Available online at www.sciencedirect.com

SciVerse ScienceDirect

ELSEVIER

Procedia Environmental Sciences 11 (2011) 552 – 557

Procedia
Environmental Sciences

A new wireless sensor platform with camera

Huang Liu *, Shouyi Yin, Leibo Liu, Shaojun Wei

Institute of Microelectronics,,Tsinghua University,,Beijing,China,
**15110262917@163.com, yinsy@tsinghua.edu.cn*

Abstract

there are several platforms of wireless sensor networks such as micaz, mica2, etc. Each of them has specific characteristics. But the complexity of novel applications requires new characteristics, which more and more new designs of wireless sensor networks are needed. In this paper, the design of a sensor named Lacuna is proposed, which is a new sensor network platform implementing reliable detecting by taking real-time pictures. The paper presents a simplified model of wireless sensor networks (WSN) which is composed of the Lacuna sensors using IEEE 802.15.4 wireless technology. This model has been tested for many times and the model experimental results show that this system can run stably, reliably and efficiently. Stability, reliability, and efficiency are important because they make the operation robust to temporary disconnections or high packet loss. Due to the stability, reliability, and efficiency , the WSN transmits large amounts of continuous stable picture data messages to notebook when one of the nodes finishes taking a picture.

Keywords: wireless sensor network;802.15.4;Lacuna; camera; picture.

1.Introduction

Monitoring remote environments, observing microclimates, surveillance of customer behavior, military observations and other applications drive researchers to explore wireless sensor network technology. This exploration is accentuated by the improvements in the Micro-Electro-Mechanical Systems (MEMS) and wireless communication technologies which make a pragmatic vision of WSN [1], [2].

In order to meeting the needs of real-time picture monitoring, the Lacuna sensor platform which has a camera is used to setting up the wireless sensor network. It can take a 640 * 480 image in real time and transmit all of the image data in a specific data structure using IEEE 802.15.4 through the RF immediately. It transmits image data from the child node to the father node using the Collection Tree Protocol (CTP). And then the father node transmits the image data to its father node. Finally, the node which connects with notebook receives the image data and transfers the image data to notebook. Then clear pictures are obtained by using image processing software in notebook [3].

doi:10.1016/j.proenv.2011.12.087

This paper is organized as follows: the next section is an introduction of the Lacuna sensor platform, the description of the WSN module experiment is presented in the section III, the experimental results are described on section IV and message structure are given in section V.

2.Lacuna sensor platform

The new sensor platform named Lacuna, shown in Figure 1, provides hardware modules as follows: radiofrequency(RF) module, processor module, memory module, camera module, power module, and peripheral interface module. RF module uses 2.4 GHz carrier frequency. Processor module is designed by us, based on a 8051 CPU core. The capacity of memory module is 32K bit. Camera module is an ordinary camera which can be bought easily. This sensor requires 2.8- 3.8 Volts and is powered by two 1.5V (3AAA) batteries. Peripheral interface module includes usb interface, LEDs, reset button, and so on.

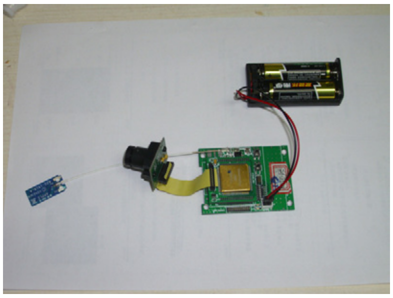


Figure 1. Lacuna sensor

This sensor has three hardware features to support efficient deployment and configuration. First, the nodes are highly-integrated which helps minimize the amount of time required to place and lowers their energy consumption. The energy consumption is less than the other distant node [4]. Second, only one-touch is required to activate a node and initiate the process of discovering and joining the network [5]. Third, after a node has been activated, it takes only one of the LEDs to verify that it is operational.

3.WSN module experiment

The WSN is composed of some wireless sensor nodes and a remote center computer system at least. Some of the wireless sensor nodes act as base stations, others act as detecting nodes and gateway nodes. A simplified WSN is shown in Figure 2.

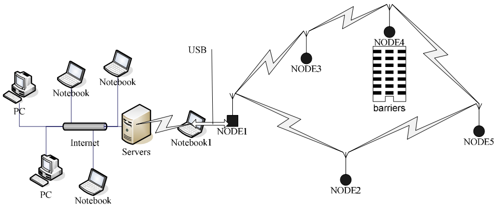


Figure 2. a simplified WSN module:there are only five nodes.

Five sensor nodes, shown in Figure 3,have been distributed with the purpose of detecting events. All of the five nodes are Lacuna sensors with different addresses and chip identity (CHIP ID) that we can upload for experimental purpose.

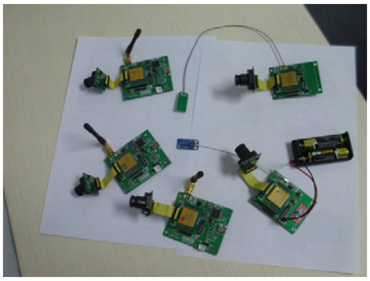


Figure 3. Five sensor nodes:seting up WSN.

The workflow that the WSN captures and transmits an image is as follows:

Firstly, all nodes start and send beacon messages to each other using CTP. CTP is a tree-based collection protocol. Some number of nodes in a network advertise themselves as tree roots. Nodes form a set of routing trees to these roots. CTP is address-free in that a node does not send a packet to a particular root, instead, it implicitly chooses a root by choosing a next hop. Nodes generate routes to roots using a routing gradient. [6]

Secondly, all nodes set up their routes in the WSN. After that, notebook1 send command to node1 through USB interface, including the choice of a particular node to start camera and whether the camera starts periodically. Suppose that notebook1 choose node5 to start camera periodically.

After node1 received the commands, node1 produces a data message which contains all information that it receives via USB interface using a dissemination protocol.

Dissemination is a basic sensor network protocol. The ability to reliably deliver a piece of data to every node allows administrators to reconfigure, query, and reprogram a network. Unlike flooding protocols, which are discrete efforts that terminate and not reach consistency, dissemination assures that the network will reach consensus on the value as long as it is not disconnected. [7]

When other nodes receive the data message, they forward it until all nodes receive. The node which matches the destination address of the data message starts its camera. Node5 starts camera every five minutes which is also controlled by the message in our experiment.

Thirdly, When node5 finishes taking a picture, it produces a data message using CTP and sends the first picture data message to the WSN. Node5 does not send the second pictrue data message until it receives a acknowledgement (ACK) message. If node5 does not receive an ACK message, it retransmits the picture message which it just sends after executing carrier sense multiple access (CSMA).

Finally, Node4 receives the message and it checks whether the message is for me. When the destination address of the message matches its address, it sends back an ACK message. Then node4 pulls the message into memory pool and forwards it. When node3 receives the message, it operates just as node4 does. Finally, node1 receives the picture messages and sends them to nootbook1 via USB interface. Notebook1 accepts and processes all the image data, and a clear picture is obtained.

As energy efficiency is one of the most important attributes in sensor networks, re-sending collided packets should be avoided as this consumes a lot of energy [8].In order to reduce energy and time consumption, another way to test the WSN module is employed, in which ACK, retransmission, and FCS are not enabled.

Both of the experiments are described in the next part.

As is seen, there is another less route in the WSN from node5 to node1. The route is from node5 to node2 to node1. Always, the picture data messages go along the route according to CTP. The other route mentioned above is discussed only for easy description of how the WSN works.

4.Experimental results

The WSN module experiment described in the section III is carried out for many times in two ways. One of the pictures is shown in Figure 4.

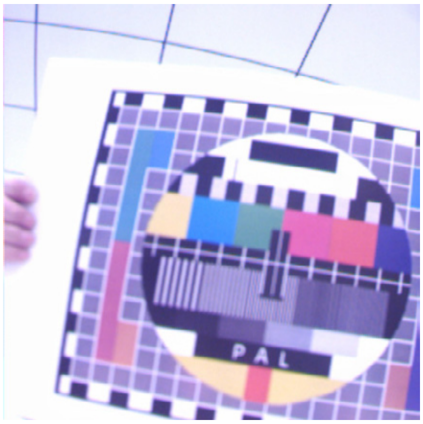


Figure 4. a pictrue:node5 take the pictrue in our laboratory and transmit to node1,node1 transfer to notebook1.

As is seen, the size of the picture is 640*480 and is clear enough for detecting.

There are some experimental data in table 1 and table 2.

Table I.The experiment with ACK, retransmission,and FCS

	Send(times)	Receive(successful times)	Total Time(Minutes)
Single-hop	10000	99998	5360
Multi-hop	3000	2994	6400

Table II The experiment without ACK, retransmission,and FCS

	Send(times)	Receive(successful times)	Total Time(Minutes)
Single-hop	10000	87246	3270
Multi-hop	3000	2134	3470

From table 1 and table 2, a conclusion can be drawn. The results of the two experiments are of huge difference.

In addition, a C51-RF packet sniffer is used to capture, filter and decode IEEE 802.15.4 MAC packets, and display them in a convenient way, with options for filtering and storage to a binary file format. The packet sniffer also has the optional ability to decode the MAC data frames at the ZigBee Network (NWK) and Application Support Sublayer (APS). Detailed data about every frame which is just received can be obtained to compare with the frame which is sent. So that calculation of the bit error rate can be done.

The experiment with ACK, retransmission, and FCS shows that: In the single-hop network like from node2 to node1, delivering an image takes about 30 seconds. In the multi-hop networks like from node3 to node4 to node5 to node1, it takes about two minutes. In the single-hop network, zero packet loss and bit error rate is guaranteed. In the multi-hop networks, packet loss rate is nearly 0, bit error rate is also 0. So we can get clear picture most of the time.

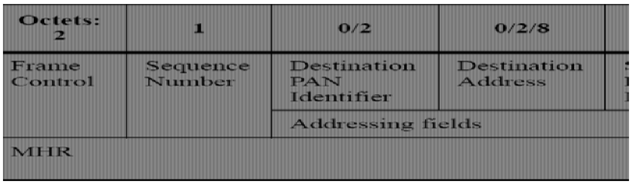
If there are not ACK, retransmission mechanism, and FCS, the results are not so good. In the single-hop network like from node2 to node1, delivering an image takes about 20 seconds. In the multi-hop networks, like from node3 to node4 to node5 to node1, takes about 70 seconds. In the single-hop network, packet loss rate is 4%, and bit error rate is also 10%. In the multi-hop networks, packet loss rate is nearly 12%, and bit error rate is also 20%.

Comparing these two experimental results, although the experiment of the table 2 cost less time and energy, the experiment of the table 1 is considered much better. In our experiments, one image requires for 128K byte picture data, each frame contains 32 byte picture data. So one image requires for 4096 continuous transmission without considering the case of retransmission. That requires large amounts of continuous stable data transmission. The basic challenge for a MAC layer in WSN is to avoid collisions among transmitted packets [9].So the experiment of the table1 is choosen to set up the WSN for further study. All of these technical parameters can be further improved.

5.Message structure

Lacuna sensor platform use IEEE 802.15.4/ZigBee. The message structure is shown in table 3.

Table III message sructure: IEEE 802.15.4



Octets: 2	1	0/2	0/2/8
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address
		Addressing fields	
MHR			

The medium access control (MAC) payload is prefixed with a MAC header (MHR) and appended with a MAC footer (MFR). The MHR contains the Frame Control field, data sequence number (DSN), addressing fields, and optionally the auxiliary security header. The MFR is composed of a 16-bit FCS. The MHR, MAC payload, and MFR together form the MAC data frame.

The fields of the MHR appear in a fixed order,however,the addressing fields may not be included in all frames. The Frame Control field is 2 octets in length and contains information defining the frame type, addressing fields, and other control flags. The Frame Type subfield is 3 bits in length and shall be set to one of the nonreserved values. The Security Enabled subfield is 1 bit in length, and it shall be set to one if the frame is protected by the MAC sublayer and shall be set to zero otherwise. The Frame Pending subfield is 1 bit in length and shall be set to one if the device sending the frame has more data for the recipient. This subfield shall be set to zero otherwise. The Acknowledgment Request subfield is 1 bit in length and specifies whether an acknowledgment is required from the recipient device on receipt of a data or MAC command frame. If this subfield is set to one, the recipient device shall send an acknowledgment frame. The PAN ID Compression subfield is 1 bit in length and specifies whether the MAC frame is to be sent containing only one of the PAN identifier fields when both source and destination addresses are present. The Destination Addressing Mode subfield is 2 bits in length and shall be set to one of the nonreserved values. The Frame Version subfield is 2 bits in length and specifies the version number corresponding to the frame. The Source Addressing Mode subfield is 2 bits in length and shall be set to one of the nonreserved values. The Sequence Number field is 1 octet in length and specifies the sequence identifier for the frame. The Destination PAN Identifier field, when present, is 2 octets in length and specifies the unique PAN identifier of the intended recipient of the frame. The Destination Address field, when present, is either 2 octets or 8 octets in length, according to the value specified in the Destination Addressing Mode subfield of the Frame Control field, and specifies the address of the intended recipient of the frame. The Source PAN Identifier field, when present, is 2 octets in length and specifies the unique PAN identifier of the originator of the frame. The Source Address field, when present, is either 2 octets or 8 octets in length, according to the value specified in the Source Addressing Mode subfield of the Frame Control field, and specifies the address of the originator of the frame. The Auxiliary Security Header field has a variable length and specifies information required for security processing.

In our experiments, MHR is 11byte in length and is set to 0X1821 for data frame, 0X1820 for beacon frame. MAC Payload is 41 byte in length, including 32 byte image data and 9byte CTP header data. A whole frame is 55 byte in length.

6.Conclusion

This article demonstrates a new wireless sensor platform named Lacuna with a camera. New software platform is developed and a simplified model of WSN is created using the sensor platform. On this platform, a large number of continuous data transmission is implemented and pictures are transferred effectively in both single hop and multi-hop networks. In a number of experiments, the platform is proved to be stable, reliable and efficient. The practical application of this new platform meets the WSN requirements.

Acknowledgment

This work was supported by Special Scientific Research Funds for Commonweal Section (200903010), National S&T Major Project (2009ZX03006-004) and Doctoral Fund of Ministry of Education of China (20070003098).

References

[1]D. Estrin, R. Govindan, J. Heidemann, and S. Kumar. Next century challenges:Scalable coordination in sensor networks. In Proc. ACM/IEEE MobiCom, pages 263-270, 1999.

[2]D. Estrin. Embedded networked sensing research: Emerging systems challenges. In NSF Workshop on Distributed Communications and Signal Processing. Northwestern University, December 2002.

[3]E. Pamba Capo-Chichi, H. Guyennet, Jean-Michel Friedt, Ian Johnson, Craig Duffy, “Design and implementation of a generic hybrid Wireless Sensor Network platform ”, IEEE Press, 2008, pp.836-840,978-1-4244-2413-9/08.

[4]E. Bayse, A. Cavalli, M. Núñez, F. Zaïd , “A passive testing approach based on invariants: application to the WAP,” Computer Networks, Vol. 48, pp. 247-266.

[5]Prabal Dutta, Mike Grimmer, Anish Arora, Steven Bibyk, and David Culler, “Design of a Wireless Sensor Network Platform for Detecting Rare, Random, and Ephemeral Events” , IEEE Press, 2005，pp.497-502,0-7803-9201-9/05.

[6]The Collection Tree Protocol (CTP).

[7]The Dissemination Protocol.

[8]W. Ye, J. Heidermann, "Medium Access Control in Wireless Sensor Networks" , ISI-TR-580, USC Information Sciences Institute, October 2003.

[9]Azni Haslizan Ab.Halim, Kartinah Zen，“MAC Protocol to Reduce Packet Collision in Wireless Sensor Network”：Proceedings of the International Conference on Computer and Communication Engineering 2008，May 13-15, 2008 Kuala Lumpur, Malaysia