INTELLIGENT IDENTITY AUTHORIZATION SYSTEM DESIGN BASED ON WSN AND CLOUD PLATFORM

Xin XIONG[1], Shang ZHANG[1,*], ShenTao WANG[1], Joe CRAWFORD[1]

Against the traditional mechanical entrance guard system which is not easy to control centrally, and the electronic entrance guard based on CAN bus which is difficult to deploy, the design scheme of an WSN based entrance guard is proposed. This paper shows the effort on work to propose a smart phone access control system scheme based on QR code hybrid encryption technology and WSN, which integrate different stand-alone identity systems in one platform to achieve better security and convenience. The hardware terminals utilize the ZigBee network to interact with control platform and transmit data through the simplified IPv6 protocol stack to build the entire transmission network, with the advantages of real time response, low power consumption and high reliability, which make users to enjoy secure and convenient experience of authentication. The system consists of the distributed electronic lock, main controller and upper units.

Keywords: intelligent identification; IOT; access control

1. Introduction

Today, the Internet of Things (IOT) has received extensive attention and the security awareness of people has increased. The traditional way of access control system which use keys and RFID cards is obviously not enough to satisfy the increasing demand of the users, who need secure and real time respond method which should utilize the mobile app to replace carrying ID cards. At the same time, most popular access control system are stand-alone system, that means they would not benefit from advantages of cloud computing and IOT. Users need to duplicate their ID information in different system and formats.

With the advantages of low cost, large capacity and high reliability, two-dimensional barcode has been widely used [1]. As one of them, QR barcode also share the characteristics of large density, small size, fast recognition and Chinese character encoding. QR barcode had been applied in a variety of areas such as warehouse management, e-commerce, data storage [2]. QR barcode are usually decoded by smart phones and personal computers, rather than terminals which are based on embedded systems. In order to extend the application of QR barcode in

[1] Computer and Information Engineering College China Three Gorges University, Yi Chang, Hubei Province, China, 443002
* Corresponding Author: wetoo@163.com

the field of the Internet of Things (IOT), the terminals which could decode QR barcode are important.

Wireless sensor network as a carrier of data had attracted great attention in recent years along with the development of IOT technology. In order to create intelligent wireless sensor network, the sensor node with high performance and ability of connection is essential. If the wireless sensor network could be connected to the TCP/IP network, the data collected by sensor would be transmitted to the cloud server for processing. To communicate with the IPv6 network, the WSN needs to extend the IPv4 network to IPv6 [3].

With the development of intelligent identity-authorization and authentication system, the new generation of accessing control system could be developed in a concise, efficient and unified direction. This kind of system could meet the personal need of various fields which are committed to solving the tedious, inefficient, low security, isolated problems in the traditional system [4].

Based on cloud computing platform with low-cost hardware infrastructure, individuals in different fields of identity authentication system could be managed through one database, in order that the authentication and authorization process become safe and convenient.

2. Brief of Key Technology

The design in this paper utilizes real-time dynamic QR barcode, which could ensure the security of customer information. It will bring efficiency, uniformity and convenience to the greatest extent, which give greater space for the development of identification system.

This system also utilizes the Wireless Sensor Network technology to make full use of the advantages of the wireless network to create a mode in which software and hardware could be interactive, thus to achieve a unified identity authentication system [5].

2.1 Authentication of user

MD5 code is used as the basis for data fingerprint comparison. At the same time, it can also be used for digital signature.

To verify user identity, this design uses the method of generate text summary which contains data and key.

During verification, the system uses the data and key to generate the secondary information summary, and matche the text according to the information summary of the data and the secondary information summary. Data matched by summary can be regarded as data published by the system. In the system, the user's password needs not to be stored directly, but the result calculated by MD5 or similar algorithm based on the password is stored [6].

When the user enters the username and password to perform the login operation, the system will calculate the MD5 value of the password input and query the MD5 value of the corresponding password in the system through the username.

The system determines whether the user name and password matched by comparing the MD5 values of two.

The database of system can also need to determine whether the user submit for authentication has a legitimate identity without saving the user's password [7].

At the same time, the administrator or hacker cannot calculate the user's password from the saving data in the database.

As Fig. 1. shows, through the triple identity information authentication of the APP to ensure the effective use and login of the authorized person, it uses the depth detection algorithm to record user behavior, and to find abnormal activity with removing it immediately. Running the information monitoring algorithm through each node will achieve the self-inspection of the system.

With the data analyzing through users' pattern, the system can conduct different working modes to match users' behavior which make the system more intelligent.

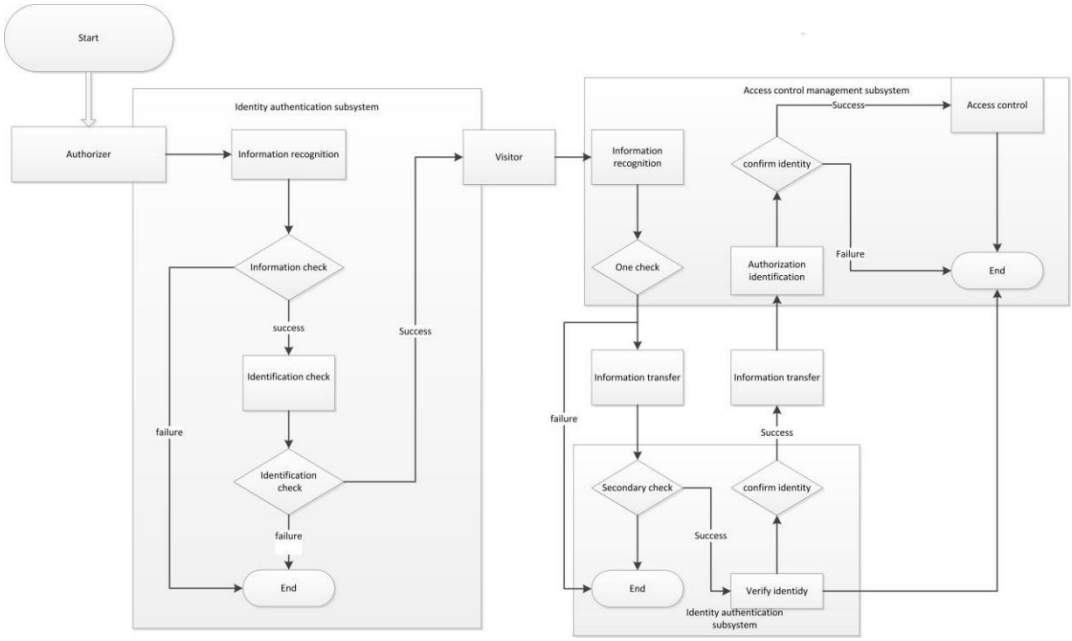

Fig. 1. The working flow of authorization

2.2 QR Barcode

QR code has the characteristics of high coding density and large amount of information.

Depending on the type of information contained, the QR code can contain information of 500 to 2700 characters. Two-dimensional code compared with ordinary bar code would have dozens of times more information capacity. At the same time, it can encapsulate a variety of formats, such as pictures, sounds and other digitized information stored in two-dimensional code, and has different levels of fault tolerance, elastic encryption ability. The reliability of decoding has been greatly improved than one-dimensional code [8].

The use of real-time dynamic QR code, on the basis of fully ensuring the security of customer information to the maximum extent with the convenience, efficiency, unity, to give the identification system a greater space for development. And compared with other access control methods, the QR code has the advantages of low cost and large information storage.

The scheme used in this system has the following characteristics: 1) It uses QR code of the registered user as the identification form, including unique sequence number of mobile phone and regularly converted key as the source of QR code. 2) Dynamic QR barcode generates in the event entering into the APP on mobile and hybrid encryption technologies ensure the timeliness and security of the QR code. 3) QR code generated on mobile phone is scanned by the camera within the lock hardware, and the information in QR code would be sent to the cloud server to verify the user identity [9].

Fig. 2. Example of QR code used in design

2.3 WSN over IPv6

Although many of wireless network solutions such as Bluetooth, Ultra Wide Band (UWB), Wireless Ethernet, and many more, are in the area of home networking, ZigBee, a newly developing protocol for wireless sensor networks based on the IEEE 802.15.4 specification, has become the most attraction technique in the research and commercial domains because of open standard, low-cost, and low power characteristics.

ZigBee network is composed of Reduced Function Device (RFD) node, Full Function Device (FFD) node, coordination node and routing node. A large number of sensor nodes are deployed in or near the monitoring area to form a network through self-organization. Data are transmitted along the sensor nodes links, in which more than one node process the data. Which go through multiple hops posterior to the gathering node, at last reach the management node. Compared with the traditional design, using ZigBee technology reduces the initial cost.

Thus, the system adopt ZigBee node which use CC2530 as the MCU.

In the process of identity authorization, the system use ZigBee network to keep in touch with the cloud server on TCP/IP network in real time, sending the QR code scanned by camera within lock to the server and accepting the authorization respond given back.

The system needs to achieve the seamless and efficient integration of wireless sensor (access control and other terminal hardware) network and IPv6 network.

On the basis of IEEE 802.15.4 standard at the bottom of wireless sensor network protocol stack, this system use the simplification of IPv6 protocol stack [10], which remove unnecessary components and extend functions such as IPv6, ICMPv6, ND, TCP, UDP and other protocols more streamlined, providing the basis for the effective fusion of wireless sensor network and IPv6 [11].

In this work, we have taken ZigBee network as the backbone of our system. We propose a digital door lock based home automation system, which exploits the full capacity of bZigBee sensor network by integrating home security with cloud system.

The identity authorization management are conducted through the IPv6 network and Wireless Personal Area Network (PAN) fusion method. To create the identity authorization system suitable for Intelligence community [12], the design implements the IPv6 network client support and IPv6 routing protocol applicable to wireless sensor network and other key technologies. The system itself can recognize not only the registered users by scanning the two-dimensional code, but also the non-registered users who had booked in earlier time.

Through mobile phones and other mobile terminals, the system achieves a variety of occasions of functions to provide identity authorization and authentication information in the network, which provide support for other public service systems.

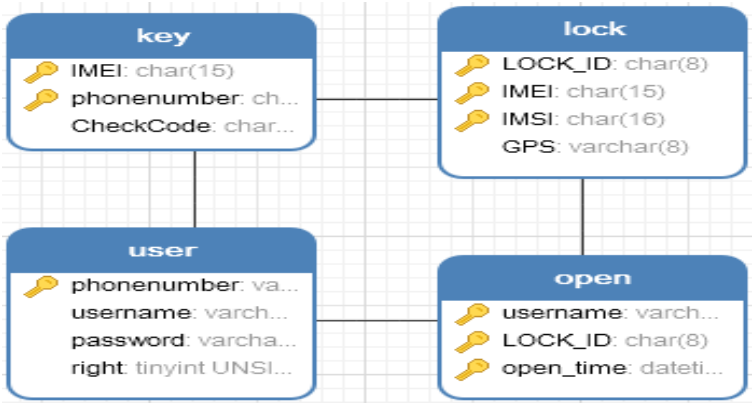

Fig. 3. The data schema of the design

3. Design of System

In our proposed system, a ZigBee module is embedded in digital door lock and the door lock acts as the central main controller of the entire system.

We use the term ZigBee module to refer to the communication module in ZigBee and sensor node to refer to the integrated node consisting of ZigBee module, sensors, actuators, and other supplementary circuits.

The system was designed into three parts: User management program on PC, cloud platform with database (As shown in Fig. 3), a network of sensor nodes with digital door lock as sink node. As shown in Fig. 4, the user open the client APP software, apply to the cloud platform for authentication via the network, the authenticated user information which in form of QR code data would be sent through the clouds. By scanning QR code the host would get the lock information and report the unlock information to the cloud server. If the QR code verification is confirmed, the host would immediately send the data to the cloud server for recording, otherwise it would be prompted to fail. After several failures, the host will send alarm signal to the cloud server.

After that the access control systems have been greatly improved in safety, timeliness, convenience, and intelligent.

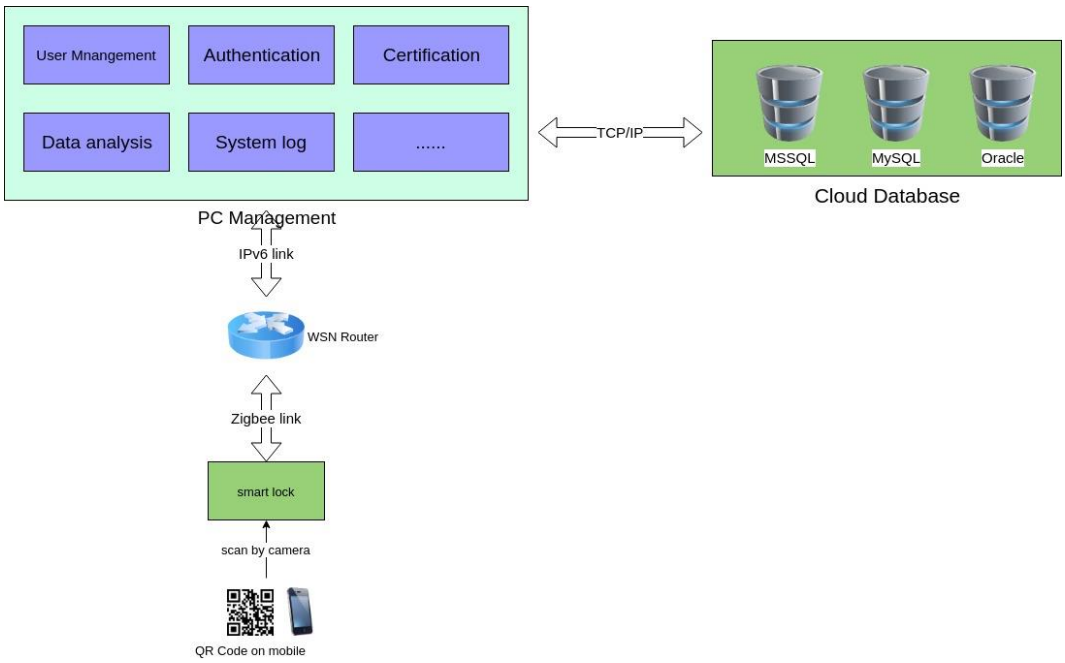

Fig. 4. The design of system

3.1 ZigBee over IPv6

The ZigBee system has the feature of low power consumption. In order to send the data collected by Smart Lock over the internet, especially the IPv6 network, here the design introduce a border router to exchange the packages between WSN and IPV6 network. Data transfer module is inserted between 6LoWPAN boundary node and IPv6 network server. And IPv6 packages are repacked by using the tunnel technology. First of all, the design use the transition technology of IPv4 to IPv6, analysis and compare the traditional methods which are based on Dual stack, Translation mechanism, and Tunnel mechanism. Comparing advantages and disadvantages of these three kinds of method, and their applicability in WSN with low rate transition and low power consumption, the design take Contiki micro operating system and TI-RTOS embedded real-time operating system as the foundation.

Secondly, the design propose a scheme based on IPv6 for network boundary router, it includes: 6LoWPAN boundary node, IPv4 data repeater and IPv6 network access server.6LoWPAN boundary node use Contiki operating system which based on TI's chip CC2530.The boundary node communicate with data repeater through the SLIP protocol, and responsible for header compression and decompression.TheIPv4 data repeater based on STM32F4 platform, which

achieve the communication between network port and serial port on TI-RTOS operating system. ·

IPv6 network server is responsible for the realization of the TUN/TAP tunnel in the Linux operating system, which conduct virtual communication between IPv4 network card and IPv4 data repeater based on TCP/IP protocol. ·

Finally, the deployment and experiment shows that the proposed Network border router based on IPv6 achieve the expected function. ·

3.2 Hardware of the lock

The smart digital door lock system can be divided into five parts: the control module, the motor module, the sensor module, the communication module and the I/O module. The control module consists of MCU embedded in the digital door lock, which is the brain of the system. The locking operation is controlled by the motor module. The communication module is for communication between devices and the control module. The user can access to the door lock system through I/O module. The I/O module includes QR code scanner and digital dialpad for authentication, TFT Touch LCD for controlling individual device and displaying the relevant information.

The control module contains STM32F4 MCU, Zigbee module A, and the locking end includes: mechanical body of the lock and Zigbee module B. As shown in Fig. 5, the control module sends the AT signal which input by the user through communication module Zigbee Module A, then the slave communication module Zigbee Module B receives the AT signal sent by A [13].

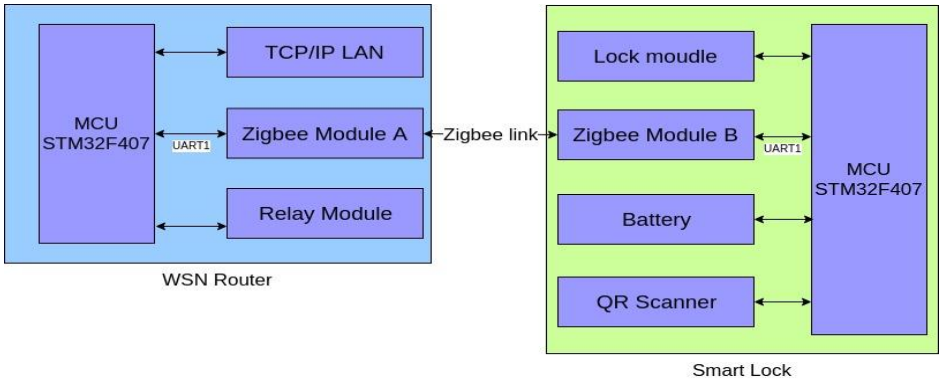

Fig. 5. The hardware of the lock structure

When the valid users need to open the door, the server send the unlock instruction to the node which including STM32F407 as MCU, which will send the signal to the main communication Zigbee module A through UART1, then, the unlock signal goes through A to the slave Zigbee module B, After received the

signal sent by A, B the lock would be open, which through the control MCU inside the lock to conduct the action.

4. Conclusion

The performance of the access control system was improved, and the cost of the access control was reduced by the method of using ZigBee technology compound of IPv6 to build the transmission network.

The shard packet of transmission in different network protocol stack adapter layers should be restructured, through header compressing, and adopting the multistage cache IEEE802.15.4 standard and IPv6 network connection to a seamless and efficient wireless sensor network (WSN).

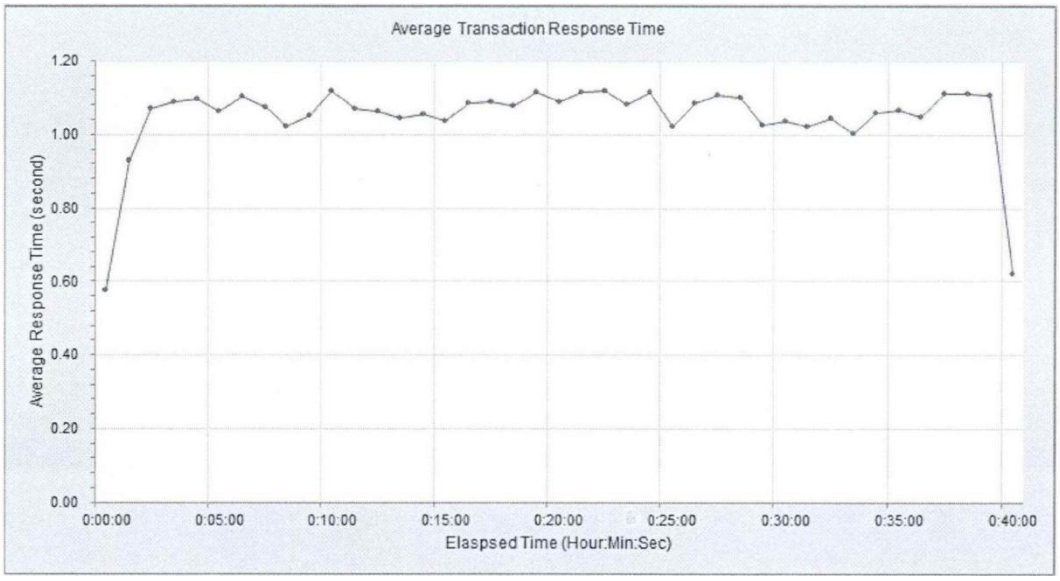

Fig. 6. Average transaction response time

During the field test, the two subsystems are deployed in two small server computers and connected to the local area network of the campus. This test mainly uses the LoadRunner load test tool, which created 100 virtual users to test, the test time is about 40 minutes. In order to ensure that the test can be carried out smoothly, the validity period of identification certificate is temporarily set to one hour. The average response time test results are shown in Figure 6.Test results of transaction execution data per minute of the system are shown in Figure 7.

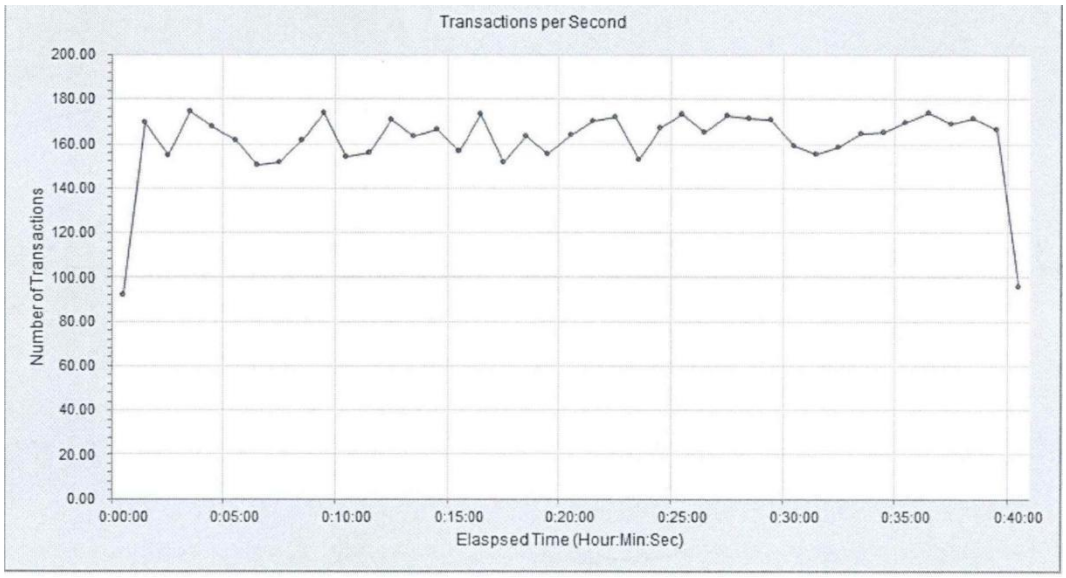

Fig. 7. The Number of transactions per minute

Big data technology which collect and analysis user identity authorization and authentication behaviors also could be implemented by using IPv6 network address and other features, such as real-time tracking and monitoring of user behaviors which visual processing can be carried out, so as to implement the interconnection between people and equipment.

The user identity authorization and authentication behavior data collected by the system could provide data support for the later application systems such as library, museum and other places identity authentication, service reservation and other application systems.

This system connects the traditional decentralized and independent access control system and devices through wireless sensor network and IPv6 network to the centers on the cloud computing platform. Users can obtain flexible and fast identity authorization and authentication experience in various application scenarios through mobile terminal devices.

Acknowledgements

This paper is supported by the CERNET through Project "NGII20161210". and Project "Z2018193/A18-302-a13".

This paper is sponsored by Research Fund for Excellent Dissertation of China Three Gorges University.

REFERENCES

[1]. F. Xu, “QR Codes and library biliographic records”, VINE, **vol. 44**, no. 3, 2014, pp. 345-356.

[2]. S. Sugawara, S. Ishikawa, “Two-dimensional code encryption program, system, and method”, JP20061294482007—22.

[3]. S. Kalwar, N. Bohra, A. Memon, “A survey of transition mechanisms from IPv4 to IPv6 Simulated test bed and analysis”, Third International Conference on Digital Information, Networking, and Wireless Communications, 2015, pp. 30-34.

[4]. F. L. Zucatto, C.A. Biscassi, F. Monsignore, F. Fidelix, S. Coutinho, and M. L. Rocha, "ZigBee for Building Control Wireless Sensor Networks," in proceeding of Microwave and Optoelectronics Conference, pp. 511-515, Oct. 2007.

[5]. S.T. Pushpendra, S. Maneesh, “Result Analysis and Benefits of Detecting Replicate Documents Using MD5 Hash Function”, International Journal of Advanced Computer Research, **vol. 1**, no. 2, 2011, pp. 21-26.

[6]. S. Zhang, M. Xiao, F. Liu, “An Ehanced Microkernel for the design of Location Based Services (LBS) Using Free Open Source Software(FOSS)”, International Journal of Simulation: Systems, Science and Technology, Dec. 2016, pp. 363.

[6]. S. Zhang, T. Xing, “Open WSN indoor localization platform design, Proceedings - 2013 2nd International Symposium on Instrumentation and Measurement”, Sensor Network and Automation, IMSNA 2013, 2013, pp. 845-848.

[7]. S. Zhang, T. Xing, “RSSI Enhanced indoor LBS platform design”, Computer Modelling and New Technologies, **vol. 18**, no. 3, 2014, pp. 170-173.

[8]. S. Zhang, “Cloud Enhanced Microkernel-based LBS platform”, Journal of Residuals Science&Technology, Dec. 2016, pp. 254.

[9]. O. Troan, B. Carpenter, “Deprecating the Anycast Prefix for 6to4 Relay Routers”, 2015.

[10]. E. Nordmark, R. Gilligan, “Basic transition mechanisms for IPv6 hosts and routers”, 2005.

[11]. T. Xing, S. Zhang, F. Zhang, “Microkernel and Middle-Ware Based GIS Platform Design”, Journal of Positioning, May. 2014, pp. 53.

[12]. S. Zhang, “OSGIS and Cloud in LBS Design”, Journal of Residuals Science&Technology, Dec. 2016, pp. 320.
[13]. A. Brandt, J. Buron, “Transmission of IPv6 Packets over ITU-T G. 9959 Networks”, 2015.