An Efficient ZigBee-WebSocket based M2M Environmental Monitoring System

Kai Shuang, Xuan Shan, Zhengguo Sheng * and Chunsheng Zhu*
State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, China;
*Electrical and Computer Engineering Department, The University of British Columbia, Canada.
shuangk@bupt.edu.cn, shanxuanbupt@gmail.com,{zhengguo, cszhu}@ece.ubc.ca

Abstract—**Technologies to support the Machine-to-Machine (M2M) is becoming more important as the need to better understand our environments and make them smart increases. As a result it is predicted that intelligent devices and networks, such as wireless network, will not be isolated but connected and integrated composing computer networks. So far, to enable an End-to-end M2M service, WebSocket has attracted lots of attentions because of its unique full-duplex communications features. Besides, ZigBee technology has widely been deployed in short-range wireless communication systems with its low-power dissipation and high transmission speed. In this paper, we focus on the emerging M2M gateway development for home and industry applications. Specifically, by providing the detailed system architecture and user cases, we give a specific analysis on environmental monitoring implemented with WebSocket and ZigBee technology. The ZigBee sensor network is used to collect the temperature and humidity information. The foreground of the system shows the related data through B/S (Browser/Server) mode by utilizing WebSocket to push the information received by a web server to the client browser.**

Keywords—WebSocket; ZigBee; Machine-to-Machine (M2M); Gateway; Environmental Monitoring

I. INRTODUCTION

WebSocket is a protocol providing full-duplex communications channels over a single Transmission Control Protocol (TCP) connection. The WebSocket protocol was standardized by the Internet Engineering Task Force (IETF) as RFC 6455 in 2011 [1].

WebSocket is originally designed to be implemented in web browsers and web servers, but it has been extended to be used in any client or server application. The WebSocket Protocol is an independent TCP-based protocol. Its only relationship to HTTP is that its handshake is interpreted by HTTP servers as an Upgrade request. The WebSocket protocol makes it possible to provide diverse interactions between a browser and a web site, facilitating live content and the creation of real-time applications. This is made possible by providing a standardized way for the server to send content to the browser without being solicited by the client, and allowing for messages to be passed back and forth while keeping the connection open. In this way, a two-way (bi-directional) ongoing conversation can be established between a browser and the server. A similar method has been developed in non-standardized ways using stop-gap technologies such as Comet [2].

On the other hand, the ZigBee Smart Energy V2.0 [3] specifications define an IP-based protocol to monitor, control, inform and automate the delivery and use of energy and water. It is an enhancement of the ZigBee Smart Energy version 1 specifications, adding services for plug-in electric vehicle (PEV) charging, installation, configuration and firmware download, prepay services, user information and messaging, load control, demand response and common information and application profile interfaces for wired and wireless networks. It is being developed by a number of industry partners and widely used in M2M applications.

Motivated by these two technologies, in this paper, we innovatively integrate both WebSocket and ZigBee into a single M2M system design. Specifically, by developing a M2M gateway, the seamless communication can be ensured between server-gateway and gateway-sensor devices. The evaluation results are supplemented to show the advantages of the prototype system design.

II. M2M SYSTEM DESCRIPTION

M2M network consists of a large number of M2M nodes and a M2M gateway forming an M2M area domain. Each M2M node is a very flexible and smart device equipped with some specific sensing technologies, and M2M gateway is responsible for connecting M2M area domain with M2M network domain [4].

Fig. 1 gives an illustration of our prototype system in environmental monitoring, which consists of a gateway and a sum of sensor nodes. In the following sections, we will provide more details of system specifications.

Our research is funded by the Fundamental Research Funds for the Central Universities（2013RC1102）, Important national science& technology specific projects: Next-generation broadband wireless mobile communications network (2012ZX03002008-002-03)

978-1-4799-5079-9/14 $31.00 © 2014 IEEE
DOI 10.1109/DASC.2014.64

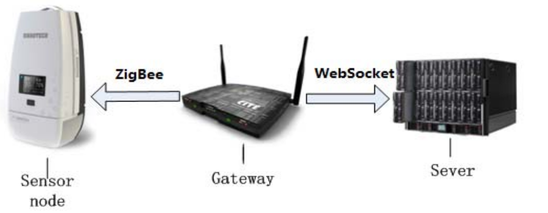


Fig. 1. System architecture

A. Gateway Framework

Multimedia data gateway applied in the wireless sensor networks or Internet of Things (IoT), which involves interactions of multimedia terminals and data service function of core control box, takes the role of data collection and management and includes the core technology of both communication and proxy in the IoT architecture. The gateway has the following functions: interactive man-machine interface, wireless internet access, cable internet access and data storage. The hardware architecture is based on Intel X86. Fig. 2 shows the detailed motherboard architecture.

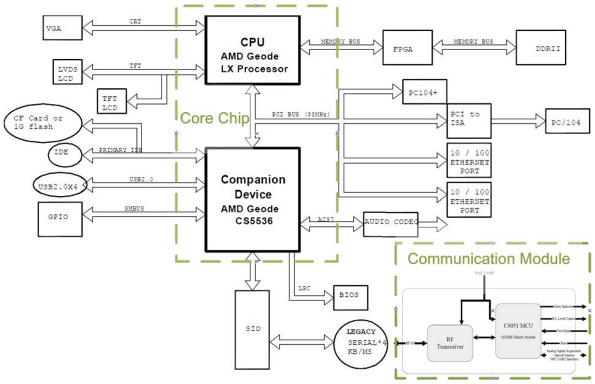


Fig. 2. Motherboard architecture

It is worth noting that the communication module includes IEEE 802.15.4 which has been implemented in the system to enable gateway-sensor communication, and IEEE 802.11 and Ethernet which have been implemented for gateway-server communication.

B. Wireless Sensor Node

Based on our experience in the field of short-range wireless communications, we independently developed a wireless sensor network protocol- Large Scale for Low Cost sensor networks (LSLC) for a wireless temperature and humidity acquisition system with full intellectual property rights and the industry's highest energy efficiency standards.

The system consists of some sensor nodes, a M2M gateway and management platform. Every sensor node sends temperature and humidity data to the server via the gateway, the real-time or historical data saved in the server can be transferred via Local Area Network (LAN) or the Internet to remote terminals. The system can detect hundreds of sensor nodes, and environmental data can be unified managed by the server, the whole process of data collection and monitoring is without human intervention. The sensor node integrates low-power wireless module which supports LSLC. Thus, it has features of low-cost, low power consumption and easy to install. Table I gives the details of wireless sensor node specification.

TABLE. I. Technical specifications of LSLC

RF parameters	
Working frequency band	2.4GHz / 780MHz
Transmit power	0dBm / 5dBm
Receiver sensitivity	-92dBm / -101dBm
Outdoor operating range	>100m
Indoor operating range	30~50m
System parameters	
Typical working mode	Every 15 minutes for a collection
Networking features	Ad hoc networks ,support multi-hop
Encryption	Support AES-128

Besides, the hardware platform of sensor node has the following advantages.

- Accurate synchronization of the entire network.
- Frequency hopping and encryption and authentication mechanisms to ensure reliable operation of the system security.
- Support IEEE802.15.4.
- Small size and ease of installation without wiring construction.
- The network can be scalable and the collector can be changed or replaced at any time.

III. PROPOSED METHOD

A. Software System Architecture

The operating system (OS) installed in the gateway is Windows XP, with MySQL database. In addition to that, the system we used to detect data and manage devices is a monitoring system with B/S (Browser/Sever) architecture.

Applicable functions of the management platform on the server include customer management, password settings, logs of system registry, lists of gateway retrieval and public management. The platform aims to easily monitor and analyze the user data collected from all sensor devices. Furthermore, it can dynamically display the current network topology on PC and the working status of each data node, and draw the data curve of the sensor. Moreover, remote configuration of sensor nodes via platform can be implemented via the gateway.

B. *WebSocket Protocol Handshake*

In the network domain, the great success of wired networks (e.g. xDLS, and PLC) and the ubiquity of wireless networks (e.g., 3G cellular, WiMAX, and Wi-Fi) provide cost-effective and reliable channels for transmitting the sensor data packets from M2M area domain to server and application domain. Therefore, we built a channel between the M2M gateway and sever using WebSocket, which can realize the real-time data transmission of temperature and humidity data [5] [6] [7].

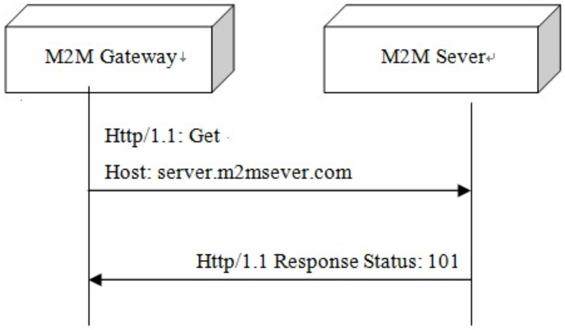
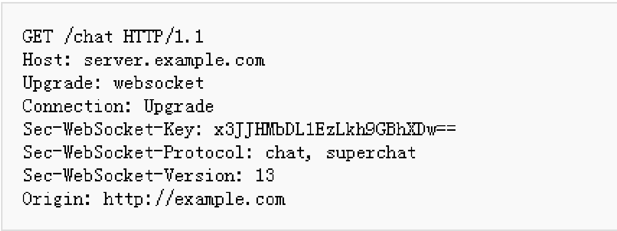


Fig. 3. WebSocket handshake

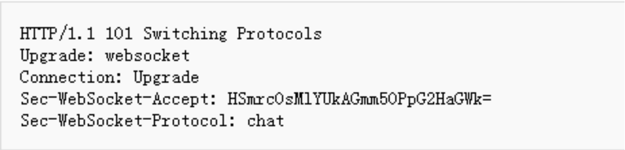
According to Fig. 3, to establish a WebSocket connection, the gateway sends a WebSocket handshake request, for which the server returns a WebSocket handshake response. The detailed information exchange can be found in the following example:

Gateway request:



```
GET /chat HTTP/1.1
Host: server.example.com
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Key: x3JJHMbDL1EzLkh9GBhXDw==
Sec-WebSocket-Protocol: chat, superchat
Sec-WebSocket-Version: 13
Origin: http://example.com
```

Sever response:



```
HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept: HSmrc0sMlYUkAGmm5OPpG2HaGWk=
Sec-WebSocket-Protocol: chat
```

Since the handshake relies on HTTP so that gateway can handle HTTP connections as well as WebSocket connections on the same port.

The gateway sends a Sec-WebSocket-Key which is a random value that has been base64 encoded. To form a response, the magic string 258EAFA5-E914-47DA-95CA-C5AB0DC85B11 is appended to this key. The resulting string is then hashed with SHA-1, then base64 encoded. Finally, the result reply occurs in the header Sec-WebSocket-Accept.

It is noted that once the connection is established, the gateway and sever can send WebSocket data or text frames back and forth in full-duplex mode. The data is minimally framed, with a small header followed by payload. WebSocket transmissions are described as "messages", where a single message can optionally be split across several data frames [8]. This can allow for sending of messages where initial data is available but the complete length of the message is unknown (it sends one data frame after another until the end is reached and marked with the FIN bit). With extensions to the protocol, this can also be used for multiplexing several streams simultaneously (for instance to avoid monopolizing use of a socket for a single large payload).

C. *The implementation of ZigBee stack*

Wireless sensor networks (WSN) should be capable of organizing hundreds or even thousands of nodes and provide reliable communication, thus these nodes must have the features of high reliability, low power, low cost, ease of installation and maintenance [9].

At present, the number of nodes of a conventional simple wireless network is generally less than 30, which is far from meeting the large scale requirements of some critical applications, and the extensive power consumption of less efficient communication protocols constraints the life time of sensor networks [10].

The proposed LSLC is based on ZigBee stack. The physical layer of LSLC implements IEEE802.15.4 and part of MAC layer is similar with ZigBee standard. The ZigBee stack architecture consists of a number of layered components including the IEEE 802.15.4 2003 Medium Access Control (MAC) layer and Physical (PHY) layer as well as the ZigBee Network (NWK) layer. Each of these provides applications with its own set of services and capabilities.

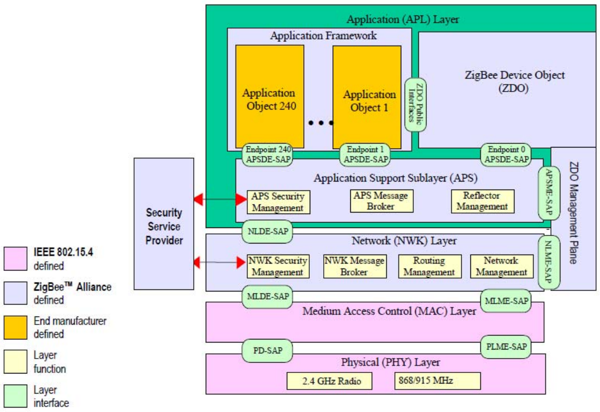
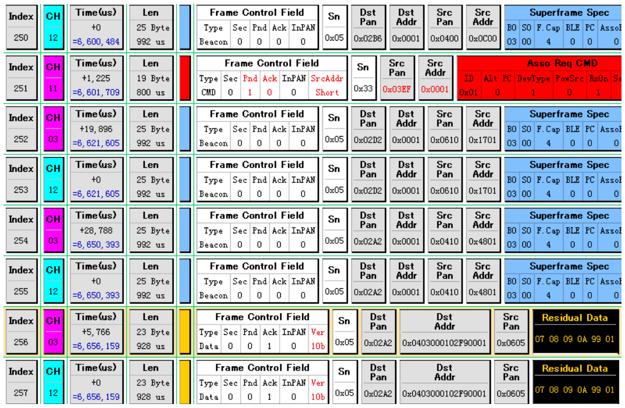


Fig. 4. ZigBee stack architecture

Fig. 4 shows the ZigBee application layer consists of the APS sub-layer, the ZDO (containing the ZDO management plane), and the manufacturer-defined application objects. The responsibilities of the APS sub-layer include maintaining tables for binding, which is the ability to match two sensors together based on their services and their needs, and forwarding messages between bound sensors. The responsibilities of the ZDO include defining the role of the sensors within the network (e.g., ZigBee coordinator or sensor nodes), discovering sensors on the network and determining which application services they provide, initiating and/or responding to binding requests and establishing a secure relationship between network sensors.



```
Index 250 | CH 12 | Time(us) +0 =6,600,484     | Len 25 Byte 992 us | Frame Control Field Type Beacon Sec 0 Pnd 0 Ack 0 InPAN 0 | Sn 0x05 | Dst Pan 0x02B6 | Dst Addr 0x0001 | Src Pan 0x0400 | Src Addr 0x0C00 | Superframe Spec BO 03 SO 00 F.Cap 4 BLE 0 PC 0 AssoI 0
Index 251 | CH 11 | Time(us) +1,225 =6,601,709 | Len 19 Byte 800 us | Frame Control Field Type CMD Sec 0 Pnd 1 Ack 0 InPAN 0 SrcAddr Short | Sn 0x33 | Src Pan 0x03EF | Src Addr 0x0001 | Asso Req CMD ID 0x01 Alt PC 0 DevType 1 PowSrc 0 RxOn 1 Se
Index 252 | CH 03 | Time(us) +19,896 =6,621,605 | Len 25 Byte 992 us | Frame Control Field Type Beacon Sec 0 Pnd 0 Ack 0 InPAN 0 | Sn 0x05 | Dst Pan 0x02D2 | Dst Addr 0x0001 | Src Pan 0x0610 | Src Addr 0x1701 | Superframe Spec BO 03 SO 00 F.Cap 4 BLE 0 PC 0 AssoI 0
Index 253 | CH 12 | Time(us) +0 =6,621,605     | Len 25 Byte 992 us | Frame Control Field Type Beacon Sec 0 Pnd 0 Ack 0 InPAN 0 | Sn 0x05 | Dst Pan 0x02D2 | Dst Addr 0x0001 | Src Pan 0x0610 | Src Addr 0x1701 | Superframe Spec BO 03 SO 00 F.Cap 4 BLE 0 PC 0 AssoI 0
Index 254 | CH 03 | Time(us) +28,788 =6,650,393 | Len 25 Byte 992 us | Frame Control Field Type Beacon Sec 0 Pnd 0 Ack 0 InPAN 0 | Sn 0x05 | Dst Pan 0x02A2 | Dst Addr 0x0001 | Src Pan 0x0410 | Src Addr 0x4801 | Superframe Spec BO 03 SO 00 F.Cap 4 BLE 0 PC 0 AssoI 0
Index 255 | CH 12 | Time(us) +0 =6,650,393     | Len 25 Byte 992 us | Frame Control Field Type Beacon Sec 0 Pnd 0 Ack 0 InPAN 0 | Sn 0x05 | Dst Pan 0x02A2 | Dst Addr 0x0001 | Src Pan 0x0410 | Src Addr 0x4801 | Superframe Spec BO 03 SO 00 F.Cap 4 BLE 0 PC 0 AssoI 0
Index 256 | CH 03 | Time(us) +5,766 =6,656,159  | Len 23 Byte 928 us | Frame Control Field Type Data Sec 0 Pnd 0 Ack 1 InPAN 0 Ver 10b | Sn 0x05 | Dst Pan 0x02A2 | Dst Addr 0x0403000102F90001 | Src Pan 0x0605 | Residual Data 07 08 09 0A 99 01
Index 257 | CH 12 | Time(us) +0 =6,656,159     | Len 23 Byte 928 us | Frame Control Field Type Data Sec 0 Pnd 0 Ack 1 InPAN 0 Ver 10b | Sn 0x05 | Dst Pan 0x02A2 | Dst Addr 0x0403000102F90001 | Src Pan 0x0605 | Residual Data 07 08 09 0A 99 01
```

Fig. 5. An example of data frame

The proposed LSLC protocol largely simplifies the packet overhead imposed by standard ZigBee MAC protocol. Especially, the frame control field and addressing field are redesigned to cope with large scale and low cost requirements. Fig. 5 shows the detailed data frame of the proposed LSLC protocol. The working procedure of joining a network is the following:

First, after the sensor node is powered on, it repeatedly sends the beacon request, which is used to ask to join the nearest network, and it builds its own network by choosing only one 16bit PAN ID which is based on the detected energy and network numbers from each allowable channel. The coordinator responses super-frame structure, when it finds the request from the sensor node, which is used for synchronization between sensor nodes. The sensor node then sends association request to the coordinator, and the coordinator responses an answer. After that the coordinator automatically assigns the 16-bit short address and the sensor node successfully joining the network. Once a new network is built, the gateway and other coordinators can be added to the network.

The phenomenon of network overlapping and PAN ID conflict may happen after building the network. The coordinator can initiate a PAN ID to solve the PAN ID conflicts, which includes changing the PAN ID and channel of a coordinator and amending its child devices at the same time. Typically, ZigBee sensor nodes will store the information of other nodes in a space of nonvolatile storage - the neighbour table.

IV. PERFORMANCE ANALYSIS

We put six sensor nodes in different areas of our office. After well configuration, we can get the real-time data of temperature and humidity from the monitoring system, and then we can get the topological structure of sensor nodes and have a clear view of networking process and data transmission.

All the sensor nodes placed are shown in Fig. 6. The orange dots represent the sensor nodes while the green dot represents the position of the gateway.

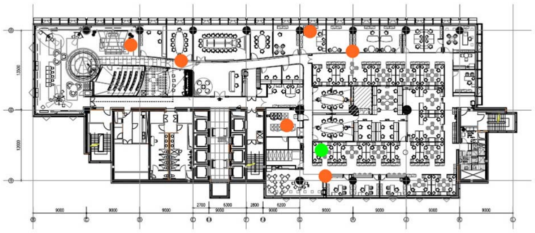


Fig. 6. Sensor network topology layout

To better describe the status of network and communication in the WSN built by the gateway and sensor nodes at different time in a day. We collect four sets of data at 10 AM, 12 AM, 3 PM and 6 PM from the sniffer, which are shown in Fig. 7. As can be seen, the green area represents effective IEEE 802.15.4 frames, while the yellow represents non-802.15.4 frames collected from the environment and the red means CRC error. The results tell that the data proportion is quite stable during the day, and the interference dominates channels. The reason is that since we use the frequency band of 780MHz, there is intense interference coexisting such as wireless mouse, wireless routers, etc. However, the proposed solution can automatically select the less interference channels to transmit (i.e., channels 3 and 12).

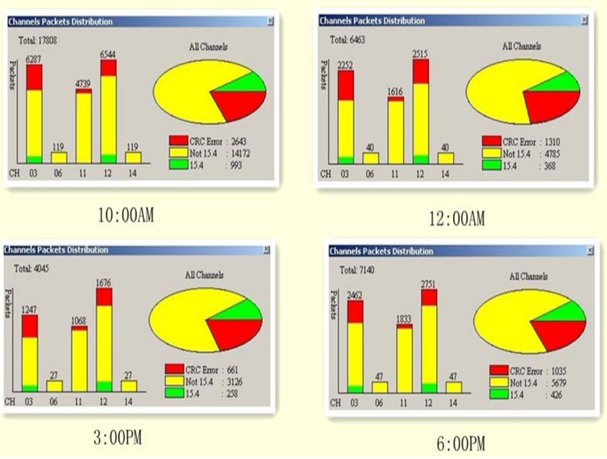


Fig. 7. Packets distribution in different channels

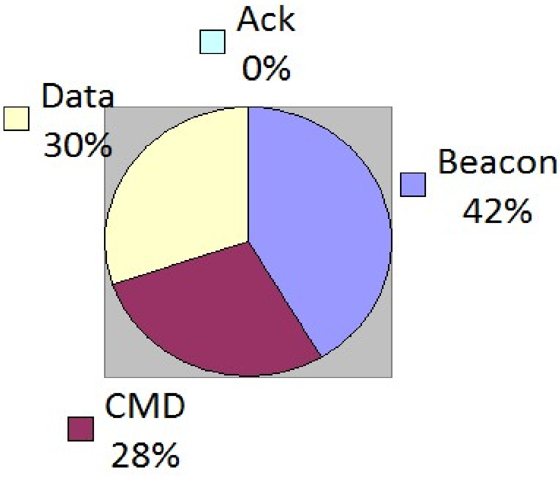


Fig. 8. Ratio of four main packets[1]

After data collection and analysis, we obtain the ratio of four main packets (Beacon, CMD, ACK and Data) from the effective IEEE 802.15.4 frames as shown in Fig. 8. It is clear that in order to combat with channel interference, the proposed solution broadcasts a large number of control packets (including CMD and Beacon) over the time to keep connected with peer node.

According to the statistics we collected from previous figures, we show the packet error rate in Fig. 9. It is shown that although there is strong co-channel interference, the proposed solution can still achieve decent error performance.

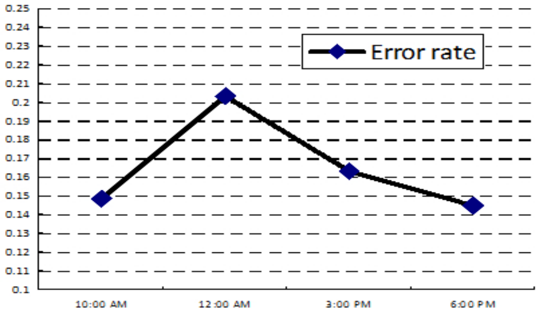


Fig. 9. Error rate over different time in one day

Fig. 10 shows the usefulness of our prototype system in monitoring temperature and displaying the collected data on the server via WebSocket from the gateway. We can clearly see the temperature changes over the time. Moreover, the figure gives detailed description containing the MAC address and temperature value of every node. Such prototype system has been successful deployed in our lab to monitor indoor environment.

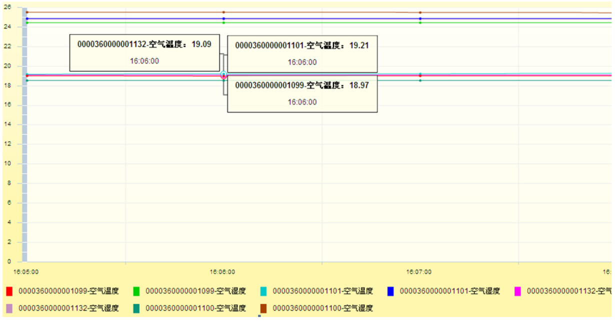

26
24
22
20
18
16
14
12
10
8
6
4
2
0
0000360000001132-空气温度：19.09
16:06:00
0000360000001101-空气温度：19.21
16:06:00
0000360000001099-空气温度：18.97
16:06:00
16:05:00
16:06:00
16:07:00
16:
0000360000001099-空气温度
0000360000001099-空气湿度
0000360000001101-空气温度
0000360000001101-空气湿度
0000360000001132-空气
0000360000001132-空气湿度
0000360000001100-空气温度
0000360000001100-空气湿度

Fig. 10. Temperature Description With MAC address

V. CONCLUSION

In this paper, we have presented the innovative ZigBee-WebSocket based M2M system. The proposed LSLC protocol can enable a large scale communication and effectively combat channel interference. Moreover, we successfully use WebSocket to retrieve real-time temperature and humidity data. Such result will have broad impact in a number of areas, such as wireless sensor networks and M2M.

REFERENCES

[1] http://www.rfc-editor.org/rfc/rfc6455.txt

[2] http://www.ibm.com/developerworks/cn/web/wa-lo-comet/

[3] http://www.zigbee.org/Specifications/ZigBee/FAQ.aspx

[4] Niyato, Dusit and Xiao, Lu and Wang, Ping, "Machine-to-machine communications for home energy management system in smart grid", *IEEE Commun. Mag.,* Vol.49, No.4, 2011

[5] Ma, Kun and Sun, Runyuan, "Introducing WebSocket-Based Real-Time Monitoring System for Remote Intelligent Buildings", *International Journal of Distributed Sensor Networks*, 2013

[6] Pimentel, Victoria, Nickerson, Bradford G. "Communicating and Displaying Real-Time Data with WebSocket". *IEEE internet computing*, 2012.

[7] LIU, Jian-ge and MU, De-jun and ZHANG, Hui-xiang and MAO, Bao-lei, "Design and Realization of Electrical Energy Real-time Distant Monitoring and Control System", *Computer Technology and Development*, Vol.9, 2013

[8] Furukawa, Y, "Web-based control application using WebSocket", *WEB-BASED CONTROL APPLICATION USING WEBSOCKET*, 2011

[9] Kuei-Li Huang, Li-Hsing Yen, Jui-Tang Wang et al. "A Backbone-Aware Topology Formation (BATF) Scheme for ZigBee Wireless Sensor Networks[J]", *Wireless personal communications*, Vol.47, No.1, 2013

[10] Kim, Seong Hoon and Kang, Jeong Seok and Park, Hong Seong and Kim, Daeyoung and Kim, Young-joo. "UPnP-ZigBee internetworking architecture mirroring a multi-hop ZigBee network topology", *IEEE Trans. Consumer Electron.,* , Vol.55, No3, 2009

[1] The ratio of ACK packet is approximately 0.1%.