



# The Open Electrical & Electronic Engineering Journal

Content list available at: [www.benthamopen.com/TOEEJ/](http://www.benthamopen.com/TOEEJ/)

DOI: 10.2174/1874129001610010189



## REVIEW ARTICLE

# Wired/Wireless Hybrid Transmission of BACnet Messages

Peizhe Tian\*, Chunwang Li and Yimin Wu

*Building Environment and Energy Application Engineering, Engineering and Art Faculty, Biochemical Engineering College of Beijing Union University, Chaoyang District, Beijing, 100023, China*

Received: February 19, 2016

Revised: September 15, 2016

Accepted: October 20, 2016

**Abstract:** This paper presents a kind of message conversion method between wired/wireless hybrid network, aiming at meeting the encapsulation and transmission application requirements of Building Automation and Control network (BACnet) protocol messages in ZigBee network. It also proposes a kind of compatible frame structure and addressing method which is specific to wired/wireless network hybrid transmission. It discusses a design of BACnet/ZigBee wireless temperature sensor node from the point of software and hardware, and completes node software and hardware design of BACnet/ZigBee wireless temperature sensor by the embedded system Lm3s6911+, and bidirectional parsing, encapsulating, addressing, sending and receiving process between ZigBee messages and BACnet Ethernet messages are realized. This solution also can extend the current transmission and application range of BACnet messages, and provide an effective way to wired/wireless network hybrid transmission of building automation data.

**Keywords:** BACnet, Inter-Connection Mechanism, Node Design, Wired/Wireless Hybrid Network, ZigBee.

## 1. INTRODUCTION

BACnet, a completely open data communication protocol for building automation system networks, was developed by the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE), and it is the only international standard (ISO16484-5-2010) in intelligent buildings field, which has been widely used in engineering. Currently, it mainly uses the wired network in data transmission. However, many applications in buildings, such as some hand held or temporary equipment, scattered equipment located in remote areas, *etc.*, are difficult to transfer data through a wired way, which are the limitations of wired networks. In recent years, with the emergence of wireless network technology based on Bluetooth (IEEE802.15.1), Wi-Fi (IEEE802.11) and ZigBee (IEEE802.15.4) protocols, it provides a new means of data communication for building control fields. ZigBee short-range wireless networking technology for its low power consumption, low cost, self-organizing, secure data transmission and other advantages attracted special attention. How to integrate ZigBee wireless network technology with traditional building control network has become a hot research topic [1, 2].

If it adopts traditional integration way of BACnet/ZigBee gateway to realize the wired and wireless hybrid transmission, the purpose of the basic design idea of BACnet and ZigBee is through data sharing between the two kinds of communication protocol processing tasks to implement the data exchange, namely the client gets the data after the temporary data sharing zone through polling the way to make a request. The BACnet can directly read data from the data sharing area and the corresponding analytic and encapsulation processing to ensure that the correct BACnet and ZigBee protocol mapping.

But there are two problems in this approach, the first is the software and hardware resources occupancy, conversion efficiency of demand data is not high which leads to the decreasing of real time ability; the second is that from the BACnet software or hardware environment, it is unable to directly identify ZigBee devices and leads to the blind area of

\* Address correspondence to this author at the Building Environment and Energy Application Engineering, Engineering and Art Faculty, Biochemical Engineering College of Beijing Union University, Chaoyang District, Beijing, 100023, China; Tel: +86 (10) 6493 0069; E-mail: [peizhetian\\_bec@163.com](mailto:peizhetian_bec@163.com)

ZigBee equipment management. According to the above problem, it presents the wireless and wired hybrid transmission solution, which can implement ZigBee devices with BACnet data transparent transmission between software or hardware and it can be encapsulated into a BACnet and ZigBee devices. It can also be directly support a wide variety of BACnet software or hardware for management or operation functions of ZigBee devices, and the real significance seamless integration can be realized .

**2. SYSTEM COMMUNICATION NETWORK STRUCTURE**

The proposed wireless transmission of BACnet protocol messages based on ZigBee technology uses ZigBee network for the transmission of BACnet messages. As shown in Fig. (1), system communication network structure is comprised of BACnet workstation, BACnet IP router, DDC, BACnet/ZigBee router, ZigBee network coordinator and terminal equipment [3]. BACnet workstation is configuration and central management device of the building automation system; BACnet IP router is used for the interconnection of different BACnet networks; DDC is BACnet’s field controller for field device connection and the implementation of control logic; ZigBee network coordinator is responsible for creating and managing ZigBee networks; BACnet/ZigBee router is for the protocol conversion, which allows other devices to join the network, and provides multi-hop routing and data forwarding; terminal devices do not conduct any network maintenance. ZigBee network can be three kinds of network topology-star, tree and mesh. This paper adopts mesh network structure to ensure fast switching to the other available route in case of certain route’s failure and to adjust data transmission path according to changes in the environment and node status, it can also overcome the problem of multipath transmission interference effectively [4, 5]. This feature makes the ZigBee network be suitable for building automation systems.

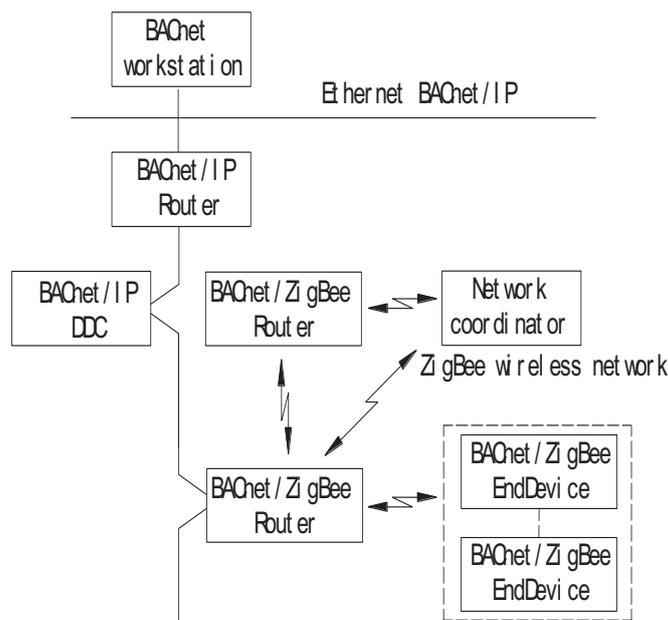


Fig. (1). BACnet/ZigBee communication network structure.

**3. BACNET ETHERNET MESSAGE TRANSMISSION IN ZIGBEE NETWORKS**

**3.1. BACnet Ethernet Protocol Messages Structure**

As shown in Fig. (2), the message of BACnet Ethernet communication protocol consists of six parts: Application Protocol Data Unit (APDU), Network Protocol Data Unit (NPDU), Link Protocol Data Unit (LPDU), Logic Link Control (LLC), X82X82X03 for service access point information and physical layer message is responsible for specific hardware sending/receiving message byte content. NPDU includes Network Protocol Control Information (NPCI) and Network User Data (NUD). As for data messages, NUD portion is APDU [6].

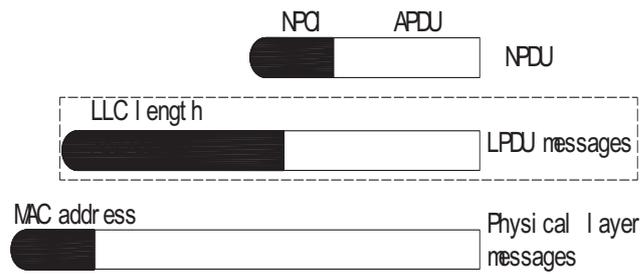


Fig. (2). Message structure of BACnet Ethernet communication protocol.

### 3.2. BACnet Ethernet Messages Encapsulated in a ZigBee Network

The BACnet message transmission scheme on the ZigBee network designed in the paper [7] is complex. As shown in Fig. (3), a virtual link layer BZLL is defined between BACnet network layer and ZigBee protocol stack, the device object instance is taken as BACnet node virtual MAC address (VMAC), meanwhile, VMAC address is also ZigBee generic tunneling cluster protocol address profile. The binding of ZigBee device MAC address with BACnet virtual MAC address will obtain ZigBee network address through MAC address, and then accomplish device addressing and data transmission [8].

Taking into account the uniqueness and invariability of ZigBee device 64 bit MAC address, in order to reduce design complexity, in the paper, MAC address was directly used to identify the device, and then ZigBee network address was obtained *via* MAC address in the communication [9, 10].

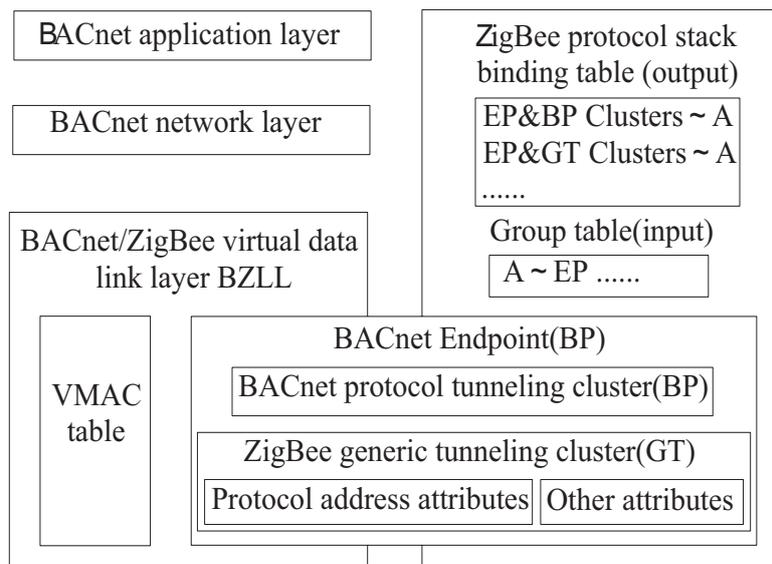


Fig. (3). BACnet/ZigBee interconnection mechanism based on BZLL.

The design for ZigBee network transmission in this paper contains the frame format of BACnet network layer message NPDU as shown in Fig. (4). Here, BACnet network layer message NPDU is served as ZigBee network application layer load. NPDU contains network protocol layer control information NPCI and user data. NPCI has the fixed format and coding, which has 6 parameters related with device address. They are: ① DNET (network number of destination address); ② DLEN (MAC address length of destination address); ③ DADR (MAC address of the destination address); ④ SNET (network number of source address); ⑤ SLEN (MAC address length of source address); ⑥ SADR (MAC address of source address). The encapsulation process is described as follows: firstly, BACnet network layer message NPDU is established by the device user application; then ZigBee application layer are used, network layer and media access control layer functions to form ZigBee frame for communication *via* ZigBee network application layer interface [11], In the encapsulation process, it is required to calculate the length of the user data, and obtain the remote device's MAC address while message error-checking is handled by MAC layer of ZigBee network.

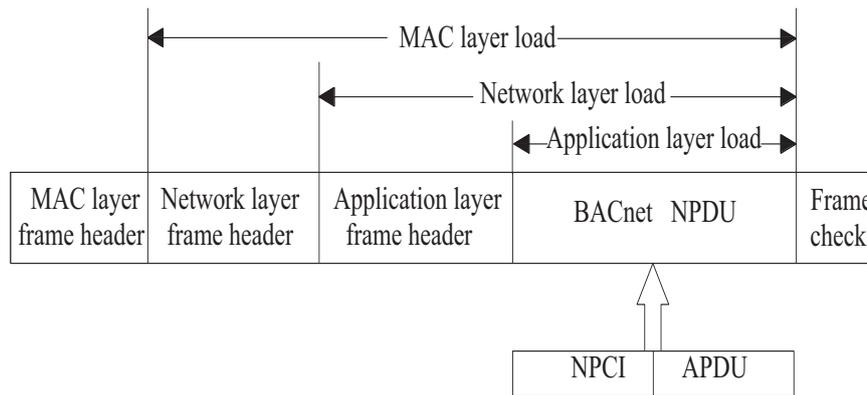


Fig. (4). BACnet protocol message encapsulation in ZigBee network.

### 3.3. Addressing Process Between Devices

The key to achieve addressing between ZigBee devices is how to obtain its ZigBee network address *via* MAC address of the device. The difficulty is that ZigBee network address is assigned dynamically when a device joins the network.

Moreover, it may vary with changes in its location in the network topology. Therefore, maintaining a MAC address of other devices and its corresponding dynamic ZigBee network address list in each device is needed and necessary. When the local device cannot obtain the ZigBee network address of remote device, it will broadcast this ZigBee frame. Only the remote device which has the same message MAC address will respond. Then, the local device can extract remote device ZigBee network address based on the respond and will insert a new item in the list. When the ZigBee network address of the remote device is changed, the local device will not receive any response message from the specified remote device. Then the local device will delete the corresponding item in the list and broadcast this ZigBee frame again.

## 4. BACNET/ZIGBEE TEMPERATURE SENSOR NODES IMPLEMENTATION

### 4.1. Hardware Structure Design

The BACnet/ZigBee temperature sensor's structure in this design includes temperature data acquisition module, data processor module, RF module and power module, as shown in Fig. (5) [12]. Data process module using TI Company's Lm3s6911+ microcontroller implementation is primarily used to achieve I/O channel driver, ZigBee message and BACnet Ethernet message bidirectional parsing and encapsulation calculation, task management, *etc.* Temperature data acquisition module is consisted of NTC, signal conditioning circuit, and A/D converter circuit. After bridging process for NTC (10K), the signal is amplified and filtered by the signal conditioning circuit and then converted into digital value from 12 bit single-channel AD9238 into Lm3s6911+ common interface GPIO. RF module using ZigBee dedicated module CC2420 is used for ZigBee network wireless communication, message exchange control and sending and receiving data. Physical layer and MAC layer functions are implemented by ZigBee chip while network layer functions are accomplished by Z-stack software protocol stack provided by Chipcon company [13]. System power provides a standard 5V and 3.3V power supply for signal conditioning circuit and control unit. Then it is adjusted to 2.75V *via* Lm3s6911+programmable-chip low dropout voltage regulator in order to meet the requirements of the chip.

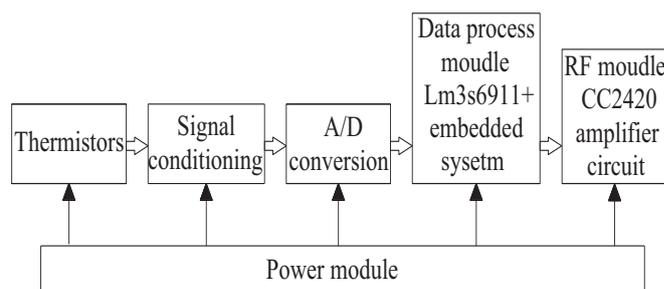


Fig. (5). BACnet/ZigBee node hardware schematic.

## 4.2. Software Design

### 4.2.1. Software Framework and Interconnection Mechanism Implementation

As shown in Fig. (6), the core function of the software is to achieve ZigBee messages and BACnet Ethernet messages bidirectional parsing, encapsulating, addressing, sending and receiving process. The complete message transmission process is as follows: ① The local device encapsulates BACnet protocol messages NPDU into ZigBee frame; ② Get its ZigBee network address based on its MAC address of the remote device, then send ZigBee frame to the specified remote device using Z-Stack protocol AF\_DataRequest function; ③ When the remote device receives the ZigBee frame from the network, it calls afIncoming Data function to parse the data frame and extract NPDU messages; ④ If the MAC address of the message is identical with its own address, it will save the ZigBee network address of the device initiating the request for message processing. Then the generated response messages are encapsulated into ZigBee frame and are sent to the ZigBee network address which is just saved.

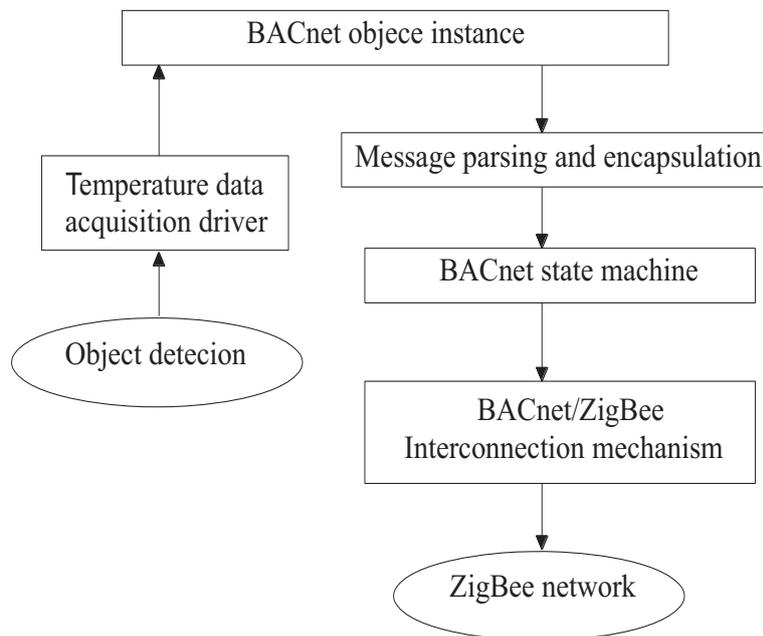


Fig. (6). The basic framework.

In order to realize the above messages' transmission process, the software assigns two separate tasks, *i.e.*, BACnet Ethernet communication protocol processing and ZigBee communication protocol processing. At the same time, synchronous communication mechanism, synchronous transmission device address and data information need to be established between the different tasks. In other words, in addition to complete their separate protocol processing tasks, BACnet communication protocol and ZigBee communication protocol processing tasks are also need to handle collaborative tasks. In order to achieve this function, the "message" mechanism is used in the software design, namely, a "message" label is established for BACnet communication protocol and ZigBee communication protocol processing tasks, respectively, and it is designed to synchronize the relevant information of NPCI segment in the messages of BACnet and ZigBee message address field, and APDU segment of BACnet messages and ZigBee message data segment. In order to achieve multi-tasking capabilities, the software system architecture uses a free open-source embedded operating system ucOSII which has compact, scalable and real-time characteristics [7]. The embedded operating system ucOSII is ported to Lm3s6911+ microcontroller and has its kernel configuration according to the need of protocol converter to achieve the corresponding functions.

### 4.2.2. Temperature Data Acquisition Driver

Temperature data acquisition driver includes A/D driving function, digital zeroing function, mean filtering function. Since NTC is a non-linear sensing element, piecewise interpolation is used to have function approximation split into a number of broken lines or curve approximation based on their changes. After obtaining a sample value R, first determine in which broken line segment the size of R is located, and then the scale conversion value can be calculated

by the linearized equation of the corresponding segment. Similarly, the more the number of segments, the higher the accuracy of linearization, and software overhead is also increased.

4.2.3. The Definition of Object Instance

According to the BACnet standard, as BACnet standard device, temperature sensor must have a device object instance and an analog input object instance. The definition of object model of the smart temperature sensor is listed in Table 1 below [14]:

Table 1. Definition of the object instance model of the sensor.

| Device object     |          | Analog input object |                |
|-------------------|----------|---------------------|----------------|
| Object identifier | Device_1 | Object identifier   | Analog input_1 |
| Object name       | “Temp_1” | Object name         | “B6”           |
| Object type       | Device   | Present value       | null           |
|                   |          | Object type         | Analog input   |
|                   |          | Units               | Celsius degree |

4.2.4. BACnet State Machine TSM Design [15]

BACnet standard services can be divided into two types of services - confirmed services and non-confirmed services [6]. The confirmed service is one-to-one communication, with one party initiating the service request, the other party to make the right response to receipt of the request. State machine TSM is used to describe the state of sender and receiver in the process of communication. This design uses a non-segmented confirm service, so as the state machine can be simplified into two states namely the idle state and waiting for a response state, as shown in Fig. (7).

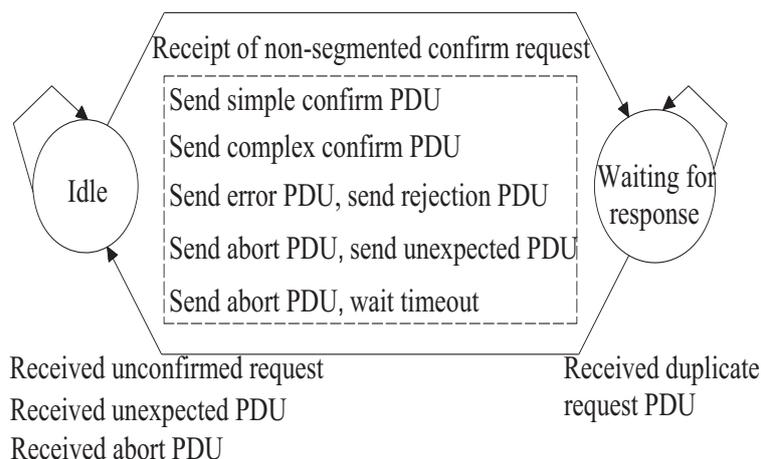


Fig. (7). Service state machine.

In non-segmented confirm service, once the client device makes a request message, the timer starts counting. Upon receipt of the error message, rejected messages, aborted or simply confirmed messages, it will stop the clock and notify the client application. If the time value of the timer exceeds the APDU timeout attribute value of the client device object, then it will resend the confirm request message, with re-timing of the timer. If the number of retransmissions exceeds the required number of the property value of number of APDU retries of the customer terminal equipment and fails to receive proper acknowledgment message, it will discard the resend message and notify client to call request service so that the client application will deal with the messages that cannot be sent.

TSM's program implementation must first define an array of structures, which contains various parameters associated with the service status including invoke ID, retransmission count, request time, destination address, APDU messages etc. Then, define TSM management and state transition function. In TSM program, it manages the entire protocol stack invoke ID's distribution and use. Invoke ID is unique at the service request end, which is used to determine and identify whether a response message is corresponding to the request. In response end it may encounter the same invoke ID from requests of different devices, so the uniqueness of the state machine will be jointly determined by invoke ID and request source address.

#### 4.2.5. Message Encapsulation and Parsing

BACnet ethernet communication protocol message consists of six parts: Application Protocol Data Unit (APDU), Network Protocol Data Unit (NPDU), Link Protocol Data Unit (LPDU), Logic Link Control (LLC), X82X82X03 for service access point information and physical layer message responsible for specific hardware transmitting/receiving message byte content. According to the definition of BACnet standard, a BACnet mark must be added before each encapsulated service data.

In data encapsulation process, the data block containing service information should be processed first. Then have APDU user data marked and encoded according to BACnet standard BACnet ASN.1 definition and service parameter structure. Then it has three parts - stationary application layer control information, network layer control information, and data link layer control information encoded. Parsing is the inverse process of the encapsulation. After receipt of message, the physical layer calls the decoding function of each layer to read the relevant parameters, and make judgments based on parameters.

### 5. EXPERIMENTS

In the experiment, it adopts YD2010 digital electric meter with BACnet/ZigBee communication interface as the equipmental terminal. The YD2010 digital meters is directly encapsulated as BACnet device which has BACnet object attribute. Wireless transmission of BACnet data packets can be realized through the ZigBee network. BACnet client can visit the BACnet device address directly without wasting of resources, and ensure the BACnet device to read real time value.

Fig. (8) is the result of the query response speed adopted the logic analyzer, white block information is the electric meter reply byte. It can be seen that the response of the content itself needs about 100 ms delivery time. White black time interval between data block length and the white block length of time is the time interval of sending query commands for the software, which is about 200 ms or so. The speed of query all power value of five meters within one second can be reached. If it adopts the traditional way of BACnet/ZigBee gateway, we take 30 integrated networked digital power meters for example, query speed gets all data of 5 meters per-second and, it will take 6 seconds to complete all data update, which leads to meter data getting through BACnet device 6 seconds lagging behind real-time value, and they all are not query data of BACnet side needed.

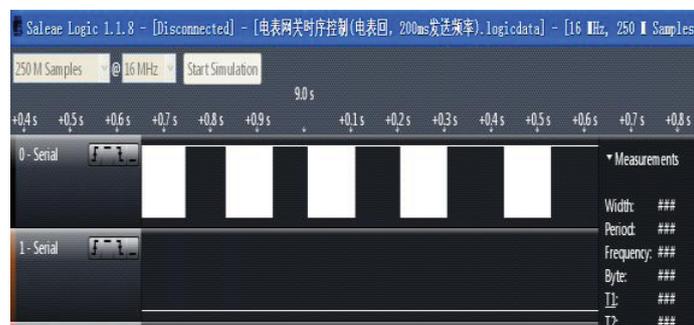


Fig. (8). Logic analyzer display YD2010 device response byte.

### CONCLUSION

This paper analyzed the mechanism of encapsulation and transport of BACnet Ethernet messages in the ZigBee network. It designed BACnet/ZigBee temperature sensor node hardware and software based on embedded technology to provide an effective way for BACnet building automation systems and ZigBee hybrid network and wired and wireless hybrid transmission, which has practical significance and reference value.

### CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

### ACKNOWLEDGEMENTS

We thank Fang Shi for critical revision of the manuscript. The project was supported by the municipal science and technology development project of Beijing educational committee (Grant No. KM201011417014).

## REFERENCES

- [1] W.J. Zhao, *Intelligent Building Monitoring System Design Based on ZigBee Technology*. Hangzhou Electronic Science and Technology University, Hangzhou, 2010.
- [2] L.C. Huang, H.C. Chang, C.C. Chen, and C.C. Kuo, "A ZigBee-based monitoring and protection system for building electrical safety", *Energy and Buildings*, vol. 43, pp. 1418-1426, 2011. [<http://dx.doi.org/10.1016/j.enbuild.2011.02.001>]
- [3] G.C. Liu, and X.H. Yang, "Wired/wireless hybrid transmission of modbus messages", In: *Tsinghua University, (Science and Technology)*, vol. 48. 2008, pp. 1844-1847.
- [4] Y.P. Xu, and M.L. Zhou, "Research on the application of wireless network technology in the intelligent building", *Computer Engineering and Design*, vol. 22, pp. 4264-4267, 2006.
- [5] Y. Peng, "ZigBee-A wireless communication protocol with features of low power, low cost, high reliability and low complexity", *Process Automation Instrumentation*, vol. 26, pp. 1-4, 2005.
- [6] "Building automation and control systems-Part 5", *Data Communication Protocol*, 2010.ISO/TC205, ISO16484-5-2010,
- [7] J. Nie, and C.H. Zhang, "Research on ZigBee and BACnet interconnection mechanism", *Low-voltage Apparatus*, vol. 22, pp. 1-3, 2008.
- [8] D. Liu, Z.H. Qian, Y. Liu, and Y. Li, "Study on ZigBee network energy optimization routing based on node Characteristics", *Journal of Northeast Normal University*, vol. 41, pp. 58-63, 2009. [Natural Scien Edition].
- [9] Z.H. Qian, S.Z. Hu, and X. Wang, "An cluster-based ZigBee routing algorithm for network energy optimization", *Chinese Journal of Computers*, vol. 36, pp. 485-492, 2012. [<http://dx.doi.org/10.3724/SP.J.1016.2013.00485>]
- [10] "Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANS), New York", *IEEE Computer Society, 2003*, 2003.IEEE Standard 802.15.4-2003,
- [11] "ZigBee Specification version 1.0", *ZigBee Alliance*, 2005. Available from: <http://www.ZigBee.org>
- [12] F. Wei, D.X. Fu, and Y.G. Wang, "Research and implementation of BACnet/ZigBee protocol converter", *Process Automation Instrumentation*, vol. 33, pp. 35-38, 2012.
- [13] G.L. Chen, S.J. Wang, and L.F. Li, "The design of wireless wave height sensor network node based on ZigBee technology", *International Conference Electric Information and Control Engineering (ICEICE) on Digital Object Identifier*, 2011, pp. 3684-3685
- [14] B.B. Shao, *Embedded Real-time Operating System ucOSII*. Beijing: University of Aeronautics and Astronautics Press, 2006.
- [15] D.Z. Hong, *Study and Implementation Based on BACnet*. East China: Normal University Press, 2012.

---

© Tian et al.; Licensee Bentham Open

This is an open access article licensed under the terms of the Creative Commons Attribution-Non-Commercial 4.0 International Public License (CC BY-NC 4.0) (<https://creativecommons.org/licenses/by-nc/4.0/legalcode>), which permits unrestricted, non-commercial use, distribution and reproduction in any medium, provided the work is properly cited.