Paper

by Fancy C

Submission date: 10-Apr-2022 09:25PM (UTC+0530)
Submission ID: 1806695350
File name: CPS_Research_Paper.docx (147.08K)
Word count: 1420
Character count: 7908

Stable Network Architecture for Automation Device Interconnection

[1]Gyanesh Samanta, [2]Devdarshan K Sardar, [3]Rishal Ramesh, [4]Rushil Saxena[1], [5]Sidhant Chourasiya, [6]Fancy C
[1]UG student, [2]Assistant Professor
[1,2]Department of Computer Science Engineering, SRM Institute of Science and Technology, Kancheepuram, India.

ABSTRACT

Cyber-physical systems integrate sensing, computation, control and networking into physical objects and infrastructure, connecting them to the Internet and to each other. Controlling each device with separate controllers or switches seems like a tedious and troublesome task. Today's world, smart devices or a smart hub allows us to connect a limited number of devices, usually around 30-40. In this paper, we propose a way in which you can connect to over 200 IoT devices seamlessly without affecting the bandwidth to a single point. In a connected network system, you can increase the number of devices linearly. It is a unique system which is different from the existing system based on WiFi and Bluetooth. We have used Zigbee as our base and for controlling the devices we are using the Arduino microcontroller. The WiFi in our project plays a small role but the major role is played by Zigbee. The Arduino sends Wifi signals to connect the device which in turn communicate through Zigbee. It is a simple IoT based work which not only connects multiple devices at once but also provides a stable, reliable and fast connection, communication and control between the devices.

KEYWORDS

Internet of Things, Embedded systems, Zigbee, WiFi, Smart devices.

1. INTRODUCTION

A CPS or Cyber Physical System is an intelligent computer system where physical devices are monitored and controlled by human created computer algorithms. CPS is a class of embedded systems which incorporates both engineered computing and communicating systems in hardware and software elements. It is the base for the development of smart buildings or smart homes, smart gadgets, new innovative medicines, etc. CPS is used in numerous fields such as Structure Health Monitoring, flight test instrumentation, networking systems, energy systems, environment monitoring.

Our system comprises the integration of wireless technologies namely WiFi and Zigbee, since cyber physical systems are systems which involve the integration of cyber and physical components. This project also involves the usage of microcontrollers and ethernet shields which are embedded systems. When we think of a traditional system built for this purpose such as Multinet even though it enables increased range and better connectivity for end users it is limited by the surge in power usage which also comes at an exorbitant price point. For a Wifi based system which uses communication and network protocol based on IoT, there are issues when it comes to range and speed when more devices are connected.

In the case of WiFi, we are moving ahead with the assumption that our router is one of the best available in the market, the "ASUS GT-AX11000 ROG Rapture Router (Black)

AX11000 ” which is compatible with most IoT devices and has long-range connectivity. All data provided below will be based on our findings in terms of WiFi and Zigbee connectivity.

2. RELATED WORK

In the paper titled “MultiNet: Connecting to Multiple IEEE 829.11 Networks Using a Single Wireless Card” by Ranveer Chandra(mail - *ranveer@cs.cornell.edu*), Paramvir Bahl (mail - *bahl@microsoft.com*), Pradeep Bahl(mail - *pradeepb@microsoft.com*) They describe a new architecture for virtualizing WLAN cards and describe an overlooked connectivity paradigm that can be enabled using this architecture. They describe the algorithms for switching between disparate networks and analyze their performance. They add on a buffering protocol that ensures packet delivery to switching nodes.

A. Number of devices

In this approach, a case is considered where we have more than 200 IoT devices. For this scenario, WiFi will not be our ideal choice as with the increase in the number of devices connected to the network the bandwidth is reduced proportionally. With the decrease in bandwidth we may observe connection failure, slow response times which would be detrimental to the utilisation capability of these devices.

B. Range

This approach integrates the different features from both the wireless technologies. Even though Zigbee is a LAN it can be combined with other Zigbee LANs to terminate the issue of blank spots without coverage. Currently for extending the range of networks we are using repeaters or extenders for this purpose. But the drawback in this approach is that in practical scenarios the range of repeaters is significantly lower than that of Zigbee modules that are currently available. Our approach significantly increases the range of networks.

C. Single Control Unit

This proposed architecture would help us with controlling all devices from a single controller (or smartphone). All these devices would be connected to the same network and will be able to receive communication from the control device. In case of any faults, our architecture will allow us to detect faults at the exact XbeeS2C module, Arduino and associated Router. This would aid the technical experts in resolving issues (if any arise) at a faster pace.

D. Best of Zigbee and WiFi

In this approach, we aim to collectively use WiFi and Zigbee with a microcontroller i.e Arduino Uno R3 which would enable us to use both wireless network systems simultaneously. The microcontroller uses an XbeeS2C and WiFi shield to add on Zigbee and WiFi connectivity respectively. The entire setup would cost less than $. This efficient system would aid macro network setups to deal with the increasing number of smart devices. The drawback of this system is based on the limitations of smart IoT devices being able to connect to Zigbee networks.

3. ARCHITECTURE DIAGRAM

In this section, we describe the proposed architecture of this paper.

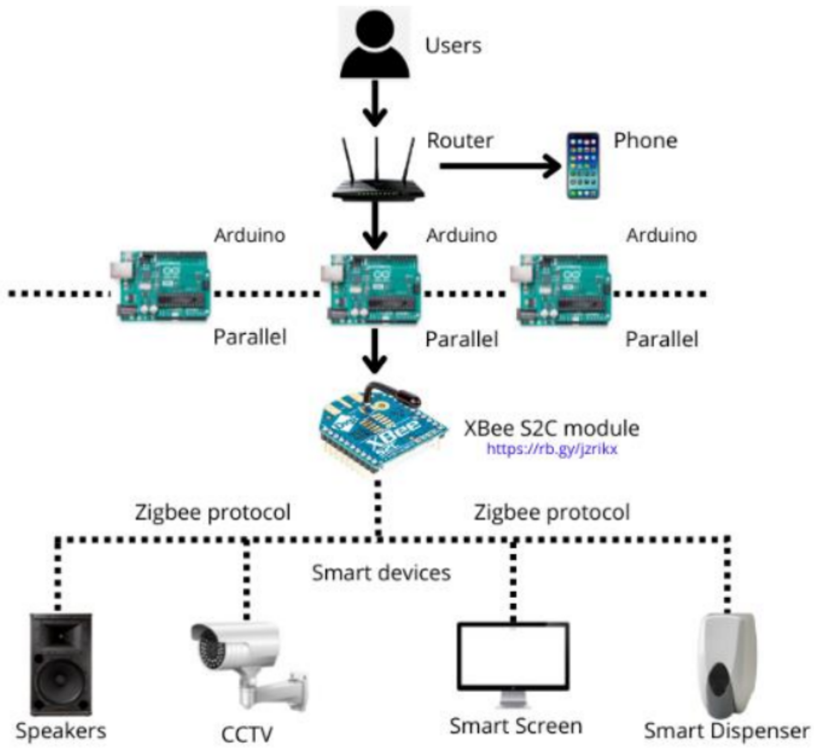

Fig-a. Showing the proposed architecture diagram

A. Methodology

In this paper, we have connected the XbeeS2C module to the main microcontroller i.e Arduino board which in turn is connected to the WiFi router. We can have multiple Arduino boards connected to the WiFi which linearly increases the number of XbeeS2C modules connected, and increases the number of IoT devices connected in an order of multiples of 250.

B. Component List

- Arduino Uno R3: This is a microcontroller that is based on a removable, dual-inline package ATmega328 AVR microcontroller. The board is issued with 14 digital input/output pins and 6 analogue inputs.
- XbeeS2C shield: This shield is used in this abstract to allow the microcontroller to add wireless capabilities to the prototype. It integrates directly with any development board that has the same trace as any Arduino board.
- A power bank: This component provides us with the DC power supply required by the prototype (5000 mAh).

- WiFi Router: This device serves as an access point in our network and connects the User to the Arduino boards to the users serving as a gateway between them. It also connects to the controller (or smartphone) in this scenario.

4. RESULTS AND CONCLUSION

To evaluate the performance of our system, we have used theoretical values adjusted to 5% deflection in numerical values to match practical usage. The change in factors associated is listed below.

A. Number of Devices Connected.

Our WiFi router can connect with upto 10 Arduinos without any observation of reduction in bandwidth speeds.

The Arduino connects to XBee modules which in turn can handle upto 250 devices.

So, 10*250 = 2500 devices at once

B. Range:

As per our theoretical calculations:

WiFi → 40m (ideally*)

Repeater → 40-50m (ideally**)

XBee Module → 100m (ideally**)

As per our architecture diagram;

Arduino is connected to WiFi and on a router we can connect upto 10 Arduinos before observing the bandwidth limitation in terms of the speed drops.

(WiFi router → tested with 10 Arduino with 30Mbps speed on 2.4 Ghz bandwidth)

The 10 Arduinos in turn are connected to 10XBee modules and considering the Arduinos are in the extent of the circle. We have a combined range of

40m(WiFi) + (10*100) = 1000 + 40 = 1040 metres

A coverage of 1040m, this is not the best case scenario as we are using a typical router.

*values obtained from Router details of (ASUS GT-AX11000 ROG Rapture Router (Black) AX11000)

**values obtained from Xbee S2C point

REFERENCES

1. Ranveer Chandra, Paramvir Bahl and Pradeep Bahl. “MultiNet: Connecting to Multiple IEEE 802.11 Networks Using a Single Wireless Card” https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/multinet_infocom.pdf
2. Digi International Inc. “DIGI XBEE S2C 802.15.4 RF MODULES” https://www.digi.com/resources/library/data-sheets/ds_xbee-s2c-802-15-4
3. Arduino. “Arduino UNO R3” https://docs.arduino.cc/hardware/uno-rev3\
4. Muthu Ramya.C, Shanmugaraj.M and Prabakaran.R. “STUDY ON ZIGBEE TECHNOLOGY” https://www.researchgate.net/publication/261497749_Study_on_ZigBee_technology
5. Vishwas K V, Abhishek V Tatachar, Shivanee Kondur, Amith R, Varun Y C, Dr.Kiran Y C. “Zigbee, It’s Applications and Comparison with Other Short Range Network Technologies” https://www.researchgate.net/publication/352935731_Zigbee_It%27s_Applications_and_Comparison_with_Other_Short_Range_Network_Technologies

Paper

ORIGINALITY REPORT

7%	6%	5%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.cs.cornell.edu Internet Source	3%
2	ceur-ws.org Internet Source	2%
3	Submitted to University of Huddersfield Student Paper	1%
4	www.ijert.org Internet Source	1%

Exclude quotes	On	Exclude matches	< 10 words
Exclude bibliography	On		