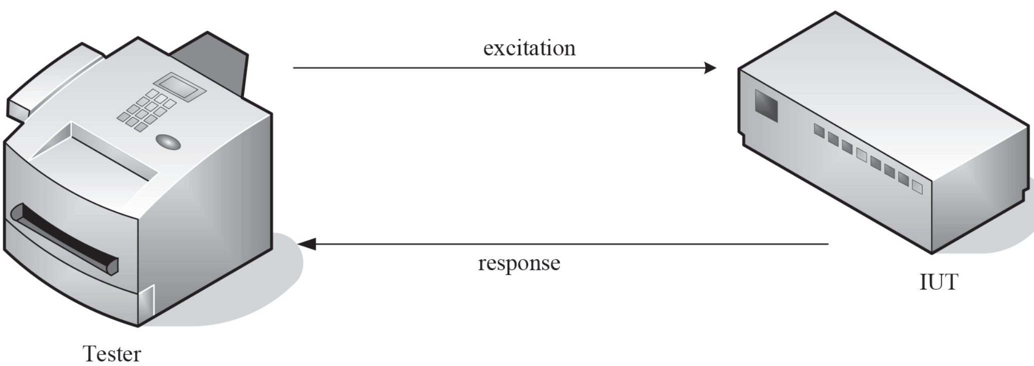


Figure 8 Conformance test topology.

where X_{recv} represents the number of anchor node signals received by the unknown node, and X_{sent} represents the total number of signals sent by the anchor node.

2) Locating unknown nodes

When the unknown node selects an anchor node with a higher communication success rate D (typically 90%) than a predetermined threshold, the coordinate of the unknown node is the geometric center of the polygon formed by these anchor nodes, known as the "centroid" in geometry, as shown in Figure 7:

$(m_1,\ n_1)$, $(m_2,\ n_2)$, $(m_3,\ n_3)$, $(m_4,\ n_4)$ represent the coordinates of the four points, and the unknown node $(m,\ n)$ is represented as:

$$(m, n) = \left(\frac{m_1 + m_2 + m_3 + m_4}{4}, \frac{n_1 + n_2 + n_3 + n_4}{4}\right) \tag{19}$$

This paper briefly explains the principle of the IoT positioning algorithm. The performance evaluation index and classification of localization algorithms are summarized, and the distance measurement technology between nodes is analyzed. Moreover, the working principles and characteristics of several typical distance-based and non-distance-based location methods are given.

4. TEST OF LARGE-SCALE BUILDING STRUCTURE SAFETY REMOTE MONITORING SYSTEM

4.1 Conformance Testing and Interoperability Testing

(1) Conformance test

A series of test instances are generally used to determine whether the Implementation under Test (IUT) meets the standard requirements. A black box test is carried out on the implementation being tested in a specific network environment. According to the similarities and differences between the actual output and the expected output of the IUT, it is determined whether the IUT conforms to the description of the protocol. The test topology is shown in Figure 8:

(2) Interoperability test

An interoperability test is used in the research and development stage to determine whether the implementation being tested and the connected similar implementation can interact correctly in the network operating environment and complete the functions specified in the protocol standard, and then assess whether the device being tested supports the required functions. For the interoperability test, the most common method is to select the interoperability-certified device and

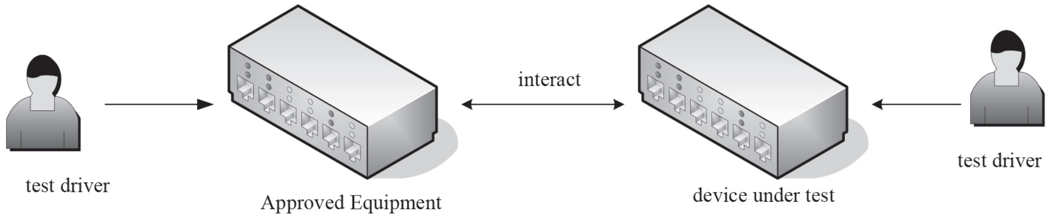


Figure 9 Interoperability test topology.

Table 1 System white-box testing (part).

	JUnit	Test content	Test Results
1	TestCRC	CRC check test	PASS
2	TestGeneratekey	key generation test	PASS
3	TestTimer	timer test	PASS
4	TestCommHandler	Communication interface layer test	PASS
5	UDPServer	UDP receive test	PASS
6	SMSRCV	SMS reception test	PASS
7	TestZip	Compression and decompression tests	PASS

the device being tested by the test unit. The authentication device may be a terminal device, network device, application software, single device or combination of multiple devices. The adopted test topology is shown in Figure 9:

4.2 Protocol Function Test

(1) Development and testing environment

The mixed-communication protocol discussed in this paper achieves the exchange function of mixed data of SOCKET class taking UDP as an example, and MESSAGE class taking SMS as an example. Development is carried out in the WINDOWS2000SERVER environment. The JAVA development environment is J2SDK6.0 and Eclipse3.3 is used as the development integrated environment. Java has the characteristics of simplicity, object orientation, distribution, robustness, security, platform independence and portability, multithreading, and dynamism.

(2) White-box testing

JUnit is a regression testing framework that belongs to white-box testing. JUnit is designed to be very small, but the function is very powerful. During the development of the mixed communication protocol, a large number of JUnits is used for testing to ensure the correct operation of each unit, which reduces the difficulty of black-box testing to identify errors after the system is completed, and ensures the correct advancement of RUP.

This paper uses JUnit to test the key classes and components of the protocol software. The results are shown in Table 1:

(3) Black box testing

Consistency and interoperability are the basic elements determined by the testing. The actual needs of the remote monitoring of large-scale building structure security are considered, and the transparency and openness of the tested protocol are taken into account. The experimental test results confirm the correctness of the protocol development and implementation. The test results are shown in Table 2:

(4) Failure simulation test

At the end of the protocol function test, a set of failure simulation tests are carried out to test the robustness, reliability and security of the hybrid communication protocol.

The correctness of the software implementation of the mixed communication protocol are indicated by the results given in Table 3.

4.3 Protocol Performance Test Evaluation

In this paper, a series of reliability data transmission use cases are made under UDP and SMS channels, and the RTT time from when the function application layer initiates data to when it receives an acknowledgement is tested. Also, the test results indicate the various factors that affect RTT.

Without any security processing, 10 bytes of functional application data payload needs to add 4bytes of functional application layer header, 1 byte of data exchange layer header and 20 bytes of communication interface layer header, which is a total of 35 bytes. In the case of security processing, the communication interface layer needs to add 64 bytes of security digest, and the encrypted data part should be filled to an integer multiple of 8 bytes.

(1) Test and analysis of the impact of data load on RTT

This current study tested the effect of SMS and UDP channel data load on performance respectively. The results are shown in Figure 10:

As shown in Figure 10(A), when the data load transmitted in a single SMS channel gradually increases from 10 bytes to 80 bytes, the RTT gradually increases from about 25 seconds to about 31 seconds. In order to avoid the influence of security processing, no security processing is done in this test case.

Table 2 System black box test (part).

	Test items	Test content	channel	Test Results
1	TestMOrder	Monitoring command transmission test (128bytes ASC sample data)	UDP SMS	PASS PASS
2	TestMMap	Monitoring electronic map transmission test (18kbytes BIN sample data)	UDP SMS	PASS PASS
3	TestMData	Monitoring data transfer tests (240bytes ASC sample data)	UDP SMS	PASS PASS
4	TestMAlert	Monitoring Threshold Alarm Test (90bytes ASC sample data)	UDP SMS	PASS PASS
5	TestSTime	Monitoring point time synchronization test (20bytes ASC sample data)	UDP SMS	PASS PASS
6	TestSAlert	Monitoring point security abnormal alarm test (20bytes ASC sample data)	UDP SMS	PASS PASS

Table 3 System failure simulation test (part).

	Test items	Test content	Test Performance	Test Results
1	TestFCRC	Simulate send: bad CRC	CRC error detected, discarded Fragmentation	PASS
2	TestFENC	Simulated packet sending: wrong encryption	Error encryption detected, send MAlert, discard data	PASS
3	TestFZIP	Simulate packet sending: wrong compression	Error compression detected, sendMAlert, discard data	PASS
4	TestFSMS1	Open SMS after manual close	SMS Status Detection Restoration	PASS
5	TestFKEY	inconsistent symmetric key group	Error encryption detected, send MAlert, discard data	PASS

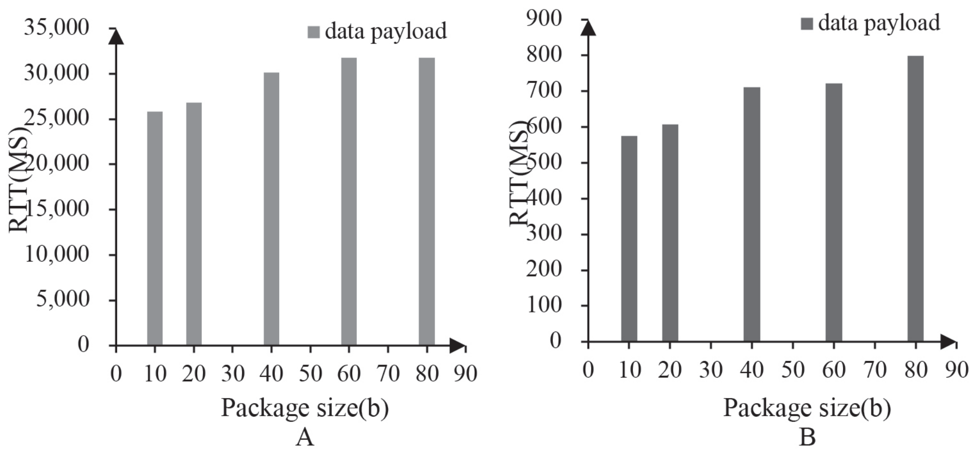


Figure 10 Effect of SMS(A) and UDP(B) channel data load on performance.

Only 80 bytes of payload was measured in this set of tests. This is because when the header of each layer is added, it reaches 105 bytes and then it becomes 140 bytes after Base64 encoding. The maximum message that can be carried in the PDU mode of SMS is 140 bytes of double-byte data or 160 bytes of single-byte data. There is a big difference in the size of the data packets that need to be transmitted in the safety remote monitoring of large buildings, and the RTT is proportional to the size of the data payload sent.

As shown in Figure 10(B), when data packets of different sizes are transmitted under a single UDP, the RTT time also increases proportionally with the packet load without any security processing. At the same time, it can be seen that the overall RTT delay of the UDP channel is much smaller than the RTT delay of the SMS channel, which can be at least an order of magnitude difference.

(2) Test and analysis of the impact of security processing on RTT

By configuring different security parameters in UDP and SMS channels, the RTT time from when the function application layer initiates data to when it receives confirmation was tested. It was found that the RTT is significantly increased after encrypting and digesting the sent data. The results are shown in Figure 11:

As shown in Figure 11A, the test was performed under a single UDP channel. By testing the packets with five data payload sizes of 18bytes, 280bytes, 1120bytes, 1513bytes and

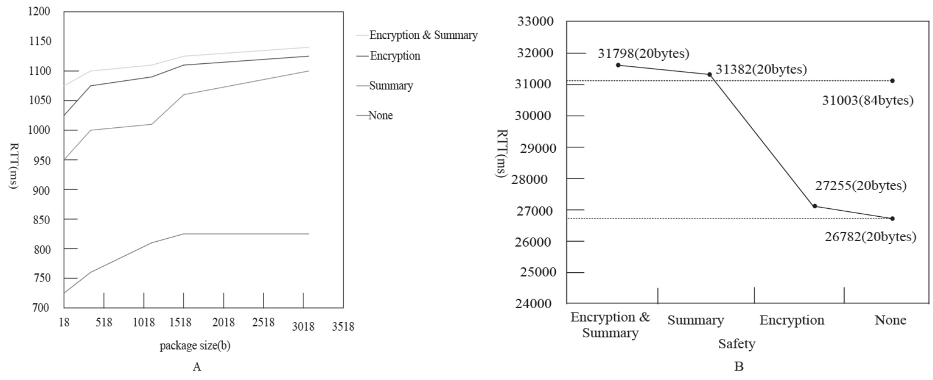


Figure 11 Impact of UDP(A), SMS(B) channel security design on performance.

3085bytes, four different channel security configuration use cases were compared in the packet: encryption and digest, encryption only, digest only, and no encryption and no digest. It was found that the change of RIT with the size of the packet payload is not obvious: the time consumption of single-action digest and encryption in security processing is basically the same. Compared with no security processing, the RIT delay needs to be increased, and the case where both digest and encryption are performed is slightly more time-consuming than the case where only one is performed.

As shown in Figure 11B, the same size of payload (20 bytes) is transmitted on the SMS channel, and it was found that the security processing has a significant impact on the RIT delay. Data encryption and digests increased by 1.7% and 17% respectively compared with those without any processing, while there was an increase of about 17.2% when both digests and encryptions were performed. However, it was found that, compared with UDP data transmission, the increased delay of encryption and digest processing is less than 500ms, which should not cause such a big gap.

After the security processing, 64 bytes of security data digest and encrypted padding should be added, and the actual fragment size sent for the 20 bytes payload increases from 45 bytes to 116 bytes. The increase in the amount of data also significantly affects the RTT, which can be seen from the comparison curve shown in the figure. At the same time, the actual fragment size increases to 109 bytes after only the security digest is processed for the 20-bytes payload, and the fragment size also increases to 109 bytes when the 84 bytes payload does not perform any security processing. Therefore, when comparing it with the 20 bytes payload in the case of only security digest processing, the RTT should be similar and the RTT time of the former is slightly smaller.

4.4 Application Practice of Remote Monitoring

(1) Engineering background

The Z bridge is located at the estuary between C and D mountains in N town. The engineering design of the bridge is novel and with a great amount of the technical content since it is a double-cable plane prestressed concrete single-pylon cable-stayed bridge with a cooperative system. There are 102 stay cables on the four cable planes on the upstream and downstream, east and west sides. The standard section of the box girder is a double-box single-chamber open box section, and the inclined tower column is a vase shape, which is the first of its kind in China.

The main task of the remote monitoring of the structural safety of the Z bridge is to identify strain and cracks in the key parts of the bridge's main girder. Hence, the wind loads, strains of main beams and stay cables, vibrations of piers and boxes, deck deformation and temperature, are measured and monitored. Furthermore, the structural safety evaluation and analysis system of the bridge is established, and the static and dynamic strain signal and crack propagation signal of the structure are analyzed by a computer. Also, the health status of the structure is analyzed through the structural safety evaluation system for the regular compilation and submission of monitoring reports.

(2) Operation status

The monitoring and analysis software of this system was also developed and implemented in Java language, which can conveniently call the function of the hybrid communication protocol stack to send and receive data. The functional application layer of the hybrid communication protocol described in this paper adds the following modules to the original basic functions:

1) System function module

   System initialization and identity authentication, acquisition of encryption parameters for data transmission, and software version update are completed.

2) Data acquisition module

   External processing is used to extract all the spectral data from the fiber bragg grating demodulator. The acquisition client can use the #GETDATA command to collect the sensor data of each channel through the SOCKET interface. By using the step value according to the minimum wavelength and wavelength, the wavelength value of each point can be found and stored in the local log and historical database.

3) Data processing module

   After collecting the spectral data of each channel, the noise is filtered out and the waveform is smoothed. Then by using the calibration wavelength of each sensor in the sensor's structural parameters, the channel and band of each sensor are scanned to determine the reflection peak of each sensor, and the wavelength shift is then

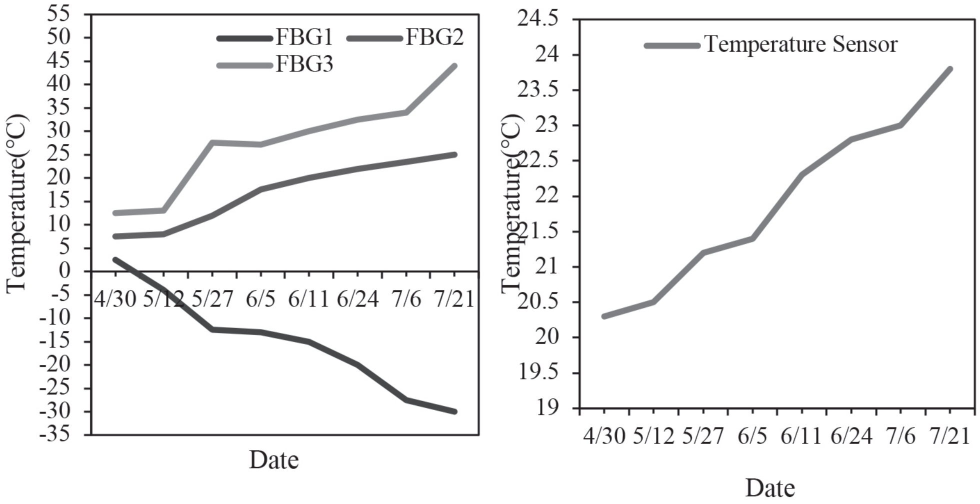


Figure 12 Partial strain sensor strain change curve and a temperature sensor temperature change curve.

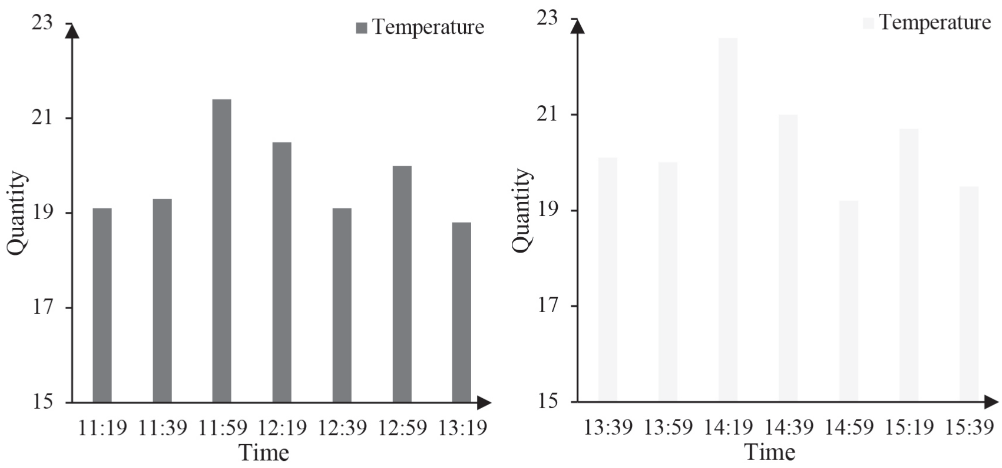


Figure 13 Diagram showing temperature change of a temperature sensor.

obtained from the calibration value. By using the type of sensor, the calibration value and the parameters of the temperature compensation point, the physical quantities such as temperature and strain are converted through corresponding methods.

By adopting the support hybrid communication technology, the system sends the hybrid communication protocol to the monitoring center for remote query, which can warn of abnormal data at the threshold. The strain data monitored by some strain sensors during the same period and the temperature data monitored by a temperature sensor for the same period are shown in Figure 12:

A set of temperature sensing data was collected from 11:19 to 15:39 on a certain day: The collection interval is 20 minutes and the results are shown in Figure 13:

After nearly a year of testing, the operation effect is good and the data is sent by ADSL in general. When the ADSL channel fails, the CDMA number can be used as the main channel to send and receive data; when the Internet communication is temporarily interrupted, the system can send data through SMS. The results obtained by this study indicate that the hybrid communication technology can meet the various requirements of remote monitoring of the bridge structure safety. At present, the structural health monitoring system of the stay cable for the bridge is under development, and the hybrid communication technology is also being used. Moreover, the technology will be tested further and improved.

To sum up, a series of unit tests and integration tests were carried out on the hybrid communication protocol during the development stage, and the correctness of the development of the hybrid communication protocol was verified through functional tests of consistency and interoperability. This study also conducted a large number of performance tests: the net load, security handling, load density and transmission scheduling parameters were tested on UDP and SMS channels; the RTT value of data transmission was analyzed; factors such as channel delay, security encapsulation, data compression, channel type, and queue parameters were analyzed. Also, by means of remote monitoring of the structural safety of a large bridge, the effectiveness, reliability and safety of remote monitoring were verified.

5. CONCLUSIONS

The safety of large building structures can be effectively monitored using a remote monitoring system, which serves as a crucial means of preventing catastrophic accidents. It is therefore essential to ensure the availability, reliability, security, and other quality indicators of the remote monitoring system. This study investigated the role of the remote monitoring system and the Internet of Things (IoT) monitoring method in enhancing the safety of large-scale construction projects. The analysis was conducted through the IoT positioning algorithm and field testing of the safety remote monitoring system for large-scale structures. At the same time, the effectiveness of the remote monitoring system for monitoring the Z bridge was verified on-site, confirming the significant role of remote monitoring and demonstrating the feasibility of the IoT-based remote monitoring system for improving construction safety.With the development of science and technology, research on monitoring systems has become extensive, involving various technologies such as data communication, sensing technology, data analysis and processing, automatic control, computer interface, and software engineering. While the research content of this paper may not be comprehensive, it nonetheless contributes to advancing this field of study. To further expand the application of the remote monitoring system for large-scale building structure safety and improve its data hybrid communication function, many challenges still need to be addressed through in-depth and extensive research. With the continuous advancement of IoT technology, it is anticipated that an increasing number of scholars will focus on this area, leading to more innovative solutions and practical applications.

REFERENCES

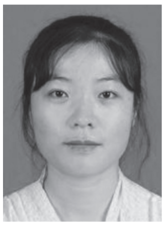
1. W. Fu, L. Zhang, C. Li, "Dynamic Access Control using Blockchain-based Attribute Encryption Scheme for Big Data Cloud Storage", Engineering Intelligent Systems, vol. 33 no. 3, pp. 263–273, 2025.
2. Zhang Y J, Li Z, Liu Q. Design and Implementation of Remote Monitoring System for High Frequency Vibrator[J]. Chung-kuo Tsao Chih/China Pulp and Paper, 2018, 37(12):51–55.
3. Li H, Guo F, Hou Y, Yang G, Guo H. Substation DC power remote monitoring system and APP application[J]. Power System Protection and Control, 2018, 46(19):144–150.
4. Cai, Changqing, Liu, Hui, Yang, Wenjun. Design and Development of a Greenhouse Remote Monitoring System Based on WinCE[J]. Meteorological and Environmental Research, 2018, v.9(04):110–115.
5. B. Wang, Y. Ye, "Construction of Internet of Things Resource-Sharing Platform Based on Intelligent Information Processing from the Perspective of Network Security", Engineering Intelligent Systems, vol. 33 no. 3, pp. 239–248, 2025.
6. Wang D, Chen D, Song B, Guizani N, Yu X, Du X. From IoT to 5G I-IoT: The Next Generation IoT-Based Intelligent Algorithms and 5G Technologies[J]. Communications Magazine, IEEE, 2018, 56(10):114–120.
7. Chen I R, Jia G, Bao F. Trust Management for SOA-Based IoT and Its Application to Service Composition[J]. IEEE Transactions on Services Computing, 2017, 9(3):482–495.
8. Broring A, Schmid S, Schindhelm C K, Khelil A, Kabisch S, Kramer D, et al. Enabling IoT Ecosystems through Platform Interoperability[J]. IEEE Software, 2017, 34(1):54–61.
9. Gharbieh M, Elsawy H, Bader A, Alouini M S. Spatiotemporal Stochastic Modeling of IoT Enabled Cellular Networks: Scalability and Stability Analysis[J]. IEEE Transactions on Communications, 2017, 65(8):3585–3600.
10. Farahani B, Firouzi F, Chang V, Badaroglu M, Constant N, Mankodiya K. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare[J]. Future Generation Computer Systems, 2017, 78(PT.2):659–676.
11. Hodo E, Bellekens X, Hamilton A, Dubouilh P L, Iorkyase E, Tachtatzis C, et al. Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System[J]. tetrahedron letters, 2017, 42(39):6865–6867.
12. Ammar M, Russello G, Crispo B. Internet of Things: A survey on the security of IoT frameworks[J]. Journal of Information Security and Applications, 2018, 38(FEB.):8–27.
13. Luong N C, Hoang D T, Ping W. Data Collection and Wireless Communication in Internet of Things (IoT) Using Economic Analysis and Pricing Models: A Survey[J]. IEEE Communications Surveys & Tutorials, 2017, 18(4):2546–2590.
14. Yu K, Wang Y, Yu J, Yu D, Cheng X, Shan Z. Localized and distributed link scheduling algorithms in IoT under rayleigh fading[J]. Computer Networks, 2019, 151(MAR.14):232–244.
15. Menke J H, Hegemann J, Gehler S, Braun M. Heuristic Monitoring Method for Sparsely Measured Distribution Grids[J]. International Journal of Electrical Power & Energy Systems, 2018, 95(feb.):146–155.
16. Kim J, Lee H, Jeong S. Sound-based remote real-time multi-device operational monitoring system using a Convolutional Neural Network (CNN)[J]. Journal of Manufacturing Systems, 2021, 58(2):431–441.
17. Keller S. Moving to a wireless remote monitoring system[J]. Control Engineering, 2017, 64(8):18–18.
18. Nazir, S., Hamdoun, H., Verdicchio, F., & Fairhurst, G. (2018). Autonomous monitoring framework for resource-constrained environments. Cyber-Physical Systems, 4(3), 137–155.
19. Madrid N, Boulton R, Knoesen A. Remote monitoring of winery and creamery environments with a wireless sensor system[J]. Building and Environment, 2017, 119(JUL.):128–139.
20. Xiaodan, Feng. Design and Implementation of Remote Health Monitoring System for 3D Visual Bridge[J]. Procedia Engineering, 2017, 174(Complete):1330–1335.

Luyue Han was born in Binzhou, Shandong, China, in 1988. She is a Senior Engineer at Binzhou Polytechnic. She received the bachelor's degree from China University of Petroleum (East China) University and her master's degree from Northwestern Polytechnical University. Her research interests include ntelligent construction and information technology.

E-mail: HLY19880612@126.com

Liyan Gao was born in Binzhou, Shandong, China, in 1979. She is an adjunct professor at Binzhou Polytechnic. She received the bachelor's degree from Tsinghua University, her master's degree from Harbin University of Science and Technology. Her main research interest is project management engineering.
Email: gaolunwen67075241@126.com

Songshan Feng was born in Shouguang, Shandong, China, in 1973. He is an adjunct professor at Shandong Urban Construction Vocational College. He received the bachelor's degree from Shandong Jianzhu University and his master's degree from Shandong University. His main research interest is construction project management.
E-mail:705522978@qq.com



Fengzhen Qu was born in Heze, Shandong, China, in 1981. She is at Binzhou Polytechnic. She received the bachelor's degree from Shandong University of Technology and her master's degree from Shandong University of Technology. Her main research interest is vehicle engineering.
E-mail: 83532851@qq.com

Bowen Song was born in Binzhou, Shandong, China, in 1998. He is at Binzhou Polytechnic. He received the bachelor's degree from Heilongjiang Institute of Technology and his master's degree from Qilu University of Technology. His main research interest is Control Engineering.
E-mail: 810161874@qq.com