

# An Analysis of Internet of Things Computer Network Security and Remote-Control Technology

Malingraya Keramagi<sup>1</sup>, Sumit Tiwari, Mrs. Aarti Gawai<sup>2</sup>

<sup>1</sup>Student, Department of Computer Science, D. G. Ruparel College, University of Mumbai, Mumbai, Maharashtra, India

<sup>2</sup>Assistant Professor, Department of Computer Science, D. G. Ruparel College, University of Mumbai,

Mumbai, Maharashtra, India

keramagimalingraya@gmail.com | [sumittiwari5704@gmail.com](mailto:sumittiwari5704@gmail.com) | [aartigawai1611@gmail.com](mailto:aartigawai1611@gmail.com)

\*\*\*

**Abstract** - To address the specific application of Internet of Things (IoT) computer network security monitoring technology in infrastructure construction, this paper proposes a design method for a remote network monitoring system, taking tunnel construction safety as a case study. Based on the characteristics of construction tunnel safety monitoring, the work provides theoretical guidance on computer remote monitoring, data decision analysis, safety control, personnel positioning and data management. Experimental results show that when sensor data is extracted over a two-minute window, detection accuracy exceeds 80%, while a four-minute window raises accuracy above 90%. In the response time tests, local control response is generally under 1 s, whereas remote control response is usually within 3 s and may occasionally exceed 5 s. The designed system transmits collected data to a remote monitoring terminal, where sensor readings are analysed through timing-based decision making. The method effectively computes the safety status of every monitoring unit of the tunnel using a weighted algorithm and formulates corresponding emergency measures according to that status, while network isolation, code management and automatic data repair safeguard the security of the IoT network itself.

**Key Words:** Internet of Things, network security, remote control, tunnel monitoring, wireless sensor network, ZigBee, decision analysis

## 1. INTRODUCTION

With the rapid development of Internet of Things (IoT) technology, its scope of application has become steadily wider. At present, the IoT is widely used in intelligent buildings, smart cities, smart transportation, smart homes, logistics systems, environmental detection, digital medicine, energy conservation, fire protection and many other fields. With the continuous growth of the transportation industry, more and more tunnels have been put into use. Because the tunnel environment is harsh and accidents occur easily, tunnel safety has become a major problem of traffic safety, and ensuring safe tunnel operation is therefore of considerable importance.

With the increase in investment in infrastructure construction, the safety of tunnel construction has attracted wide attention. Common tunnel disasters include fire, excessive harmful gas, water inrush and collapse. How to predict such disasters and control safety after a disaster is a key point of tunnel construction monitoring. A construction tunnel monitoring system is a large system involving multidisciplinary knowledge such as computers, communications and software development.



**Fig -1:** Application domains of the Internet of Things.

According to the characteristics of construction tunnel safety monitoring, exploratory research was carried out from the aspects of data decision analysis, safety control, personnel positioning and data management. A construction tunnel safety monitoring solution based on the Internet of Things is proposed in this paper. The environmental characteristics, safety protection requirements and control requirements of tunnel construction are analysed in detail, together with the disaster characteristics of tunnel fire, harmful gas exceeding the standard, water inrush and collapse.

Combined with the actual situation of tunnel construction, a method combining local control and remote control of tunnel safety is put forward. When the level of tunnel disaster is low, the control command is sent through the monitoring software to drive the control execution equipment in the tunnel field. When the level of disaster is high and the on-site danger is beyond local control, the monitoring software requests remote assistance from the remote 3G terminal and reports the on-site situation. In order to manage and monitor construction personnel better, the system also uses a ZigBee network to locate the workers.

The IoT must ensure the security and confidentiality of computer network information transmission during operation and strengthen the management of network services. Illegal program codes in the network can destroy important data and control functions in an IoT system. Managers therefore need to strengthen the management of illegal program codes and formulate effective control measures to ensure the security of the code running in the system. The application of remote control technology can meet the needs of remote data transmission and acquisition, and network code management must be strengthened during that period so that illegal code cannot damage the IoT system or affect communication security.

## 2. RELATED WORK

Shi and Zhou believed that it was of great significance to study a remote tunnel monitoring system based on IoT architecture, since ensuring the safe operation of tunnels is not only a management system issue but also requires reliable technical support [1]. Mansour et al. argued that effective tunnel safety emergency command requires not only a sound safety management organisation but also an efficient and intelligent information management system [2]. Chen et al. held that a remote tunnel monitoring system can provide data support for management and decision making, allowing real-time monitoring and remote control, eliminating potential hazards in advance and enabling emergency rescue measures, thereby reducing harm and loss and improving the intelligence of the system [3].

Tong and Sun observed that the development of IoT technology is still at an early stage, with various technologies and modes not yet mature and the application scope still limited [4]. Wei et al. noted that the Internet of Things is the next major target of the information industry worldwide [5]. Honar Pajoooh et al. concluded that applying IoT technology in tunnels not only improves the data level of tunnels but also promotes the development of the entire IoT industry [6]. Wei et al. further stressed that safe tunnel operation is an important part of safety work in the transportation construction industry [7], while Qiao argued that research on IoT applications in tunnel remote monitoring also has reference value for unified safety monitoring and emergency command systems [8].

Guo et al. pointed out that the IoT is being applied constantly across industries, with smart cities and smart transportation advocated nationwide [9]. Monitoring systems based on the IoT are developing rapidly, but problems remain. Most such systems are only simple technical improvements of traditional monitoring systems and lack a genuine thing-to-thing connecting concept. Zhang et al. noted that most monitoring systems use a single sensor and a single communication mode, so the degree of integration is low [10]. The whole monitoring process includes data acquisition, communication, processing, evaluation and visualisation, and part of this chain still does not involve the IoT or provides only weak functionality.

Traditional tunnel monitoring systems mostly use fieldbus technology to transmit the underlying data. This approach has clear disadvantages: the cost of wiring is a large overhead, and the complexity and difficulty of wiring and maintenance create considerable trouble for construction personnel. It cannot meet the requirement of dynamically adding monitoring points in the tunnel, because new monitoring points or additional monitored quantities require rewiring. These limitations motivate the wireless, IoT-based monitoring architecture described in the following section.

## 3. SYSTEM DESIGN AND METHODOLOGY

### 3.1 Overall System Architecture

The monitoring system of a construction tunnel concentrates sensor data collection, data analysis and processing, in-situ disaster processing equipment, 3G remote linkage equipment and mobile positioning into one whole system. It detects all

kinds of disasters in the tunnel in real time and reports the data to the monitoring centre, where monitoring software analyses and processes the data. According to the level of risk, local tunnel processing equipment is called or the 3G remote linkage mechanism is started, so that losses caused by tunnel disasters are minimised. The hardware structure of the tunnel monitoring system is composed of a sensor network, a 3G network, a ZigBee network and the monitoring centre [11].

### 3.2 Sensor Network and Data Acquisition

The sensor network mainly accomplishes data acquisition. The acquired data include temperature, humidity, light, oxygen, carbon dioxide, carbon monoxide, smoke, nitric oxide, nitrogen dioxide, methane, dust, noise, wind speed, liquid level, stress, vibration and displacement. Because wireless sensor nodes are battery powered, data acquisition is performed at time intervals. Each sensor node sets an alert value for every data item. Once the collected data exceeds the alert value, the node enters emergency pass-through mode and collects data uninterruptedly, so that decision makers can grasp the change trend of the disaster in time. When the collected data falls below the safe value, the node exits the emergency pass-through mode.

The collected data is sent to the wireless gateway through the WIA-PA network and then forwarded by the gateway to the remote computer network monitoring centre through a router [12, 13]. WIA is an industrial wireless network in full compliance with the national WIA-PA standard for process automation. A WIA network consists of at least one WIA gateway and one device, and a single gateway can manage at most 100 devices. Multiple WIA networks can form largescale complex networks through Ethernet interconnection [14]. The 3G information is sent by the monitoring centre to the 3G terminal equipment supplier through the Internet, then to the 3G public network by the supplier's server, and finally to the 3G terminal equipment.

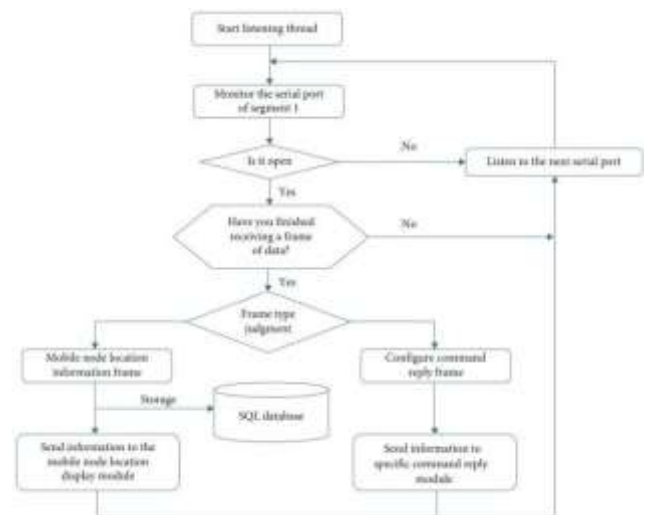


Fig -2: Multiserial port monitoring process.

### 3.3 ZigBee Positioning and TOF Ranging

The ZigBee network consists of a master node, mobile nodes and anchor nodes. The master node acts as the network gateway and is responsible for collecting data from the reference and

mobile nodes. The positioning algorithm of the ZigBee wireless positioning network adopts RF-TOF ranging technology, and the position of construction personnel can be calculated by placing a sensor node on the worker's helmet. In this research the device provided signal sending and receiving, time stamp recording and delayed sending. When the clocks of the hardware are not synchronised, single-sided two-way ranging (SS-TWR) can be adopted, and the flight time of the signal is calculated as shown in Eq. (1).

$$TOF = \frac{1}{2} * ((T_3 - T_0) - (T_2 - T_1)). \quad (1)$$

This method is not commonly used, because there is a deviation between the clock of the base station, the clock of the tag and the standard clock, represented by the clock drift rate  $k$  ( $k = 10$  ppm). Assuming that the tag delay time  $T_d$  is 3 ms and that the signal flight time is negligible compared with the delay time, the ranging error caused by the delay time  $T_d$  is given by Eq. (2).

$$|r| = \frac{1}{2} * |k_b - k_t| * T_d * c. \quad (2)$$

The positioning subsystem is completed by the ZigBee network data collection management module. Because the system monitors three sections of the construction site at the same time, the network is composed of three sub-positioning networks, each consisting of a master node, a reference node and a mobile node. The master node acts as the gateway and completes the data receiving and sending of the reference and mobile nodes, while the upper computer sends data through the serial port [16]. Since the construction sections are not connected, the WIA network and the ZigBee network are likewise composed of three subnetworks that collect and manage their own blocks and resist the electromagnetic interference typical of industrial fields.

### 3.4 IoT Computer Network Security Measures

The IoT must analyse and process data during operation, so the computer must have sufficient space to store the data. Once data in the IoT is damaged, the damaged data can be automatically repaired with the support of the system. There are multiple technical control areas in an IoT deployment and these areas need to be isolated from one another. Effective isolation between technical control areas avoids damage to the network system by illegal intruders and secures the IoT computer system as far as possible. In addition, strengthening IoT computer network security management requires corresponding operating norms, an implemented responsibility system and clearly defined operating rights for operators.

### 3.5 Decision Analysis of Tunnel Safety

After the monitoring system collects data, the sensor readings are stored in the database of the remote computer. To determine the current state of the tunnel, data fusion and state analysis are necessary. A block of tunnel is long, so even when sensor data is analysed the endangered position cannot be identified from the results alone [17]. The system therefore adopts a decision analysis method based on remote monitoring units: a block of

the tunnel is divided into a number of monitoring units, and each unit collects all kinds of sensor data and stores them in the database. Decision analysis is the analysis of the state of a single monitoring unit.

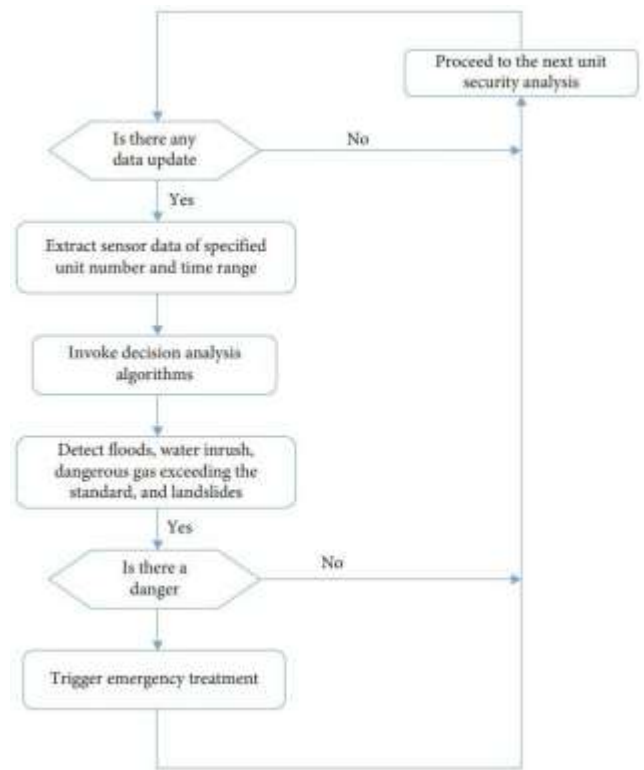


**Fig -3:** Flow chart of decision-making analysis and processing.

The system detects four kinds of dangerous situations in the tunnel - fire, dangerous gas exceeding the standard, water inrush and collapse - and outputs the grade of each danger for the unit. When the danger level exceeds the normal level, the computer triggers corresponding emergency measures automatically so as to respond to the dangerous situation as soon as possible. According to the data of different sensors, tunnel disasters are divided into five grades: normal, existence of hidden danger, danger treatment, emergency avoidance and disaster relief.

Safety inspection is carried out unit by unit. By analysing all the data uploaded by the unit node over a period of time, the security level of the unit is concluded. Data uploaded by the sensor nodes within 2 to 10 minutes is extracted from the field information collected through the monitoring network. If the time span is too long the analysis takes too long, and if it is too short the results become inaccurate. In terms of the weight of the data, the more recently the data was uploaded, the greater the weight it should carry [19, 20]. At the same time, tunnel danger must be judged from multiple sensor readings, each of which carries a different importance; in fire detection, for example, temperature, humidity, oxygen, carbon monoxide, carbon dioxide and smoke are tested together.

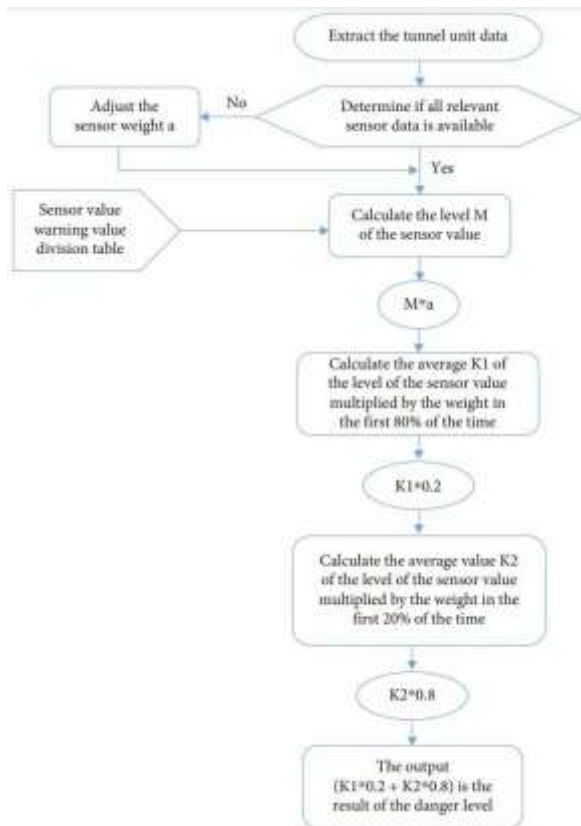


Fig -4: Decision-making algorithm for analysis of construction tunnel safety.

### 3.6 Emergency Treatment and Remote Linkage

Correct and reasonable prevention and control measures inhibit or reduce the degree of disaster harm; conversely, inattention or wrong countermeasures aggravate the disaster and may even induce further damage. Tunnel emergency treatment therefore takes different countermeasures for different categories and levels of disaster [18]. The emergency response measures are of three kinds: rewriting the colour of the monitor view area, sending a local control command, and starting the remote linkage. The latter two send control commands to the field and to the remote terminal respectively and involve relatively complex processing logic.

In local control the monitoring centre sends control commands to the execution nodes through the WIA gateway. After transmission is complete it is necessary to wait for the execution result of the terminal device, and the next control action is taken according to that result. If the command is unsuccessful more than three times, the result is recorded in the database and a prompt is displayed on the interface.

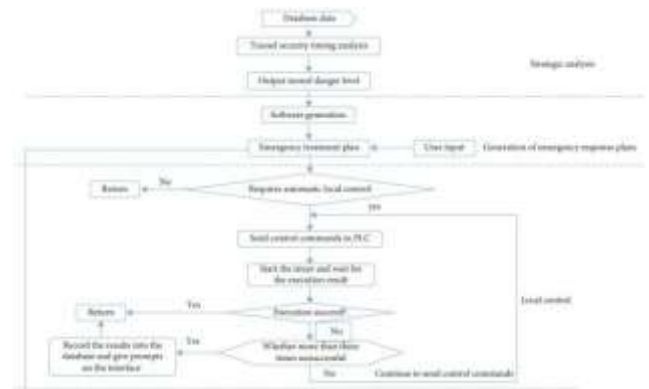


Fig -5: Flow chart of strategic analysis and local control processing.

Remote linkage reports the scene situation to the remote 3G terminal equipment. The information to be sent is packed by the monitoring software and sent to the 3G terminal server through the Ethernet interface; the server then delivers the message to the terminal device through the 3G network. Because 3G delivery is not guaranteed, a resending mechanism is added in the design of the software: when no acknowledgement is received from the 3G terminal device within a certain period, the control command is resent. Reports are sent to equipment placed in the fire department, emergency department and government departments.

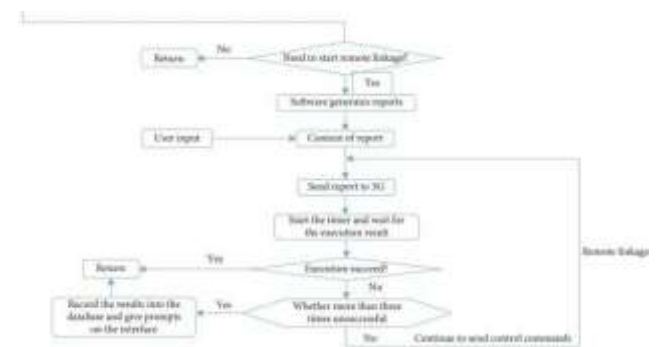


Fig -6: Flow chart of remote linkage emergency processing.

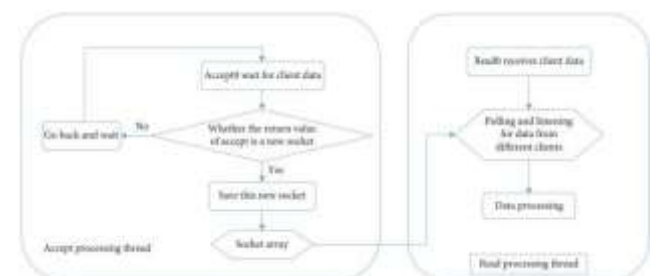


Fig -7: Flow chart of multiterminal network data processing.

## 4. RESULT ANALYSIS

The main components of a controlled network are hardware and software, which work together to provide control services. The core of the controlled system is the control of data collection, and the control system is centred on the computer. When designing a controlled system it is necessary to adhere to the principle of security, to strengthen the protection of user information and to repair any problem immediately once it occurs. Remote control technology can control both computer

hardware and software equipment and complete file transmission and management tasks.

Because fires and landslides are difficult to reproduce, the method of burning paper in the field was used in the tunnel danger simulation, with sensors placed around the combustion for detection. Landslides could not be simulated in the laboratory environment, so the test method adopted was to simulate the change characteristics of the support subplane during collapse by pressurising the pressure sensor and changing the displacement value of the sensor. When testing whether harmful gases exceeded the standard, the analysis method for each gas was similar, so detection was carried out according to the concentration of carbon dioxide [23].

#### 4.1 Safety Detection Accuracy

The security analysis test extracted data within 2 minutes and within 4 minutes for decision analysis. In the decision analysis algorithm, the weight of the historical data in the first 80% of the window accounted for 20% of the result and the most recent 20% of the window accounted for 80%. When data within 2 minutes was taken for testing, the detected disaster time was 24 to 30 s in theory and the detection accuracy was higher than 80%. The test results are shown in Table -1.

**Table -1:** Extracting historical data within 2 minutes for decisionmaking analysis.

| Test items             | No. of tests | Analysis time < 30 s | Analysis time > 30 s | Not detected | Detection accuracy |
|------------------------|--------------|----------------------|----------------------|--------------|--------------------|
| Fire (simulation)      | 25           | 13                   | 8                    | 4            | 84.00%             |
| Water inrush           | 32           | 28                   | 4                    | 0            | 100%               |
| Excess of harmful gas  | 42           | 34                   | 6                    | 2            | 95.23%             |
| Landslide (simulation) | 19           | 11                   | 7                    | 1            | 94.74%             |

When the extraction window was 4 minutes, detection results were normally obtained in 48 to 60 s and the detection accuracy rose above 90%, as shown in Table -2.

**Table -2:** Extracting historical data within 4 minutes for decisionmaking analysis.

| Test items             | No. of tests | Analysis time < 60 s | Analysis time > 60 s | Not detected | Detection accuracy |
|------------------------|--------------|----------------------|----------------------|--------------|--------------------|
| Fire (simulation)      | 25           | 14                   | 9                    | 2            | 92.00%             |
| Water inrush           | 32           | 26                   | 6                    | 0            | 100%               |
| Excess of harmful gas  | 42           | 25                   | 16                   | 1            | 97.62%             |
| Landslide (simulation) | 19           | 11                   | 8                    | 0            | 100%               |

#### 4.2 Local Control Response Time

The local control command was executed by the PLC controller at the construction site. The monitoring software sent the control command to the WIA gateway through Ethernet, and the gateway forwarded the message to the underlying executing node according to the write-command format. After receiving the data, the executing node sent it to the RS232-to-485 serial port, and finally the data reached the 485 interface of the PLC

controller and each control device [24]. Tests were run with 10, 20 and 40 network nodes and the results were classified into four situations, as shown in Table 3 and Fig -8.

**Table -3:** Test results of local control response time.

| Network scale (nodes) | No. of tests | Response < 1 s | 1 s < Response < 3 s | No execution |
|-----------------------|--------------|----------------|----------------------|--------------|
| 10                    | 35           | 35             | 0                    | 0            |
| 20                    | 36           | 34             | 2                    | 0            |
| 40                    | 35           | 30             | 4                    | 1            |

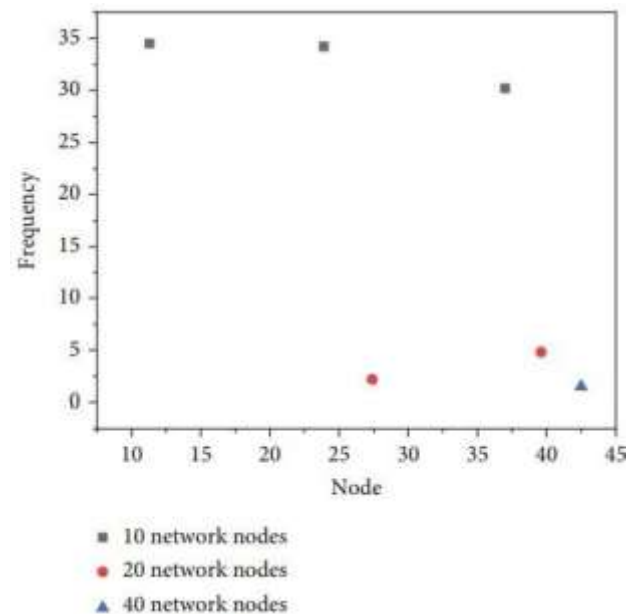


**Fig -8:** The test results of local control response time.

The local control response time was generally less than 1 s. As the network size increased, a delay phenomenon appeared in the execution of control commands, and the larger the network the more pronounced the delay. The main cause is that node processing capacity - computing power configuration, backplane bandwidth and forwarding buffer - is limited, so the time slice obtained by each node becomes smaller. When the network size reached 40 nodes, one control command was not executed within 30 s. The scale of the network should therefore be considered carefully when the network is laid out, and the number of sensor nodes in each bidding section should not be too large [25].

#### 4.3 Remote Linkage Response Time

In testing the remote linkage response, a command was sent to the terminal several times and the time at which the terminal received the packet was recorded [26]. The characteristics and distribution of the response time are shown in Fig -9. The results show that the response time of the 3G network was relatively dispersed. In general a response within 3 s could be expected, but responses of more than 5 s also occurred, and occasionally no response was received at all, because the 3G terminal depends on external network information whose stability requirement is high.

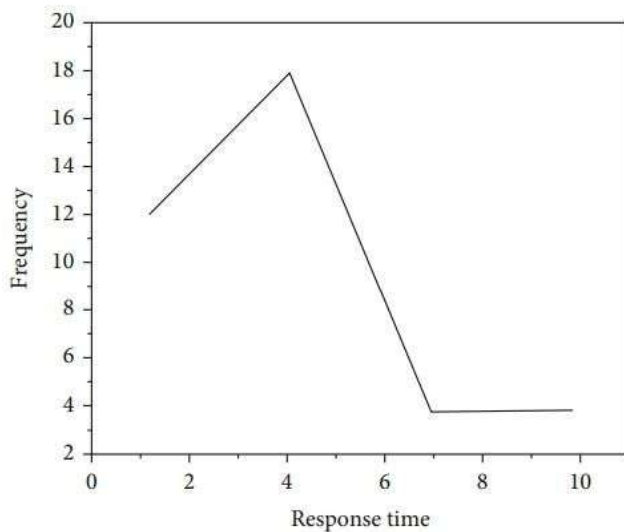


Fig -9: The test results of remote linkage network response time.

#### 4.4 Personnel Positioning Accuracy

In a construction tunnel the structure is usually linear and the localisation algorithm is relatively complex to implement, particularly for two-dimensional systems, which have a long development cycle. The system therefore adopts a onedimensional localisation system that outputs the segment number of the moving node and the corresponding onedimensional coordinate value [27, 28]. ZigBee communication protocols are used in the positioning network and the ranging algorithm uses time-of-flight measurement. The mobile node sends a wave to the reference node and the round-trip time is measured; since transmission time is proportional to distance, the distance between reference node and mobile node - and hence the location of the mobile node - can be calculated. The positioning principle is shown in Fig -10.

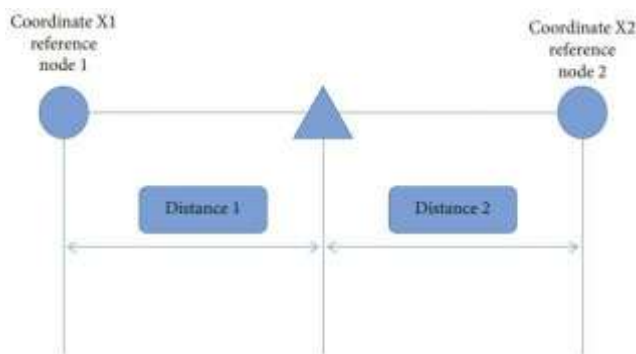


Fig -10: Schematic diagram of the localisation algorithm.

The test was divided into a corridor test inside the experimental building and an outdoor square environment test, so as to evaluate positioning in different environments. The distance between the two reference nodes was 30 m. Owing to current conditions, the positioning effect was tested only with two and three reference nodes. A result deviating from the true value by more than 3 m was considered invalid. The deviation error values and the percentage of valid data were recorded, as shown in Table -4.

Table -4: The test results of positioning.

| Test conditions                 | Valid data (within 3 m) | Deviation from normal m) test data | Total value (3 | Min error (cm) | Max error (cm) | Valid data % |
|---------------------------------|-------------------------|------------------------------------|----------------|----------------|----------------|--------------|
| Square, two reference nodes     | 31                      | 6                                  | 37             | 4              | 293            | 83.78%       |
| Square, three reference nodes   | 24                      | 4                                  | 28             | 12             | 225            | 85.71%       |
| Corridor, two reference nodes   | 38                      | 2                                  | 40             | 27             | 275            | 95.00%       |
| Corridor, three reference nodes | 26                      | 7                                  | 33             | 9              | 295            | 78.79%       |

Because of hardware instability and other factors, errors of more than 3 m appeared in some measurements. The results show that test accuracy had no clear connection with the test environment or with the number of reference nodes, so the environmental impact on the positioning system is relatively small. However, with an accuracy of only about 80%, the precision of the positioning system still needs further improvement.

## 5. CONCLUSIONS

Internet of Things technology is a clear development trend for the future, and its effective use in enterprises can improve the efficiency of resource sharing. During this period technicians need to strengthen the management of the operating environment of the IoT and further improve the functions of the remote control system to guarantee its operational safety and stability. With the intensification of road traffic construction, increasing attention has been paid to the monitoring of construction tunnels, where common disasters include fire, harmful gas exceeding the standard, water inrush and landslides. The computer remote monitoring system presented here collects 17 kinds of sensor values through a wireless sensor network, monitors the running state of the construction tunnel in real time and derives the safety state of the tunnel by analysing sensor data. The main contributions of this work are summarised below.

- Analysis of tunnel safety: safety analysis of each unit of the construction tunnel is carried out regularly. Recent historical data is extracted from the database and different weights are allocated to data of different times and different sensor types, and the status of each monitoring unit is computed by the decision analysis algorithm.
- Multiterminal network communication management: the monitoring system is composed of a WIA sensor network, a ZigBee positioning network and a 3G remote linkage, with each bidding section forming a subnetwork, so multiterminal and multinetwork management is realised.
- Tunnel emergency treatment: different emergency measures are required at different danger levels, and a reasonable emergency treatment scheme and the corresponding software process were designed and implemented.
- Remote linkage control: when the risk level is high and field equipment cannot control the situation, an integrated remote control scheme based on 3G communication sends the report through the Ethernet interface to the fire department, emergency department and government departments.

- System monitoring view management: the running condition of each tunnel section and of execution equipment such as fans and water pumps is monitored graphically in real time.
- Database management: sensors continuously collect data that forms the basis both for tunnel safety analysis and for post-event accident analysis, with data dump, query and printing functions provided.

Future work will focus on improving the precision of the positioning subsystem beyond the present 80% level, on reducing control command delay in larger networks, and on strengthening intrusion detection and code management so that the security of the IoT network keeps pace with the growth of the monitoring infrastructure.

## ACKNOWLEDGEMENT

The author sincerely thanks Mrs. Aarti Gawai, Department of Computer Science, D. G. Ruparel College, University of Mumbai, for her valuable guidance and continuous encouragement throughout this work, and the Department of Computer Science for providing the facilities required to complete this study.

## REFERENCES

- [1] Y. Shi and Y. Zhou, "Gene extraction of Leizhou kiln porcelain patterns based on safety Internet of Things and its application in modern design," *IETE Journal of Research*, vol. 3, pp. 1–8, 2021.
- [2] R. F. Mansour, M. M. Althobaiti and A. A. Ashour, "Internet of Things and synergic deep learning based biomedical tongue color image analysis for disease diagnosis and classification," *IEEE Access*, vol. 9, pp. 94769–94779, 2021.
- [3] G. Chen, F. Zeng, J. Zhang, T. Lu and W. Shu, "An adaptive trust model based on recommendation filtering algorithm for the Internet of Things systems," *Computer Networks*, vol. 190, no. 15, art. 107952, 2021.
- [4] Y. Tong and W. Sun, "The role of film and television big data in real-time image detection and processing in the Internet of Things era," *Journal of Real-Time Image Processing*, vol. 18, no. 4, pp. 1115–1127, 2021.
- [5] T. Wei, W. Feng, Y. Chen, C. X. Wang, N. Ge and J. Lu, "Hybrid satellite-terrestrial communication networks for the maritime Internet of Things: key technologies, opportunities and challenges," *IEEE Internet of Things Journal*, vol. 8, pp. 8910–8934, 2021.
- [6] H. Honar Pajooh, M. Rashid, F. Alam and S. Demidenko, "Multi-layer blockchain-based security architecture for Internet of Things," *Sensors*, vol. 21, no. 3, p. 772, 2021.
- [7] D. Wei, H. Ning, F. Shi et al., "Dataflow management in the Internet of Things: sensing, control and security," *Tsinghua Science and Technology*, vol. 26, no. 6, pp. 918–930, 2021.
- [8] X. Qiao, "Integration model for multimedia education resource based on Internet of Things," *International Journal of Continuing Engineering Education and Life-Long Learning*, vol. 31, no. 1, p. 17, 2021.
- [9] C. Guo, S. Su, K. Choo, P. Tian and X. Tang, "A provably secure and efficient range query scheme for outsourced encrypted uncertain data from cloud-based Internet of Things systems," *IEEE Internet of Things Journal*, vol. 9, no. 3, pp. 1848–1860, 2021.
- [10] W. Zhang, X. Wang, G. Han, Y. Peng and M. Guizani, "SFPAG-R: a reliable routing algorithm based on sealed first-price auction games for industrial Internet of Things networks," *IEEE Transactions on Vehicular Technology*, vol. 70, pp. 5016–5027, 2021.
- [11] S. Qu, Z. Wang, Z. Qin, Y. Xu and Z. Liu, "Internet of Things infrastructure based on fast, high spatial resolution and wide measurement range distributed optic-fiber sensors," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2882–2889, 2021.
- [12] L. Nie, Y. Wu, X. Wang, L. Guo and S. Li, "Intrusion detection for secure social Internet of Things based on collaborative edge computing: a generative adversarial network-based approach," *IEEE Transactions on Computational Social Systems*, vol. 9, no. 1, pp. 134–145, 2021.
- [13] P. Wei and F. He, "The compressed sensing of wireless sensor networks based on Internet of Things," *IEEE Sensors Journal*, vol. 21, pp. 25267–25273, 2021.
- [14] Z. Yue, H. Sun, R. Zhong and L. Du, "Method for tunnel displacements calculation based on mobile tunnel monitoring system," *Sensors*, vol. 21, no. 13, p. 4407, 2021.