IoT Based Fast Access NRF Communications Using Arduino Microcontroller

[1]K.Chaitanya Sravanthi, [2] Dr.S.SwarnaLatha [3]Dr.B.Shoban Babu
[1]P G Scholar, [2] Professor [3]Professor
[1,2]Department of ECE, S.V. University College of Engineering, Tirupati, Andhra Pradesh, India.
[3]Department of ECE, SVEC, Tirupati, Andhra Pradesh, India.

Abstract: ***T*****he development of Internet of Things (IoT) technology, the application of IoT is more and more importantly widespread. Meanwhile, how to achieve fast access for various IoT devices, especially for a large-scale of IoT devices, also has been a significant challenge in the development of IoT systems. To address this issue, a fast access protocol for NRF-enabled IoT devices is proposed in this paper, in which, the NRF module embedded in a registering IoT device could automatically obtain a Personal Area Network (PAN) address and instantly access the target NRF wireless network through the signaling interactions among the involved protocol entities. After that, the operation and control of the accessed IoT devices are conducted based on the NRF communications. To evaluate the effectiveness and efficiency of this protocol, a prototype system is developed. The experiment and analysis results also have been shown to demonstrate the performance by comparing with the existing access methods. The proposed system has been verified in three cases.**

Index Terms **– Node MCU, NRF Transmitter, NRF Receiver etc...**

I. INTRODUCTION

Internet of things (IoT) as an extension of Internet is a network which uses sensing devices to achieve interconnection and interworking of any objects according to some specific agreements, and realizes intelligent identification, location, tracking, monitoring and management [1]. Currently, with the development of IoT technology and the reducing cost of wireless communication modules, more and more ordinary physical objects could become IoT devices by embedding or integrating specific wireless communication modules (e.g., Wi-Fi, Bluetooth, ZigBee, etc.) and access wireless networks to achieve various purposes (e.g., data collection, operation, control, etc.) [2]. However, with the widespread application of IoT systems, the number of IoT devices which attempt to access the network is experiencing a rapid growth [3]. Therefore, how to achieve fast network access for large-scale IoT devices which is the precondition in the development of a IoT system, and realize the interconnection and interworking have been critical challenge issues. Recently, an extensive body of research has focused on designing effective and efficient network access strategies. The popular methods in the existing network access technologies for IoT devices can be summarized as follows [4, 10]. (1) Method-1: Configuring the IoT device in a direct manner by directly connecting the IoT device with a computer. (2) Method-2: On the IoT device with a touch screen or a keyboard, the network access can be achieved through the input Service Set Identifier (SSID) This work is supported by National Nature Science Foundation under Grant Nos. 61300198 & 61772233; the outstanding young teacher training program of the Education Department of Guangdong Province under Grant No. YQ2015158; Guangdong University Scientific Innovation Project under Grant No. 2017KTSCX, Guangdong Provincial Science & Technology Plan Projects under Grant No. 2016A010101035 & 2016A010101034. and Password. (3) Method-3: Broadcasting the SSID and Password to the IoT devices through AP (Access Point). An AP can be a mobile phone or a computer. The acceptant IoT devices then access the network using obtained SSID and Password. (4) Method-4: The IoT device broadcasts a network access request to the gateway devices. The target gateway responses the IoT device with SSID and Password, and the IoT devices access the network using obtained SSID and Password. While acknowledging the achievements of the existing proposals, which have been found to perform effectively in some specific cases, however, each proposal still has some limitations, e.g., increased cost and volume of IoT devices, complicated and cumbersome operations, and poor user experience. Especially, with the rapid growth of

the number of IoT devices which attempt to access the network, the existing proposals are hard to cope with the access requests of large-scale IoT devices. Inspired by previous research achievements, a fast access method for ZigBee-enabled IoT devices is proposed in this paper to address these challenges.

II. INTERNET OF THINGS

The Internet of Things (IOT) is an important topic in technology industry, policy, and engineering circles and has become headline news in both the specialty press and the popular media. This technology is embodied in a wide spectrum of networked products, systems, and sensors, which take advantage of advancements in computing power, electronics miniaturization, and network interconnections to offer new capabilities not previously possible. An abundance of conferences, reports, and news articles discuss and debate the prospective impact of the "IOT revolution"— from new market opportunities and business models to concerns about security, privacy, and technical interoperability.

IOT systems like networked vehicles, intelligent traffic systems, and sensors embedded in roads and bridges move us closer to the idea of "smart cities'', which help minimize congestion and energy consumption. IOT technology offers the possibility to transform agriculture, industry, and energy production and distribution by increasing the availability of information along the value chain of production using networked sensors. However, IOT raises many issues and challenges that need to be considered and addressed in order for potential benefits to be realized

III. EXISTING SYSTEM

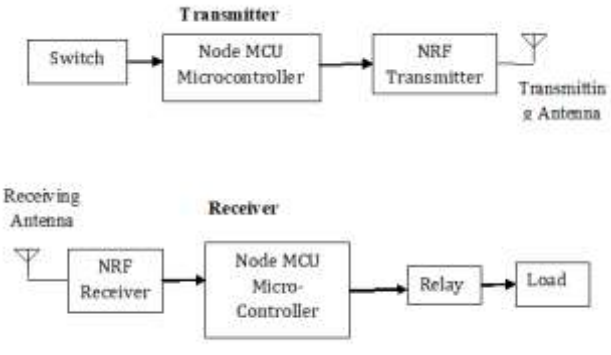
Previously implemented fast access protocol for ZigBee-enabled IoT devices, the following entities is necessary. Also, the corresponding function of each involved entity is described as follows.

- IoT device which is embedded with a ZigBee communication module has an access demand.
- ZigBee coordinator is used to interact with the ZigBee module embedded in the IoT device attempting to access the target ZigBee wireless network (also can be called registering IoT device) to complete the configurations of PAN ID, signal channel and PAN address.
- Mobile phone client is a customised software, which is used to input the information about the registering IoT device.

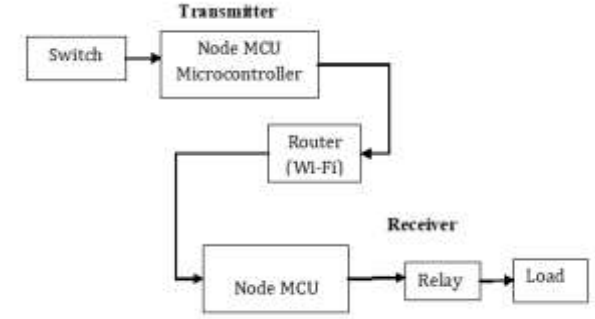
IV. PROPOSED SYSTEM

To implement the proposed fast access protocol for NRF Transceiver module enabled IoT devices and the data communicate in the 3 different cases.

Case (1):-



Case (2):-



Case (3) :-

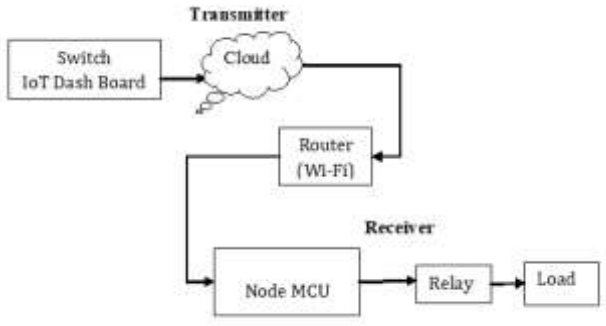


Figure1: Architecture of the Proposed System

A. NRF Transceiver module

In this wireless communication between two Arduino boards using the NRF24L01 transceiver module For explaining the wireless communication we will make two

examples, the first one will be sending a simple "Hello World" message from one Arduino to another, and in the second example we will have a bi-directional communication between the Arduino boards, where using the Joystick at the first Arduino we will control the servo motor at the second Arduino, and vice versa, using the push button at the second Arduino we will control the LED at the first Arduino**.**

The NRF24L01 transceiver module. It uses the 2.4 GHz band and it can operate with baud rates from 250 kbps up to 2 Mbps. If used in open space and with lower baud rate its range can reach up to 100 meters**.**

Figure 2: NRF Transceiver module

The module can use 125 different channels which gives a possibility to have a network of 125 independently working modems in one place. Each channel can have up to 6 addresses, or each unit can communicate with up to 6 other units at the same time. The power consumption of this module is just around 12mA during transmission, which is even lower than a single LED. The operating voltage of the module is from 1.9 to 3.6V, but the good thing is that the other pins tolerate 5V logic, so we can easily connect it to an Arduino without using any logic level converters.

Three of these pins are for the SPI communication and they need to be connected to the SPI pins of the Arduino, but note that each Arduino board have different SPI pins. The pins CSN and CE can be connected to any digital pin of the Arduino board and they are used for setting the module in standby or active mode, as well as for switching between transmit or command mode. The last pin is an interrupt pin which doesn't have to be used.

B. Node MCU

Node MCU is an open source Lua based firmware for the ESP8266 Wi-Fi SOC from Espress if and uses an on-module flash-based SPIFFS file system. Node MCU is implemented in C and is layered on the Espress if NON-OS SDK. The firmware was initially developed as is a companion project to the popular ESP8266-based Node MCU development modules, but the project is now community-supported, and the firmware can now be run on *any* ESP module.

Fig.3 Node MCU

C. LCD:

We used 16*2 LCD module in our project which is connected to Node MCU through a LCD interface IC or directly to its address and data bus and few control pins.

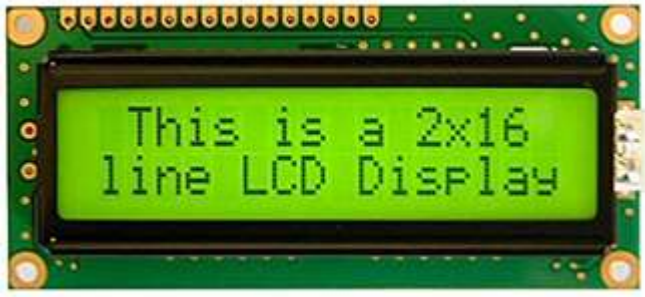


Figure 4: LCD Display

D. Wi-Fi

In order to upload sensor readings from all sensors to the open-source cloud ThingSpeak, Arduino UNO interfaces at the output with Wi-Fi module ESP8266. It is a low-cost Wi-Fi microchip with a full TCP/IP stack. It works on the 3.3V that is provided by Arduino UNO in our system. The module is configured through AT commands and needs the required sequence to be used as a client. The module can work as both client and server. It gets an IP on being connected to Wi-Fi through which the module and then communicates over the Internet. After testing our ESP8266 module, we connected it with Arduino UNO and then programmed Arduino UNO to configure the ESP8266 Wi-Fi module as TCP client and send data to ThingSpeak server which is an open IoT platform to visualize and analyse live data from sensors.

V. EXPERIMENTAL RESULT

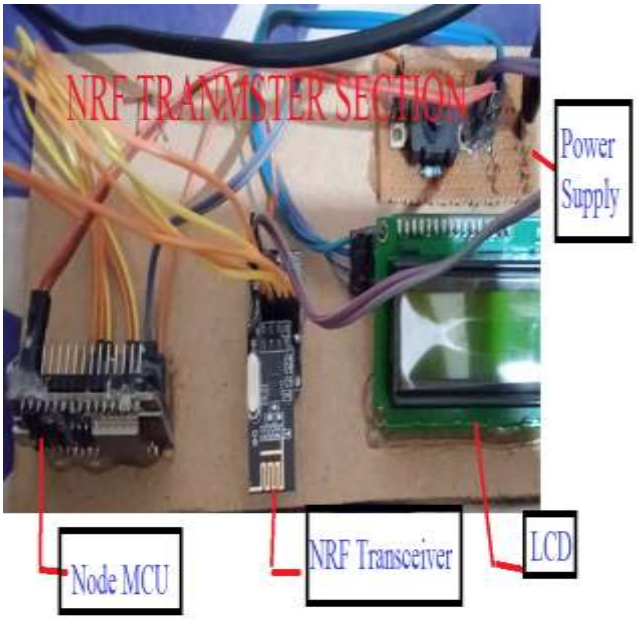


Figure.5: Experimental Setup for Transmitter Section

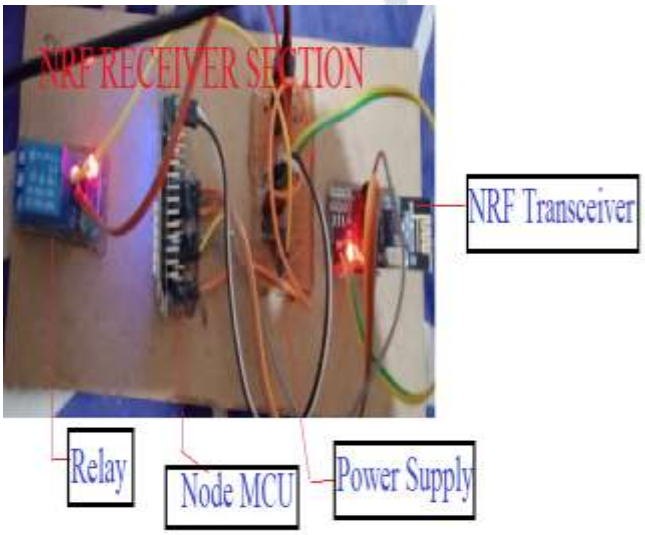


Figure.6: Experimental Setup for Receiver Section

IV. CONCLUSION

In this paper, to address the realistic challenge that the number of registering IoT devices is experiencing a tremendous growth in the development of IoT application systems, a fast access protocol for NRF module IoT devices is proposed. Through the signaling interactions among the involved protocol entities, the NRF module embedded in a registering IoT device could automatically obtain a PAN address and instantly access the target wireless network. A prototype system is also developed to evaluate the effectiveness and efficiency of this protocol, and the experiment and analysis results have demonstrated the performance by comparing with the existing network access methods, which indicate that the proposed protocol can be widely used in the development of NRF Communications, based IoT application systems, and can improve the developing efficiency

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, et al. Internet of things: A survey on enabling technologies, protocols, and applications, IEEE Communications Surveys & Tutorials, Vol.17, No.4, 2347-2376, 2015.

[2] J. Gubbi, R. Buyya, S. Marusic, et al. Internet of Things (IoT): A vision, architectural elements, and future directions, Future generation computer systems, Vol.29, No.7, 1645- 1660, 2013.

[3] M. Tao, K. Ota, M. Dong. Ontology-based data semantic management and application in IoT- and cloud-enabled smart homes, Future generation computer systems, Vol.76, 528- 539, 2017.

[4] P. M. Sanchez, R. M. Lopez, A. F. G. Skarmeta. Panatiki: A network access control implementation based on pana for iot devices, Sensors, Vol.13, No.11, 14888-14917, 2013.

[5] C. W. Zhao, J. Jegatheesan, S. C. Loon. Exploring IOT Application Using Raspberry Pi, International Journal of Computer Networks and Applications, Vol.2, No.1, 27-34, 2015.

[6] A. N. Ansari, M. Sedky, N. Sharma, et al. An Internet of things approach for motion detection using Raspberry Pi, Proceedings of IEEE International Conference on Intelligent
Computing and Internet of Things (ICIT), 131-134, 2014.

[7] G. Barbon, M. Margolis, F. Palumbo, et al. Taking Arduino to the Internet of Things: the ASIP programming model, Computer Communications, Vol.89, 128-140, 2016.

[8] R. Piyare. Internet of things: ubiquitous home control and monitoring system using android based smart phone, International Journal of Internet of Things, Vol.2, No.1, 5-11, 2013.

[9] S. Ferdoush, X. Li. Wireless sensor network system design using Raspberry Pi and Arduino for environmental monitoring applications, Procedia Computer Science, Vol.34, 103- 110, 2014.

[10] T. Ming, K. Ota, M. Dong, Z. Qian. AccessAuth: Capacity-aware security access authentication in federated- IoT-enabled V2G networks, Journal of Parallel and Distributed Computing, DOI: 10.1016/j.jpdc.2017.09.004, 2017.

ABOUT AUTHORS

1. Ms. K.Chaitanya Sravanthi received B.Tech degree from Department of Electronics & Communication Engineering from Sree Rama Engineering College and Pursuing M.Tech in Communication System in S.V. University College of Engineering Tirupati. Her interested areas are Wireless Communications etc.

2. Mrs. Dr.S.Swarnalatha, Associate Professor at SVUCE (SVU) Tirupati. Received Doctorate from SVUCE (SVU) in the image processing domain. Served as associate and assistant professor in ECE department, MITS, Madanapalle, Associate professor in ECE Department CMIT, Hyderabad.

3. Dr.B.ShobanBabu, Professor at SVEC, Ph.D from SVUCE in the image processing domain. Served as assistant and associate professor at MITS, Madanapalle and associate professor at SVCET, Chittoor