Computer Communications 153 (2020) 169–176

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

The method of Internet of Things access and network communication based on MQTT

Xiangtao Liu [a], Tianle Zhang [a], Ning Hu [a,*], Peng Zhang [b], Yu Zhang [a]

[a] Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China
[b] Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

ARTICLE INFO

Keywords:
MQTT protocol
Embedded network communication
Wi-Fi distribution network
IoT equipment

ABSTRACT

With the rise of intelligent hardware and the rapid development of the Internet of Things, its security issues are also facing severe challenges. Internet of things devices are often limited devices with limited computing power and limited resource space. Therefore, a lightweight security solution needs to be designed specifically for this purpose. The purpose of this article is to study the method of IoT device access and network communication based on MQTT (Message Queuing Telemetry Transport). Based on the MQTT protocol and the theoretical foundation of Wi-Fi technology, this paper proposes a Wi-Fi distribution network optimization scheme and terminal communication method, and sets up a system test platform. The experiment proves that the communication method of the IoT terminal equipment based on MQTT proposed in this paper can reliably and flexibly implement the communication function of the equipment and meet the communication needs of the IoT system. According to the performance of the Wi-Fi access configuration method, this paper tests the performance of transmitting information with lengths of 10 bytes, 30 bytes, 50 bytes, and 70 bytes, respectively, the average time of the distribution network is 0.6692s, 1.3546s, 2.8600s, 4.7319s, all rates are 100%. It can be seen that the system has a higher efficiency in network distribution.

1. Introduction

With the continuous development of information technology and the Internet, the Internet of Things has become a hot area of global concern and is considered to be one of the most significant technological innovations after the Internet [1]. The Internet of Things refers to the classification, networking, and networking of physical entities through various network connection technologies and information transmission technologies to achieve the connection and interaction between things and things, things and people, and complete a wide range of data collection, transmission and application, to achieve automatic management and remote control [2]. The Internet of Things connects physical entities to the network through the Internet, and performs data transmission, data storage, data control and management through communication networks to achieve interconnection at any time, any place, and any object [3]. It can be said that the Internet of Things integrates a variety of sensing, communication and computing technologies, which can realize the information interaction between people and things and between things, communication with the physical world is more convenient [4]. The Internet of Things has shown a strong driving force in promoting technological innovation, promoting economic growth, and improving people's quality of life, governments of various countries have promoted the innovation and development of the Internet of Things to national strategies [5]. IBM put forward the commitment to integrate the new generation of information technology into all walks of life, and put forward the idea of "smart earth" [6]. In 2009, the EU and South Korea respectively issued relevant policies to accelerate the development of the Internet of Things [7]. The Chinese government also attaches great importance to the development of the emerging industry of the Internet of Things, in the 2010 government work report, it was clearly stated that the Internet of Things industry should be revitalized, China has included the Internet of Things in the National Mid- and Long-Term Science and Technology Development Plan (2006–2020) and 2050 National Industry Roadmap [8].

With the development of the Internet of Things technology, various sensors and actuators on the production site are connected to the network, and a large amount of data is collected and analyzed to achieve operation monitoring, predictive maintenance, and manufacturing collaboration and other industry trends [9,10]. In this trend, the network access and interconnection of a large number of devices distributed in different regions has become the basis of the entire IoT industry, and it is also the most demanded and important link in the entire IoT industry chain [11]. However, the Internet of Things is different from

* Corresponding author.
E-mail addresses: liuxt@gzhu.edu.cn (X. Liu), tlezhang@gzhu.edu.cn (T. Zhang), huning@gzhu.edu.cn (N. Hu), pengzhang@iie.ac.cn (P. Zhang), 2111806072@e.gzhu.edu.cn (Y. Zhang).

https://doi.org/10.1016/j.comcom.2020.01.044
Received 17 December 2019; Received in revised form 13 January 2020; Accepted 22 January 2020
Available online 24 January 2020

the traditional Internet, its terminal sensing and information acquisition equipment has the characteristics of large quantity, wide field, various specifications, strong mobility, poor operating network environment, limited resources [12]. It is characterized by large differences in functions, diversity of network access, communication complexity between devices, and coordination requirements between devices [13]. At the same time, as the scale of the Internet of Things continues to expand and the number of device accesses increases, the amount of data processing brought by it is also increasing rapidly, which places higher requirements on system reliability, stability, and data concurrency processing capabilities [14]. The research on the architecture, communication methods and networking methods of the Internet of Things system, and the information interaction of the complex relationships between devices, has become an urgent problem for the large-scale application of the Internet of Things [15]. Existing IoT communication architectures are usually based on the cloud foundation, the cloud platform acts as middleware and connects IoT devices together, this solution promotes the disparity of heterogeneous devices from application developers or devices manufacturers are connected to the complexity of the platform, but for the communication of these devices, a standard protocol is required, among the many IoT communication protocols, the MQTT protocol is the most popular [16,17].

Suiyan and his team believe that because the seeding performance of precision rice seeders is not only affected by operating parameters, but also by the physical characteristics of the seeds, the seeding amount of plug trays sometimes changes during the rice seedling process. Therefore, in order to solve the problem of long working hours and low efficiency in artificial outdoor environments by using a seeder to monitor the seeding amount, they designed a wireless transmission system for seedling tray images based on embedded machine vision. Embedded development platform Tiny4412, Wi-Fi gateway, network camera, infrared sensor module and remote computer. Embedded Linux operating system, camera driver, GPIO port driver and network file system configuration are installed in the embedded development platform. The application includes image acquisition, and the image-friendly interactive interface is displayed on the screen in real time. Compress images using Jpeglib static library. Through the Wi-Fi network, the embedded system and the remote server implement socket communication according to the protocol data transmission regulations. The remote server implements collection, verification, display and saving. They found that the transmission of BMP and compressed JPEG images can meet the operating requirements of the rice automatic seeding test line, which greatly improved the transmission rate of JPEG images. Collect a stable seeding tray image and upload it to the server successfully. The average packet loss rate is 0.23%, and the error rate is 0.23%. The design of the system lays an experimental platform for remote control of rice seeding [18]. Yeh and his team believe that the e-health care trend has spread globally. Internet of Things (IoT) devices for medical services and popular personal health information (PHI) systems play an important role in the eHealth environment. Cloud-based PHI systems look promising, but raise concerns about privacy and information security. They proposed a cloud-based fine-grained health information access control framework for lightweight IoT devices with dynamic data auditing and attribute revocation functions. IoT devices (eg, wireless human sensors) need only symmetric encryption. Based on ciphertext policies, attribute-based encryption, double encryption, and variants of the Merkle hash tree are used to support fine-grained access control, effective dynamic data auditing, batch auditing, and attribute revocation. In addition, in addition to the fact that cloud service providers can help each other avoid fines due to data loss, the proposed scheme also defines and addresses cloud reciprocity issues [19]. Y.-J. Zhang and his team designed and implemented a monitoring system combined with the Internet of Things to address the problems faced by paper equipment suppliers, namely, how to achieve efficient and reliable remote monitoring of paper equipment sold to different regions. The monitoring center and smart gateway use the MQTT protocol topic subscription / message delivery mechanism to centrally remotely manage and operate the papermaking equipment distributed in different regions through the MQTT server deployed in the cloud. At the same time, a large amount of historical data stored in the cloud server can help make scientific decisions by using data mining and information processing technology, improve production efficiency and reduce costs. Finally, the stability and reliability of the system were proved by high-frequency vibrator tests [20].

Based on the MQTT protocol and the theoretical foundation of Wi-Fi technology, this paper proposes a Wi-Fi distribution network optimization scheme and terminal communication method, and sets up a system test platform. The experiment proves that the communication method of the IoT terminal equipment based on MQTT proposed in this paper can reliably and flexibly implement the communication function of the equipment and meet the communication needs of the IoT system.

2. Proposed method

2.1. IOT communication protocol

(1) Characteristics of the Internet of Things system

Internet of things is the most basic feature of the Internet of Things system, and data interaction between the three ends is an inevitable requirement of the Internet of Things system. The Internet of Things system is different from ordinary Internet application systems and has special requirements for communication protocols, which are summarized as follows:

(1) The communication subject is mainly an embedded hardware device with limited resources. Therefore, it is usually required that the communication protocol be streamlined and lightweight;

(2) It is required to realize real-time monitoring and control of hardware equipment, and has high requirements for the immediacy of two-way communication;

(3) The equipment's working environment is complex, and it is not possible to guarantee good network conditions for a long time. It is necessary to rely on the communication protocol to provide mechanisms to maintain communication relationships and ensure communication reliability.

(4) There are a large number of hardware devices and complicated communication relationships, which require the system to have good scalability and low coupling.

(5) A lot of sensitive information is usually reflected in the Internet of Things system. It is necessary to avoid illegal eavesdropping and tampering of communications by third parties, thereby ensuring the security of communications.

At present, the more popular instant messaging protocols in the Internet of Things system are MQTT, CoAP, AMQP, HTTP. A summary and comparison of these four protocols. The comparison results are shown in Table 1:

(2) Introduction to MQTT protocol

The MQTT protocol is an application layer messaging protocol based on publish/subscribe under the ISO (International Organization for Standardization) standard, it works on the TCP/IP protocol family [21]. The MQTT protocol is a very simple, lightweight information transmission protocol designed for use with restricted equipment, low bandwidth, high latency, or unreliable networks. MQTT aims to minimize network bandwidth and equipment resource requirements, while ensuring reliability and a certain degree of delivery guarantee, which is ideal for IoT devices that require bandwidth and batteries.

(3) Analysis of MQTT communication architecture

MQTT adopts a client–server architecture and performs message transmission based on topic subscription/message publishing. Clients can act as both publishers and receivers of messages, clients receive messages from other clients by subscribing to topics of interest to the server [22]. When publishing a message, the client can choose to keep

Table 1
Comparison of typical IoT protocols.

Standard	MQTT	CoAP	AMQP	HTTP
Model	Publish/Subscribe	Request/Response	Publish/Subscribe	Request/Response
Packet size	Very small	Smaller	Larger	Big
Transport layer protocol	TCP	UDP	TCP	UDP
Encoding format	Binary	Binary	Binary	text

Table 2
Format of fixed header.

Bit	7 6 5 4	3	2 1	0
Byte1	Message type	DUP flag	QoS level	RETAIN
Byte2	Remaining length			

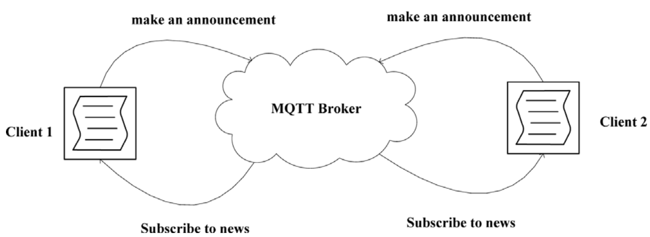


Fig. 1. MQTT communication architecture.

the content on the server, so that when there are new subscribers, it will directly receive the latest published message. The MQTT server is the intermediary of the client that publishes the message and the client that subscribes to receive the message. It can process the client's subscription and unsubscribe requests, receive the message published by the client and push the message to the corresponding client according to the topic. The MQTT communication architecture is shown in Fig. 1:

(4) Analysis of MQTT protocol control messages

An MQTT message consists of a fixed header, a variable header, and a payload at most. The fixed header is available in all types of messages, and the variable header and payload are only present in a part of the messages . The format of the fixed header is shown in Table 2:

(5) Characteristics of MQTT protocol

The MQTT protocol provides three levels of message transmission service quality for different scenarios.

QoSLevel0: At most once, this is the simplest level. It does not require the receiver to confirm. The publisher only sends the current message once. The sending of the message depends entirely on the underlying operating environment. The message may be delivered successfully or may be lost.

QoSLevel1: Ensure that the message is sent to the receiver at least once, which may be repeated; the receiver needs to return an acknowledgment (ACK packet) when receiving the data packet, and the message sender does not receive the reply packet within the specified time and will resend the current message until you receive a confirmation message from the other party;

QoSLevel2: Only once, to ensure that the message arrives only once. This level requires both parties to exchange 4 data packets, which is relatively complicated and suitable for scenarios where message loss or duplication is never allowed.

2.2. Wi-Fi communication technology

The various terminals in the Internet of Things system are widely distributed in space, and all terminals in the system are required to be able to connect to the cloud platform directly or indirectly through the Internet. However, there are a large number of hardware devices in the

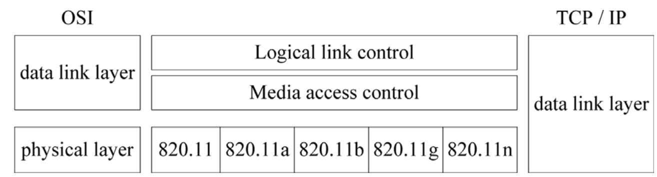


Fig. 2. Wi-Fi basic network structure.

Internet of Things system and the working environment is complicated. The use of wired network access for hardware devices cannot be implemented in many cases. Network access technology is gradually being promoted in IoT systems.

Among them, Wi-Fi technology is not limited by the wiring conditions, and the transmission rate is very high, in the case of weak signals or interference, the bandwidth can be adjusted, which effectively guarantees the stability and reliability of the network, at a stage of rapid development, transmission rates, security, power consumption, bandwidth, stability, functions, and other aspects are constantly improving [23]. What is more important is that Wi-Fi is now widely used around the world and covers a large area in our daily living environment. This provides a good network environment for the Internet of Things system and is a highly competitive wireless network communication technology.

(1) Overview of Wi-Fi technology

Wifi is a technology that allows electronic devices to connect to a wireless local area network (WLAN), typically using 2.4g UHF or 5G SHF ISM radio frequency bands [24]. Wifi technology is a wireless network communication technology based on the IEEE802.11 series standards, and the purpose is to improve the interoperability of wireless network products based on the IEEE802.11 series standards. The basic network structure of wifi only involves the lowest two layers of the OSI seven-layer reference model: the physical layer and the data link layer, which correspond to the network access layer of TCP/IP, and further divide the data link layer into logical links, control sublayer and media access control sublayer. The basic network structure of Wi-Fi is shown in Fig. 2:

Physical layer: This layer is directly connected to the transmission medium equipment and serves the data link layer upwards, and provides other relevant characteristics of the communication equipment such as electrical, function and process. For example, the ISM frequency band of the corresponding protocol of 802.11 is specified, and multiple modulation rates are supported.

Media access control layer (MAC layer): Implements fair control of access to shared media by terminals connected to the wireless network, and how channels are allocated for use rights.

Logical link control layer: completes the exchange of frames between stations, realizes source-to-destination error-free frame transmission, response control and flow control.

(2) Wi-Fi working mode

Wi-Fi has the following working modes:

(1) AP mode: Wi-Fi module acts as an AP (access point) to transmit wireless signals to create a wireless network, which can provide wireless access services and allow access by other wireless devices;

(2) STA mode: Any Wi-Fi module supports STA mode. In this mode, the Wi-Fi module does not accept access from other wireless devices, but connects to the AP as a client;

(3) Listening mode: In listening mode, the Wi-Fi module can receive all data packets passing through it, regardless of whether the destination MAC address of the data packet is consistent with the MAC address of the Wi-Fi module itself.

2.3. Wi-Fi access configuration method

(1) Distribution network design

The basic network (Infra) topology commonly used in Wi-Fi is mainly to form a full coverage of the network by adding wireless network access points, in fact, it is an application mode that integrates the wired and wireless LAN framework rights, it is also the most widely used wireless network, in communication mode, each wireless access point acts like a switch or hub in a wired network, and plays a role of signal forwarding [25].

The topology network is created by wireless AP, and many STA join. The AP is the center of the entire network, and all communications in the network are completed by AP forwarding.

In a basic wireless network based on AP, STA need to complete authentication through an access point name (i.e, SSID, Service Set Identifier) and password before they can access the AP for network access. However, in IoT systems, terminal node devices are usually miniaturized and low power, and do not have hardware resources such as keyboards and display screens. Users cannot directly enter the access point when configuring their Wi-Fi network. information. Some manufacturers use sonic and manual input methods to configure access point information, which will undoubtedly increase hardware costs. Because mobile phones, PAD and other devices have wireless Wi-Fi communication functions, it is intended to directly use these devices to configure access point information through Wi-Fi communication.

Wi-Fi is used for configuration, and AP-STA can be used, that is, the configuration end (such as mobile phone, PAD) works in STA mode, and the terminal device works in AP mode. After the connection is successful, the configuration end will access the information. Send directly to the terminal device, but this method has the following problems:

(1) Terminal equipment needs to be switched in AP and STA mode. During the configuration, the terminal device needs to be set to the AP mode. After the configuration is completed, the switch to the STA mode is tedious.

(2) The terminal devices that need to be configured need to be connected one by one and configured sequentially. In the case of a large number of devices, the efficiency is low.

(3) The SSID and password of the terminal device may be changed or forgotten, which makes it difficult to connect successfully in AP mode. Through further research, it is found that when the Wi-Fi module works in the listening mode, it is not necessary for the configuration end to establish a Wi-Fi connection with the terminal device, so that the configuration end can communicate with the terminal device. In the listening mode, the Wi-Fi module can receive all data packets passing through it, regardless of whether the destination MAC address of the data packet is consistent with the MAC address of the Wi-Fi module itself.

(2) Formulation of distribution network agreement

(1) Physical layer protocol

In terms of signal encoding, the destination MAC address field and the data frame length of the controllable 802.11 data frame are used for encoding. The destination MAC address field carries Wi-Fi configuration data, and the data frame length represents the serial number of the configuration data. The serial number of each field starts from 1 and each serial number carries 2 Bytes of user data. The device side parses the encoded data with the serial number of the data frame to obtain the SSID and password of the wireless network access point and other configuration data.

Because the wireless network environment in which the device is located may be extremely complicated, it is likely that there are multiple AP in the same space, but these AP are distributed on the same or different channels. The receiver of the message does not know which channel to send the message from 1–14, there may be other devices sending UDP multicast packets on the same channel. In this case, the data packets monitored by the receiver are massive and must be obtained from the massive data information to find the channel on which the sender is located. In addition, during the transmission of UDP multicast data packets, the data packets at the transport layer must be encapsulated in the network layer and the data link layer, and then sent after being encrypted, so the length of the UDP multicast data packets sent by the sender. There is a difference between the length of the data frame monitored by the receiver and this needs to be escaped.

In order to solve these two problems, before sending link layer data, it is necessary to send a 20-frame preamble field. The destination MAC address of the preamble field is fixed to 0x01-00-5E-76-00-00, and the data frame length is fixed to 1. After receiving the leading domain data packet, the receiver locks on the current channel to continue receiving other data sent by the sender, and uses the length of the received data frame to subtract 1 to obtain this length difference.

(2) Link layer protocol

The data structure of the link layer is mainly composed of two fields: magic code and data code. The data code is divided into ap_field and extra_field. Among them, ap_field contains the SSID and password information of the wireless network access point by the ssid field and password field. Carry other information configured by the user (for example, information with a small amount of data such as authentication information). All fields are coded with 23 high-order bits and 7 high-order bits to indicate the field type, and the low 16 bits are user-configured data information. In order to prevent the failure of the distribution network information caused by packet loss, the sender of the information is set to send 20 frames of magic code, and all data code field information is sent 15 times in a loop.

2.4. Terminal equipment communication method

In the "Internet + end" structure of the IoT system, terminal devices distributed in different wide-area spaces are connected to the cloud server, and end-to-end data interaction is achieved by means of the cloud server. Therefore, in the research of communication methods for IoT terminal equipment, it is necessary to ensure that the terminal equipment can securely access the cloud server and establish communication between the device and the cloud server. Finally, through the cloud server, a pair of devices and devices one, one-to-many, and many-to-many binding relationships to achieve flexible communication between devices. In the communication process, it is also necessary to ensure the real-time and reliability of the communication.

(1) Cloud platform access for terminal equipment

The access to the cloud platform of the terminal equipment is a necessary prerequisite to realize the integrated and unified management of the equipment by the cloud platform, the real-time and reliable remote control and monitoring of the equipment to the equipment, and the sharing of information between equipments. In order to prevent illegal device access, the legitimacy of the access device must be verified. Therefore, a secure access verification method needs to be researched and designed. The unique key of the device is written into the device before leaving the factory. The key is used to authenticate the device to determine that the device is a legitimate device.

(1) The cloud platform access method is designed in the Internet of Things system. Due to the complexity and variety of terminal equipment, and the different functional requirements and targeted user groups in different projects, in order to facilitate the management of IoT terminal equipment, "products" are defined. The concepts of "device"

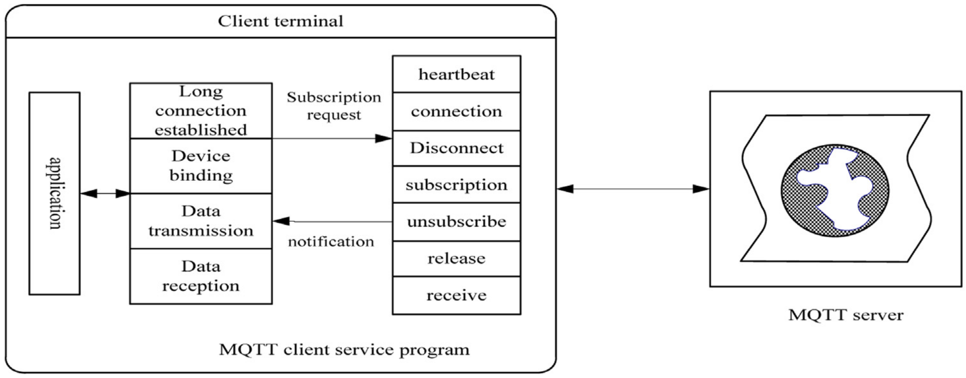


Fig. 3. Message service mechanism of MQTT protocol.

and "device" are abstract descriptions of terminal devices. "Device" refers to a specific terminal device, and "product" is a collective term for a class of terminal devices. It can also be understood as "project" or "system". A product can contain multiple devices, and each device can belong to only one product.

(2) HTTP defines 8 methods such as GET, POST, PUT, DELETE to instruct the desired action to be performed on the identified resource. The most commonly used methods are the GET and POST methods. The GET method is used to request data from a specified resource. For submitting the data to be processed to the specified resource, POST is generally used when transmitting a large amount of data. In this article, the HTTP protocol needs to be used to complete some simple data interactions, and the cloud platform's access information request is completed by the GET method.

(2) Establishment of communication between the device and the cloud server

The MQTT client service program establishes a connection with the MQTT server, subscribes to topics according to the needs of the application, and when it receives the message pushed by the server, it performs preliminary processing before sending the message to the corresponding application for processing. The MQTT client service program can also receive the application's message sending request, encapsulate the application data in the MQTT message format, and send the message to the MQTT server, which then forwards the message to other clients. The message service mechanism of the MQTT protocol is shown in Fig. 3:

3. Experiments

3.1. Data collection

This article studies the network access and communication methods of the IoT terminal equipment. In order to verify the feasibility of the proposed method, a system test platform is built, which mainly includes user APP, cloud platform and 4 terminal equipment. The four terminal devices are named test01, test02, test03, and test04. The data in this article mainly comes from the operation of these four terminal devices on the APP.

3.2. Experimental environment

In view of the security and stability, cost savings, and reliable performance of the cloud platform, Alibaba Cloud was selected as the operating platform for the program. On the Alibaba Cloud, the Windows 2008 32-bit operating system, 2G memory, and 1M broadband were purchased on the Alibaba Cloud. And set the relevant variables according to the requirements of the development environment. The APP in this article uses Java language and is developed on eclipse development tools.

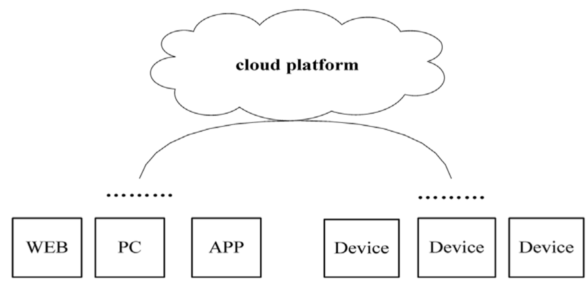


Fig. 4. Overall system architecture.

3.3. System design

The IoT system designed in this article adopts a "cloud + end" structure. The system includes three parts: cloud platform, device end, and user end. The device establishes a connection with the cloud server to form a communicable network, and implements cloud server forwarding and routing. User to terminal equipment and data interaction between terminal equipment. The overall system architecture is shown in Fig. 4:

The cloud platform mainly completes the management of users and equipment to achieve the cloud platform access of the terminal. The cloud platform deploys rich functional components to provide comprehensive services for the IoT system to meet various application needs: designing RESTFUL API to provide access to application services for the terminal; deploying an MQTT server based on the "publish/subscribe" model, between devices and users 3. Establish a real-time stable communication service between devices. Set up a MongoDB non-relational database to store heterogeneous data from users and devices, and provide a data foundation for big data analysis and calculation.

The user terminal mainly performs user functions such as remote control of the device, historical data query and statistics, fault query and diagnosis, and device parameter settings to meet the user's different management and control requirements for the control system in different time periods and different regions.

The device side includes both sensors and actuators that have the ability to directly connect to the cloud platform and can directly communicate with the cloud platform. It also includes the data collected by each sensing node and then uploads it to the cloud platform, and receive the intelligent gateway sent to the underlying device under the cloud platform remote command.

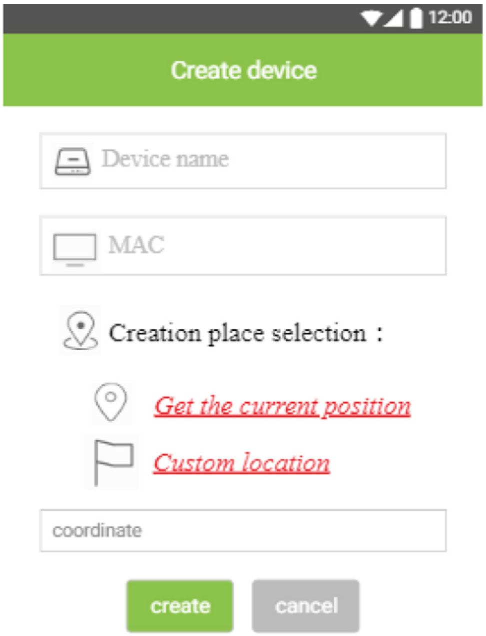
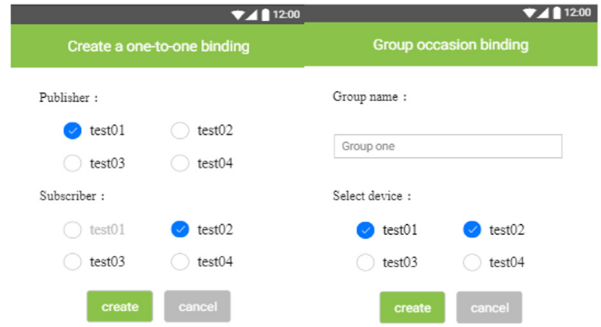


Fig. 5. Device registration.



(a) Single occasion binding (b) Group occasion binding

Fig. 6. Device binding.

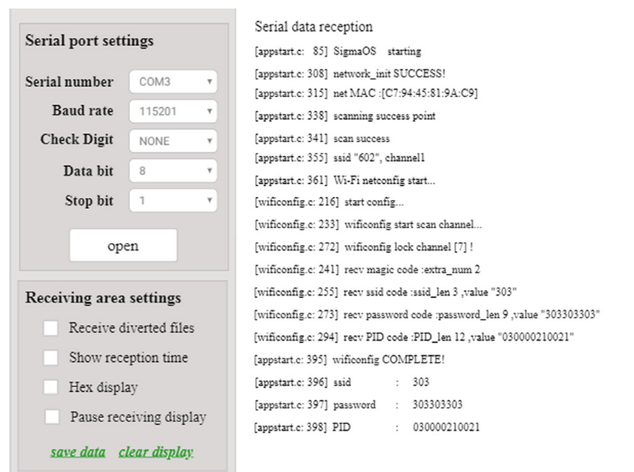


Fig. 7. Information output result of Wi-Fi access terminal equipment.

4. Discussion

4.1. Device registration and binding

(1) Device registration module

The user APP is mainly used to assist the implementation of the network access and communication functions of the terminal device. In the device registration module, the user can add basic information about the device, including device name, MAC address, device positioning and other attributes. Then click the "Save" button. When the device information is saved to the database, an identifier will be generated in the database to ensure the uniqueness of the device. However, in this module, the device is not networked, which means that communication functions cannot be used. Device registration is shown in Fig. 5:

(2) Equipment binding module

In the device binding module, the APP is divided into three different binding modes: single occasion binding, group occasion binding, and complex occasion binding. A single occasion is bound to the message publisher and subscriber can only select one device to communicate with each other; a group occasion is bound to group multiple devices into a custom group and then communicate within the group; a complex occasion is bound to the message publisher and the number of subscriber devices is one or more, and the number is not fixed. Single occasion binding and group occasion binding are shown in Fig. 6:

4.2. Analysis of Wi-Fi access test results of terminal equipment

(1) Analysis of functional test results of Wi-Fi access configuration methods

First initialize the Wi-Fi module, obtain the MAC address of the Wi-Fi module (using this MAC address as the MAC address of the terminal device), and then obtain the wireless network access point information from Flash. When the acquisition fails, enter the network distribution process and set the Wi-Fi module works in the listening mode, gets wireless network data packets and parses them. After the network is successfully configured, set the Wi-Fi module to work in station mode, scan the wireless network access point according to the ssid, obtain information such as its encryption method, and connect to the wireless network access point according to the ssid, password, and encryption method for subsequent network communications, prepare for the subsequent network communication service. The output result of Wi-Fi access terminal equipment information is shown in Fig. 7:

(2) Performance test of Wi-Fi access configuration method

In order to test the efficiency of the configuration method of Wi-Fi access of the terminal equipment designed in this paper, the distribution time of the transmitted information is 10 bytes, 30 bytes, 50 bytes, and 70 bytes. It can be seen that the configuration method of Wi-Fi access of the IoT terminal equipment designed in this paper has a high success rate, and the configuration success rate can reach 100% in all four groups of tests. And it has low time consumption, the average time is only 0.7692 s at 10 bytes, and the average time is 4.8319 s at 70 bytes, which greatly reduces the distribution time, improves the distribution efficiency, and can meet the needs of fast and stable distribution. At the same time, the distribution network protocol is simple and easy to implement, and the user operation is simple and convenient, which improves the user experience. The performance test results of the Wi-Fi access configuration method are shown in Table 3 and Fig. 8:

Table 3
Test results of Wi-Fi access configuration methods.

Bytes	Average time	Shortest time	Longest time	Success rate
10	0.6692	0.457	0.842	100%
30	1.3546	1.212	2.320	100%
50	2.8600	2.115	3.486	100%
70	4.7319	2.116	8.848	100%

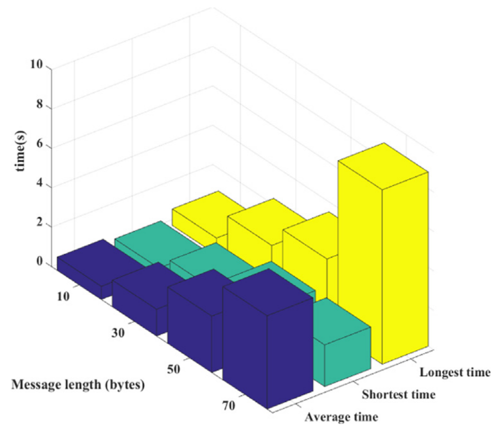


Fig. 8. Performance test results of Wi-Fi access configuration method.

5. Conclusions

(1) This paper studies the cloud platform access method for IoT terminal equipment. A scheme is proposed in which the device domain name accesses the cloud platform to complete the identity authentication of the device, and then accesses the MQTT proxy server according to the authentication information. Deeply study the data format of the HTTP protocol, implement an HTTP client on the terminal device, and provide a request interface for the cloud platform access of the terminal device.

(2) This article analyzes the Wi-Fi access configuration method's network distribution scheme and coding method. In order to make the device's network access more convenient, fast, efficient, and low cost, a UDP multicast address and data length are designed. Coding network distribution method, and formulated a specific coding protocol, completed the specific implementation on the configuration tool and terminal equipment.

(3) This article builds a system test platform and completes the function and performance tests of the terminal device's network access configuration method. The results show that the network access method and communication method of the terminal equipment proposed in this paper are reasonable and feasible, and can meet the communication needs of the Internet of Things system.

Declaration of competing 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.

CRediT authorship contribution statement

Xiangtao Liu: Conceptualization. **Tianle Zhang:** Methodology. **Ning Hu:** Funding acquisition. **Peng Zhang:** Software. **Yu Zhang:** Resources.

Acknowledgments

This work is supported in part by the Guangdong Province Key Research and Development Plan, China (No. 2019B010137004), the Beijing Municipal Natural Science Foundation, China (No. 4172006), the National Natural Science Foundation of China (61976064, 61871140, 61572153, U1636215, 61572492, 61672020, 61602474, 61602467, 61702552) and the National Key research and Development Plan (Grant No. 2018YFB0803504).

References

[1] Jin Li, Min Zhang, Danshi Wang, Joint atmospheric turbulence detection and adaptive demodulation technique using the CNN for the OAM-FSO communication, Opt. Express 26 (8) (2018) 10494.

[2] Wan Du, Zhenjiang Li, Jansen Christian Liando, From rateless to distanceless: Enabling sparse sensor network deployment in large areas, IEEE/ACM Trans. Netw. 24 (4) (2015) 1.

[3] Ruslan Kirichek, Alexander Paramonov, Andrei Vladyko, Implementation of the communication network for the multi-agent robotic systems, Int. J. Embedded Real-Time Commun. Syst. 7 (1) (2016) 48–63.

[4] Dmitry G. Korzun, Ilya Nikolaevskiy, Andrei Gurtov, Service intelligence and communication security for ambient assisted living, Int. J. Embedded Real-Time Commun. Syst. 6 (1) (2015) 76–100.

[5] Davide Bertozzi, Giorgos Dimitrakopoulos, José Flich, The fast evolving landscape of on-chip communication, Des. Autom. Embedded Syst. 19 (1–2) (2015) 59–76.

[6] Meng Li, F. Richard Yu, Pengbo Si, Green machine-to-machine communications with mobile edge computing and wireless network virtualization, IEEE Commun. Mag. 56 (5) (2018) 148–154.

[7] H. Wang, D. Xiong, P. Wang, et al., A lightweight XMPP publish/subscribe scheme for resource-constrained IoT devices, IEEE Access 5 (99) (2017) 16393–16405.

[8] Michael W. Condry, Catherine Blackadar Nelson, Using smart edge IoT devices for safer, rapid response with industry IoT control operations, Proc. IEEE 104 (5) (2016) 1–9.

[9] M.P. Gopinath, G.S. Tamizh Arasi, L. Kavisankar, R. Sathyaraj, S. Karthi, S.L. Aarthy, Balamurugan Balusamy, A secure cloud-based solution for real-time monitoring and management of internet of underwater things (IOUT), Neural Comput. Appl. 31 (S-1) (2019) 293–308.

[10] Said El Kafhali, Khaled Salah, Efficient and dynamic scaling of fog nodes for IoT devices, J. Supercomput. 73 (12) (2017) 5261–5284.

[11] Hichem Sedjelmaci, Sidi Mohamed Senouci, Tarik Taleb, An accurate security game for low-resource IoT devices, IEEE Trans. Veh. Technol. 66 (10) (2017) 9381–9393.

[12] A. Mirhoseini, B.D. Rouhani, E. Songhori, et al., Chime: Checkpointing long computations on interm ittently energized IoT devices, IEEE Trans. Multi-Scale Comput. Syst. 2 (4) (2017) 277–290.

[13] Minseok Lee, Seunghyeok June, Sehwan Kim, Developing a compact multiple laser diode combiner with a single fiber stub output for handheld IoT devices, J. Korean Phys. Soc. 72 (1) (2018) 71–78.

[14] M. Kodialam, T.V. Lakshman, S. Sengupta, Traffic-oblivious routing for guaranteed bandwidth performance, Commun. Mag. IEEE 45 (4) (2017) 46–51.

[15] F.B. Zarrabi, Z. Mansouri, N.P. Gandji, et al., Triple-notch UWB monopole antenna with fractal koch and T-shaped stub, AEU - Int. J. Electron. Commun. 70 (1) (2016) 64–69.

[16] Frank Barnes, Ben Greenenbaum, Some effects of weak magnetic fields on biological systems: RF fields can change radical concentrations and cancer cell growth rates, IEEE Power Electron. Mag. 3 (1) (2016) 60–68.

[17] Begum Korunur Engiz, Cetin Kurnaz, Long-term electromagnetic field measurement and assessment for a shopping mall, Radiat. Prot. Dosim. 175 (3) (2017) 321–329.

[18] T. Suiyan, M.A. Xu, D. Wenhao, et al., Design of rice nursery tray images wireless transmission system based on embedded machine vision, Trans. Chin. Soc. Agric. Mach. 48 (4) (2017) 22–28.

[19] L.Y. Yeh, P.Y. Chiang, Y.L. Tsai, et al., Cloud-based fine-grained health information access control framework for lightweight IoT devices with dynamic auditing and attribute revocation, IEEE Trans. Cloud Comput. 6 (2) (2018) 532–544.

[20] Y.-J. Zhang, Z. Li, Q. Liu, Design and implementation of remote monitoring system for high frequency vibrator, Chung-kuo Tsao Chih/China Pulp Pap. 37 (12) (2018) 51–55.

[21] Fei Xiong, Aijing Li, Hai Wang, An SDN-MQTT based communication system for battlefield UAV swarms, IEEE Commun. Mag. 57 (8) (2019) 41–47.

[22] Youn-Sik Hong, Jae-Ho Lee, An improvement of energy consumption efficiency for MQTT-SN using transmission scheduling and variable period of keep-alive, Adv. Sci. Lett. 23 (10) (2017) 9634–9638.

[23] August Betzler, Carles Gomez, Ilker Demirkol, CoAP congestion control for the internet of things, IEEE Commun. Mag. 54 (7) (2016) 154–160.

[24] Lina Yao, Quan Z. Sheng, Schahram Dustdar, Web-based management of the internet of things, IEEE Internet Comput. 19 (4) (2015) 60–67.

[25] Keshav Sood, Shui Yu, Yong Xiang, Software defined wireless networking opportunities and challenges for internet of things: A review, IEEE Internet Things J. 3 (4) (2015) 453–463.

Xiangtao Liu was born in Loudi, Hunan, P.R. China In 1977. He received the Ph.D degree from Institute of Computing Technology, Chinese Academy of Sciences. Now, he works as an associate professor in Cyberspace Institute of Advanced Technology, Guangzhou university, His research interests include artificial intelligence, Internet of things security, cloud computing and data mining. E-mail: liuxt@gzhu.edu.cn.

Tianle Zhang was born in Zibo, Shandong, P.R. China, in 1977. He received the Ph.D degree from Institute of Computing Technology, Chinese Academy of Sciences. Now, he works as a professor in Cyberspace Institute of Advanced Technology, Guangzhou University. His research interests include Internet of things security, network routing and modeling. E-mail: tlezhang@gzhu.edu.cn.

Ning Hu was born in Changsha, Hunan, P.R. China, in 1972. He received the Ph.D. degree from the National University of Defense Technology (NUDT), China. He is currently a Professor of the Cyberspace Institute of Advanced Technology, Guangzhou University. He has published over 30 papers in journals and conferences. His current research interests include artificial intelligence safety and security. He has also achieved the Second Class Prize of the Chinese State Scientific and Technological Progress Award. E-mail: huning@gzhu.edu.cn.

Peng Zhang was born in Anhui, P.R. China, in 1984. He received the Ph.D degree in the area of service computing from University of Chinese Academy of Sciences, P.R. China, in 2013. Now, he is an associate professor in the National Engineering Laboratory for Information Security Technologies, Institute of Information Engineering, Chinese Academy of Sciences. His research interest includes streaming data mining, computational intelligence, information security and big data analysis. E-mail: pengzhang@iie.ac.cn.

Yu Zhang was born in Nanchong, Sichuan, P.R. China in 1996. He received the bachelor's degree from Southwest Jiaotong University, P.R. China. Now, he studies in Cyberspace Institute of Advanced Technology, Guangzhou University. His research interests include Internet of things, facility location and deep learning. E-mail: 2111806072@e.gzhu.edu.cn.