The Hub: IoT in Education

By Winnie Zheng, ECE '19

Introduction

Wi-Fi is a wireless way to handle networking between devices using radio. Historically, most common usage of Wi-Fi is in computers. Today, due to the increase simplicity and accessibility of networks, Wi-Fi capabilities are being integrated into more devices such as: cars, microwave, chairs, etc. As a result of this expansion, the Internet of Things (IoT) was developed. IoT is a network of devices of miscellaneous software, hardware, and network protocols joined together in one network to exchanging and compile information.

As the usage of IoT devices become more widespread, many industries are integrating it into their fields. One such industry is academia; IoT devices can be used in classrooms to promote higher levels of personalized learning.

INTERNET OF THINGS (IoT)

What is IoT?

Internet of Things is a network of wirelessly connected devices that can communicate with each other via the Internet. The concept of IoT comes down to three Cs: Communication, Control and Automation, and Cost Saving.[1]

The idea behind this network is to connect many *things* to the internet so that data can be shared. These *things* can be both living or non-living such as data from wind turbines or from a person's pedometer. As long as the *things* have a sensor that can be used for data collection, they can be connected to the IoT. These data are hosted online and should be able to be access from any device in the system.

With devices connected and communicating among each other, users are given more control over their devices. Rather than having to turn on/off or adjust a device in person, users are now able to control devices from across the world using Internet. Using similar channels, devices are also capable to delivering alerts to users. If a schedule/script is set, devices are capable of performing actions by themselves and send updates and/or alerts to the users.

As a result of this ability to collect data and control devices remotely, IoT can save consumers money. IoT devices have the ability to provide measurements via the sensors rather just providing an estimate, giving users a clearer view of what is going on.

Different Types of Protocols

There are several types of wireless protocols that can be used for IoT: RFID, Bluetooth, Zigbee, Wi-Fi, and etc. As each device in an IoT network has different physical metrics-battery life, radio range, processing power, etc.- it is important to pick a corresponding protocol that works for it as different protocols also have different speed, power consumption, and network architecture. ZigBee, Bluetooth, and RFID are all short-ranged networks, meaning that devices using these protocols have to be in close proximity with each other. These three protocols require different network architecture and have different ranges of data rates. [4]

Wi-Fi, on the other hand, have varying data rates depending on user network. The benefit of having varying rates within the network is that Wi-Fi allows for remote access. Devices can be far from each other and still be able to communicate without using huge amounts of power.

WIRELESS COMMUNICATION

Why Wi-Fi?

Wi-Fi is a wireless protocol that is available in most institutions, making it one of the obvious choices for communications. Wi-Fi 802.11 allows for communication over unlicensed bands and is easy to implement. It provides easy short-range wireless connectivity to ubiquitous vendors. In addition, it uses 256-bit encryption, providing a higher level of security.

Wi-Fi delivers a moderate range, with high accuracy, along with high throughput. Some versions of the protocol, such as 802.11ac, can transmit up to 1.3 Gbps making it ideal for bandwidth intensive data. In addition, the device's location can be triangulated using the MAC address, making it ideal for various sensors.

One problem, however, is that servers has a high energy requirement. Fortunately, most access points, usually routers, are plugged into a power source. Standard protocols, such as 802.11a/b/g/n/ac, all face the similar problem. The range and energy efficiency issues were addressed in the IEEE standard specifications for 802.11ah and 802.11ax.

Structure of Wi-Fi

Wi-Fi has a star-based network topology where the center of the star is a wireless access point, usually a router. The endpoints, nodes, of the star are wireless devices. The nodes cannot communicate with each other, rather the center is used a relay. As a result of this setup, it is easy to add and remove device without disrupting the network since cutting off an endpoint only affect the center. This structure, however, has a big risk: if the center fails, the network fails. [3]

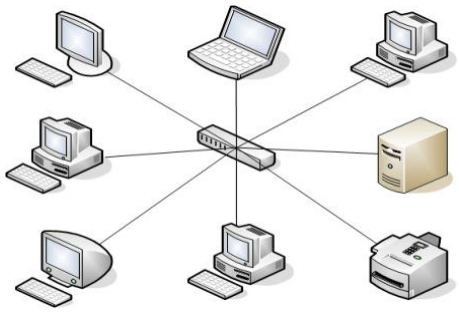

Figure 1. Star Network Architecture [6]

Wi-Fi uses an infrastructure network for its mode of operation. One characteristic of infrastructure mode is that the wireless network requires a physical structure that can provide access to other networks, forward data, and is a medium for access control. When multiple structures are linked together, an infrastructure network is created. To boost signals, more access points, physical medium, can be added. Within these networks, communication takes place between the access points and wireless nodes. [3]

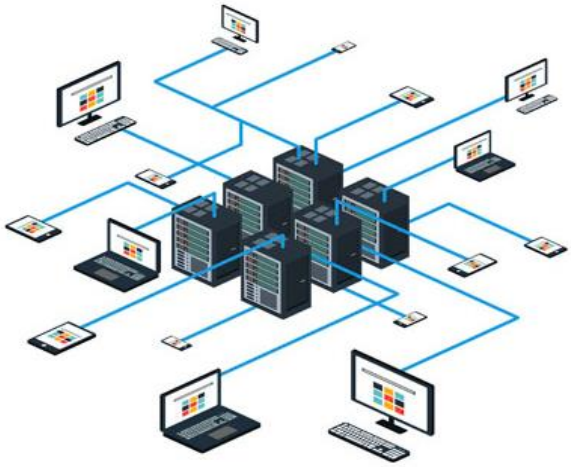

Figure 2. Infrastructure Network Architecture [5]

IEEE IoT Friendly Standards

Protocol 802.11ah, Wi-Fi HaLow, was a standard that was ratified in October 2016 to address the range and power concerns of the IoT devices. It uses a 900 MHz ISM license-exempt band to deliver a wider range, up to a radius of one kilometer, while using lower power. The protocol allos for station grouping which helps relay to extend the reach of its communication will also minimizing contention. Power usage is optimized by using predefined wake/doze periods. The reason why Wi-Fi HaLow has not been popularized because it requires specialized wireless access points and client hardware.

Protocol 802.11ax, High Efficiency Wireless (HEW), is an upcoming standard that aims to add more IoT friendly features. In addition to extending the range of Wi-Fi using similar feature as HaLow, it adds uplink multi-user MIMO capabilities coupled with a smaller subcarrier spacing, sucj as 78.125 kHz. This allows for up to 18 clients, in this case IoT

devices, to transmit data at once with in a 40 MHz channel. Because HEW was developed as an improvement to HaLow, its adoption will be dependent on HaLow's adoption.

ROLE OF INTERNET IN INTERNET OF THINGS

History of Internet

In 1908, Nicholas Tesla talked about a vision of the Internet. He envisioned that "It will be possible for a business man in New York to dictate instructions, and have them instantly appear in type at his office in London or else-where…An inexpensive instrument, not bigger than a watch, will enable its bearer to hear anywhere, on sea or land, music or song, the speech of a political leader, the address of an eminent man of science, or the sermon of an eloquent clergyman, delivered in some other place, however distant."

In 1820, the concept of wireless was defined in a physics experiment. In 1878, David Hughes was able to send and receive Morse code through wireless means, specifically radio waves. In 1896, Tesla was able transmit signals over a distance up to 30 miles. In 1900, Reginal Fessenden became the first to successfully transmit voice over radio waves. From there, radio technology has only continued to improve, allowing it to reach across the globe.

In 1962, J.C.R. Licklider presented his vision of a Galactic Network where a series of connected computers was able to link people to a "universe of information." In 1965, Larry Roberts was able to set up a connection between a computer at MIT Lincoln Laboratory in Cambridge, Massachusetts and a computer at System Development Corporation in Santa Monica, California. During this time, similar networks "threads" were being set up on the east coast of US, west coast of US, and in the United Kingdom. These threads were eventually merged, and the technology polished to enable better performance, reliability, and sustainability. Finally, in the Fall of 1969, the Internet was born. [8]

Cloud Computing

In the recent years, many schools have already or is looking to adopt cloud technology and integrate it into their classrooms. The reason for this is because Cloud technology requires little more than a browser and an internet connection, frequently lowering the overall software and hardware cost for schools. Furthermore, unlike more traditional software or hardware, Cloud technology is scalable to the size of the classroom. The same technology can be used for a classroom of ten and a classroom of a hundred.

Teachers are now able to setup classes remotely, distribute materials and assignments to a miscellaneous number of students, directly assist each student, as well as offer real-time feedback. They can even collaborate with several students at the same time. For students, cloud technology has also transformed the ways they gather, analyze, and learn information. Using cloud-based applications, any notes, photos, videos can now be synced across devices allowing for a improve workflow with a more productive environment.

IoT in CLASSROOMS

Why the Need?

Due to the increase popularity and usage of IoT devices, it is extremely important for people to be educated in these concepts. As a result, IoT is being introduced in more and more schools today with increasingly younger students.

Incorporating IoT devices into classrooms raises a lot of questions. Is this feasible? What do teachers think about incorporating IoT into their curriculum? Can these new tools be used effectively? Can these new tools even be used in the school? What kind of problems do they raise? What are the trade-offs? Is it worth it?

Requirements

In order for IoT devices to be utilized the best of their capabilities in the classrooms, schools are required to have reliable Wi-Fi, thorough network analytic technology, and trained educators.

Reliable and widespread Wi-Fi coverage is required to provide stable, quick access everywhere on school ground. Dead zones within school buildings will cause disruption in communication through the network, leading to latency and possible information

losses. An additional requirement for these networks is sufficient bandwidth to be able to support the data traffic. Fortunately, most schools are currently using either 802.11n, 150Mbit/s protocol released in 2009, or 802.11ac, 800 Mbit/s protocol released in 2013, both of which are barely sufficient enough.

As Wi-Fi capable devices are becoming more and more accessible, faculty and students are starting to bring their own devices to school. To protect the network, institutions need to have efficient network analytics to provide IT personnel with a deeper understanding of what is going on in the network. They need to be able to identify who/what is accessing the school network, assign roles to all users/devices, internal and external, and then create and enforce policies to help control access capabilities.

On the user side, it is also important that administration provides funding for the teachers to learn more about IoT devices. Frequently, these devices are integrated into the classroom upon the teacher's request where they are already familiar with the technology. This is, however, not always the case. Sometimes teachers are forced to adopt them in order to meet district standards. While the goal of these devices is to bring learning to another level for the students, they become nothing more than hinderance if the educators are not comfortable with the technology.

Issues

Many older designs for wireless networks were on one sole requirement: coverage. As devices gets faster and more versatile, they need constant connectivity. As a result, older networks are no longer capable of managing the load necessary to support IoT devices and online learning. Wi-Fi networks in school need to have a high bandwidth to support the robust load and demand due to ever-increasing number of devices. In 2014, the Federal Communications Commission (FCC) set a minimum Internet bandwidth of 100 kilobits per second per student. They project that by 2018, a new minimum would be set: 1 Mbps per student due to the increased number of devices and heavier load per connection. [2]

External devices that faculty and students bring into school are also unknowns to the network; adding them to the network puts the integrity of the existing devices and data at risk. IoT devices are sometimes external to the school network. The internet-based network these devices develop are often prone to cyberattack. By 2020, it is projected that there will be 25 to 30 billion IoT devices connected to the internet and 25% of cyberattacks will be targeting such networks. [7] This is a huge risk because IoT security is not keeping up with IoT devices workload even though the devices are getting better and better at measuring and collecting data from students. One prime example of IoT network securities not being advanced enough is the Mirai botnet attack in 2016 where Mirai was able to login a huge amount of IoT with embedded, striped-down, non-patchable Linux systems and amass hundreds of these devices, including cameras and routers.

Case Study

Sara Willner-Giwerc is a Tufts University doctoral student whose research is focused on developing new IoT technology for elementary school students. Her goal is to lower the barrier of entry for teaching engineering concepts. In an interview, Sara was asked about the current situation on teaching IoT devices in schools today.

"

Which IoT devices are necessary for your curriculum?

- It's not so much about the devices as it is the concept. Bluetooth devices are common in Educational technology. Wi-Fi technology is harder to come by, but you can do more things with it.

What is your workaround when you cannot connect to the internet?

- There really isn't one. Teachers don't have time for work arounds
- As an engineering education researcher, there are a few options. Some dongles exist to allow for Bluetooth to Wi-Fi conversion, but they are iffy at best. The only other option is to write your own code which I don't really know much about.

Is the lack of internet access for IoT a severe hindrance to your teaching?

- I'm not a teacher, but you can't really teach IoT without the internet. The whole point of IoT is that devices can talk to one another through a central cloud. Bluetooth devices don't have a central cloud; therefore, they aren't conducive to this.

Why is the communication between devices necessary?

- Right now, if I have a classroom of 30 kids, my WeDo can't talk to my classmates WeDo (or other devices). Being able to control a network of connected devices opens up learning opportunities, increases the different types of things you can teach, and is increasingly relevant given the direction most industry technology is taking.

Why have others not solved this problem?

- It's kind of a niche need. To be honest I'm not sure that many people see it as a problem. IoT education is very much a new and emerging idea, but as more and more technologies rely on it, it becomes more and more important to educate young students about it.

„

Nov. 28, 2018 [9]

Conclusion

The creation of the Internet has allowed people to share information across vast distances in the least amount of time. The ability to "*store*" things on the Internet has allowed people the ability to access information shared in the past. The ability to communicate with the Internet wirelessly has allow a greater audience to use it with ease. As a result of the versatility that wireless communications provide, a lot of technology today communicate wirelessly. Combined with the ability to send data over the Internet, technology is advancing such that users are able to control many appliances via their internet. The idea of a network of WiFi devices resulted in the creation of the Internet of Things, a technological concept that is becoming more and more advanced. As a result of its increased presence in everyday life, it has become important for young students to learn about IoT. The integration of modern technology with traditional methods, however, has resulted in many issues. The pre-existing technology is often not enough to support the new technical contents. There is need for new low-cost hardware to create a platform that allows for pre-existing technology to have similar capabilities of the new.

References

[1] "An Introduction to the Internet of Things (IoT)" https://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf. November 2013. San Francisco, Loprez Research LLC. [Accessed: 20-Nov-2018].

[2] S. Emily, "Calculating your school district's bandwidth need: Network Essentials for Superintendents," *EducationSuperHighway*, 10-Feb-2015. [Online]. Available: https://www.educationsuperhighway.org/blog/calculating-your-school-districts-bandwidth-need-network-essentials-for-superintendents/. [Accessed: 16-Dec-2018].

[3] "Connectivity of the Internet of Things - learn.sparkfun.com," *SparkFun*. [Online]. Available: https://learn.sparkfun.com/tutorials/connectivity-of-the-internet-of-things/all. [Accessed: 16-Dec-2018].

[4] Sarawi, Shadi & Anbar, Mohammed & Alieyan, Kamal & Alzubaidi, Mahmood. (2017). Internet of Things (IoT) Communication Protocols: Review. [Accessed: 14-Dec-2018].

[5] *Network-Infrastructure-Solutions.jpg*.

[6] *Star network*. 2018.

[7] N. Ismail, "The Internet of Things: The security crisis of 2018?," *Information Age*, 22-Jan-2018. [Online]. Available: https://www.information-age.com/internet-things-security-crisis-123470475/. [Accessed: 16-Dec-2018].

[8] L. Kleinrock, "History of the Internet and its flexible future," in IEEE Wireless Communications, vol. 15, no. 1, pp. 8-18, February 2008. [Accessed: 20-Mar-2019].

[9] W. Zheng and A. Geheran, "Wilner-Giwerc, Sara: Need for central Bluetooth to Wi-Fi Convertor," [Interview] 28-Nov-2018.