International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

The Modbus Protocol Based Wireless Sensor Networks

[1] Mohammad Rashid Ansari

[1] Department of Electronics and Communication Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh

[1] rashid.ansari@galgotiasuniversity.edu.in

Abstract: Wireless ZigBee is very low-cost, very low power consumption, two-way, wireless communications technology which can be used extensively in consumer electronics, home and building automation, industrial controls, PC peripherals, medical sensor applications, toys and games. Now ZigBee technology also can be used in agriculture monitoring and control. ZigBee wireless communication is transparent to the user, which is not suitable for the user to be familiar with the successive data information in a real-time system. We need a friendly interface to study the information in the wireless network. MODBUS protocol is widely used in industrial monitoring and test, which is an application layer messaging protocol, positioned at level 7 of the OSI model, that provides client/server communication between devices connected on different types of buses or networks. In the plant physiological ecological monitoring system, the information transmission between the coordinator and PC by MODBUS protocol, we can easily observe the real-time data from the remote field-device.

Keywords: MODBUS Protocol, MODBUS Function, Protocol data unit, Wireless Sensor Networks, ZigBee.

INRODUCTION

The Wireless Sensor Networks (WSN) comprise of relatively inexpensive sensor nodes capable of collecting, processing, storing and transferring information from one node to another. These nodes are able to autonomously form a network through which sensor readings can be propagated. Since the sensor nodes have some intelligence, data can be processed as it flows through the network. Sensing devices will be proficient to monitor a wide variety of ambient conditions such as temperature, pressure, humidity, soil makeup, vehicular movement, noise levels and lighting conditions, the presence or absence of certain kinds of objects, mechanical stress levels on attached objects and so on. These devices will also be equipped with significant processing, memory and wireless communication capabilities. Emerging low-level and low-power wireless communication protocols can be used to networks the sensors. This potential will add a new measurement to the capabilities of sensors. Sensors will be able to coordinate among themselves on a higher-level sensing task. The information transmission is transparent for the user in the ZigBee[1] wireless sensors network, which are lack of interactivity and self-constrain. The information in the ZigBee wireless sensors network cannot be viewed in a real time by a friendly interface. MODBUS protocol is embedded into ZigBee stack, in this way, we can implement interaction well and the information can be viewed in a friendly interface. So, here we presents the measures to embed the MODBUS protocol into the ZigBee stack which contains address bound mechanism, information centralized storage and flexible monitoring, by which we can monitor the real time information from the ZigBee wireless network and use some instructions to control the remote device in a friendly interface, which can be used well in the middle and small ZigBee monitoring wireless sensors network. Fig. 1 shows the architecture of wireless system networks.

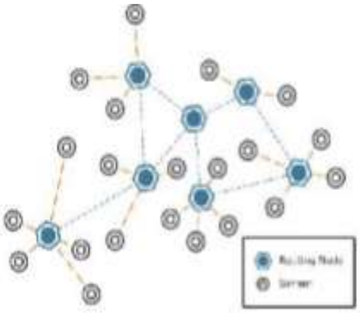

Fig. 1: Wireless Sensor Networks Architecture

OVERVIEW OF MODBUS

MODBUS is an application layer messaging protocol, positioned at level 7 of the OSI model that provides client/server communication between devices connected on different types of buses or networks. The industry's standard since 1979, MODBUS continues to enable millions of automation devices to communicate. Today, support for the simple and elegant structure of MODBUS continues to grow. The Internet community can access MODBUS at a reserved system port 502 on the TCP/IP stack. MODBUS[2] is a request/reply protocol and offers services specified by function codes. MODBUS function codes are elements of MODBUS request/reply Protocol Data Units (PDU).

It is currently implemented using:

- TCP/IP over Ethernet.
- Asynchronous serial transmission over a variety of media
- MODBUS PLUS, a high speed token passing network.

MODBUS PROTOCOL ARCHITECTURE

The MODBUS protocol[3] follows a master/slave architecture where a master will request data from the slave. The master can also ask the slave to perform some action. The master initiates a process by sending a function code that represents the type of transaction to perform. The transaction performed by the MODBUS protocol defines the process a controller uses to request access to another device, how it will respond to requests from other devices, and how errors will be detected and reported. The MODBUS protocol establishes a common format for the layout and contents of message fields. During communications on a MODBUS network, the protocol determines how each controller will know its device address, recognize a message addressed to it determine the kind of action to be taken and extract any data or other information contained in the message.

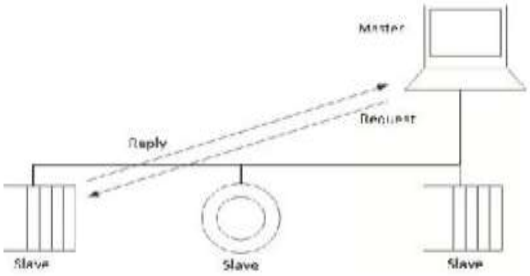

Fig. 2: Basic MODBUS Network

Controllers communicate using a master/slave technique where only one device, the master, can initiate transactions or queries. The other devices, slaves, respond by supplying the requested data to the master or by taking the action requested in the query. Typical master devices include host processors and programming panels. Typical slaves include programmable controllers. The messages exchanged between the master and the slaves are called frames. There are two types of MODBUS frames: Protocol Data Unit (PDU) and Application Data Unit[4] (ADU). The PDU frames contain a function code followed by data. The function code represents the action to perform and the data represents the information to be used for this action. ADU frames add a little more complexity with an additional address part. ADU frames also provide some error checking. Fig. 2 shows the basic MODBUS network.

MODBUS FUNCTIONS

The specification defines a certain number of functions, each of which is assigned a specific function code. They are in the range 1-127 (decimal), as 129(1+128) or 255(127+128) represents the range of error codes. While the first published version of the specification defined different classes of functions, for example Class 0, Class 1 and Class 2, the newly released specification defines categories of function codes:

- Public: These are guaranteed to be unique[5] and specify well defined functions that are publicly documented. These are validated by the community and a conformance test exists.
- User-Defined: These are available for user-defined functions, thus their codes might not be unique. The specification defines the code ranges 65-72 and 100-110 for user-defined functions.
- Reserved: These are currently used by some companies for legacy products and are not available for public use.

The documentation for a function consists of:

1. A description of the function, its parameters and return values.

2. The assigned Function Code

3. The Request PDU

4. The Response PDU

5. The Exception Response PDU

IMPLEMENTATION PLATFORM

The implementation platform contains software platform and hardware platform. The basic software platform is the TI ZigBee-stack 2006 and the MODBUS Protocol is embedded into the ZigBee-stack then we execute the wireless field-bus protocol. The ZigBee module associated with some sensors which compute the environment parameters and the plant physiological ecological information. By that information we can analysis the plant health status.

- System Overview Framework

The plant physiological ecological monitoring system is composed of PC, some sensors node and a coordinator. PC is the friendly interface to show the information in the wireless network, which connects with the Coordinator by RS-232 interface. Sensors nodes[6] send the data to the Coordinator and it stores the data by MODBUS protocol. When the PC sends some instructions to query the sensor node information the Coordinator will response to the query instructions.

- Hardware Platform

The chip CC2430[7] is as the core of the hardware, CC2430 integrated RF transceiver, CPU and 128K flash memory and very few external components are required in the CC2430 typical application. In the system the CC2430 module connects with some different kinds of sensors, and the Coordinator node has the same structure with the sensor node except the sensor module.

- Software Platform

Using the TI ZigBee stack as the software platform. APP directory is the area for the project creature which contains the application layer files and the main contents of the project. HAL directory contains hardware configuration, driver, and relevant functions. MAC directory contains MAC layer parameters configured files and some API libraries. MT directory contains some serial operator files.

ZigBee[8] stack runs in an operator system called OSAL (Operator System Abstract Layer). OSAL takes task scheduling mechanism. Each task contains some events and each event own the only events ID. Task scheduling is implemented by the event trigger of the task. When an event appears, the corresponding event of the task will set an event ID, then the task scheduling will call relevant task processing function.

MODBUS protocol is widely used in industrial automation field. The typical transmission characteristic is that no query, no reply. If we want to query the sensor node's information we should send the command first, then the sensor node will reply the relevant information to the host computer. There are two message frame structures in MODBUS protocol of which we take RTU message frame structure. MODBUS[9] is a very convenient software platform for the MODBUS transmission test. The Coordinator is connected with the host computer by serial port. Slave is the object that we want to observe and write the sensor node's MODBUS ID here. Function is one of the command options to read holding register. Address is the start address of the register need to read and length is the number of register need to read consecutively. Scan rate is the interval between two commands. All these configurations are following the MODBUS protocol frame structure. Slave is the object that we want to observe and we write the sensor node's MODBUS ID here. Function is one of the command options and function commands are chosen to read holding register. Address is the start address of the register need to read and length is the number of register need to read consecutively. Scan rate is the interval between two commands.

CONCLUSION

ZigBee wireless sensors network based on MODBUS protocol can be used well in the Plant physiological ecological monitoring system. Modbus protocol has a typical advantage, if there is no query for the node, there will be any response information to the host computer. If the nodes in the ZigBee wireless network are too many and we only care for some nodes in the node, we can choose the nodes which we want to monitor. It also can reduce the load of the processor of the coordinator. The advantages of the ZigBee wireless sensors network system based on MODBUS protocol are as follows:

1) The wireless sensors system is of high convenience in the course of the system installation.

2) The ZigBee technology makes the power consumption very low

3) The MODBUS protocol provides a friendly interface for the system observation.

4) MODBUS protocol as a mature field bus standard provides a general interface for the system.

So we can use this interface to connect with GPRS, Industry Ethernet and so on. So this system can be expanded well.

REFERENCES

[1] S. Mahlknecht, T. Dang, M. Manic, and S. A. Madani, "ZigBee," in *Industrial Communication Systems*, 2016.

[2] M. de Sousa and P. Portugal, "Modbus," in *Industrial Communication Systems*, 2016.

[3] R. Belliardi and R. Neubert, "Modbus protocol," in *Industrial Communication Technology Handbook, Second Edition*, 2017.

[4] F. G. D. Comittee, "Coastal and marine ecological classification standard, June 2012," *Natl. Ocean. Atmos. Adm.*, 2012.

[5] D. Type and P. Date, "Introduction to Modbus," *Natl. Instruments*, 2014.

[6] M. Faisal, A. A. Cardenas, and A. Wool, "Modeling Modbus TCP for intrusion detection," 2017, doi: 10.1109/CNS.2016.7860524.

[7] W. Liu and Y. Yan, "Application of ZigBee wireless sensor network in smart home system," *Int. J. Adv. Comput. Technol.*, 2011, doi: 10.4156/ijact.vol3.issue5.17.

[8] N. Ashok Somani, "Zigbee: A Low Power Wireless Technology for Industrial Applications," *Int. J. Control Theory Comput. Model.*, 2012, doi: 10.5121/ijctcm.2012.2303.

[9] I. N. Fovino, A. Carcano, T. De Lacheze Murel, A. Trombetta, and M. Masera, "Modbus/DNP3 state-based intrusion

detection system," 2010, doi:
10.1109/AINA.2010.86.