The Benefits of New Internet Protocols for Soil Sensors

By Zachary Sogard, ECE '16

In recent years, the number of smart, wireless, low-power devices connected to the Internet, such as soil monitor sensors, has exploded. Consequently, engineers are developing new protocols designed to replace Wi-Fi and better suit the needs of networked soil sensors and other IoT devices..

Introduction

Rise of the Internet of Things

In recent years, the amount of devices connected to the Internet has exploded. This rapid increase in smart devices is more commonly known as the Internet of Things (IoT). Nguyen et al. (2015) defines the IoT as "a highly interconnected network of heterogeneous devices".

IoT devices are often used in wireless sensor networks (WSNs). In a WSN, a large number of low-power sensors are placed in various locations. These sensors take measurements and talk to a central server that records all of the data from each sensor. According to National Instruments (2012), WSNs are applied to monitor industrial machines, structural strength of bridges and buildings, and environmental conditions.

Examples of IoT Devices

The application of IoT devices to consumer products, vehicles, etc. is widespread. Examples of consumer products include smart speakers that can play music and respond to questions from users, thermostats that can be controlled via mobile apps, and smoke detectors that can alert users who aren't home. Additionally, IoT medical devices can report patients' data such as heart rate or blood pressure over the Internet to doctors. Finally, IoT cars can receive software updates to improve things like fuel consumption.

Networked Soil Monitoring Sensors

In the 2016 Senior Design class of Tufts University's Department of Electrical and Computer Engineering, the Red Team has developed a wireless soil monitoring sensor system. This device measures soil conditions such as moisture, temperature, sunlight, and nutrient content that are then sent over Wi-Fi to a server. Farmers can use these devices to create a WSN on their field that monitors the soil conditions. With this information available, farmers can reduce fertilizer runoff and prevent overwatering.

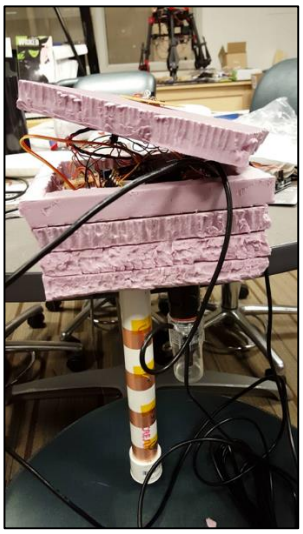

Figure 1. Working Prototype of Networked Soil Monitoring Sensor

How Computers Currently Talk to Each Other

The IoT raises several design challenges that the current methods of computer communication do not support. To address these challenges, we first need to understand the traditional model of how computers talk to each other.

Computers talk to each other on an agreed-upon, standardized set of rules, or protocols. These rules determine things like how long the messages should be,

how they should be addressed, what happens if messages get lost, and how messages should be routed. There are five major layers of communication, and each layer is governed by a certain protocol. Together, these layers form a stack where each protocol depends on the one below it. This is similar to how each soil layer depends on the one below it as shown in Figure 2. Just as topsoil depends on the subsoil beneath it for foundation and nutrients, the application layer, for example, depends on the transport layer for the services it provides.

At the bottom of this stack is the physical layer (Layer 1) that describes how individual 1's and 0's, or bits, get transmitted across a physical wire.

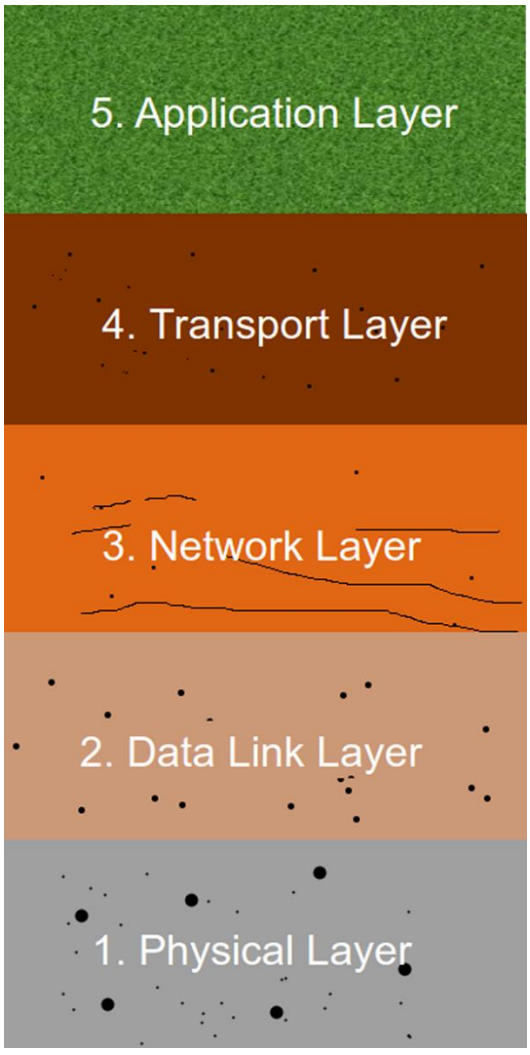

Figure 2. The Network Protocol Stack

The next layer is the data link layer (Layer 2). This layer is governed by two major protocols, Wi-Fi for wireless communication and Ethernet for wired communication. This layer describes how different devices take turns sending bunches of bits over the air or wire.

The network layer (Layer 3) is governed by the Internet Protocol, or IP. IP gives addresses to every device on the Internet and specifies how these groups of bits, or packets, get routed across the Internet in an efficient manner. This layer depends on Wi-Fi and Ethernet to get packets between individual devices on the Internet.

Zooming out further, the fourth layer (Layer 4) is the transport layer. This describes how entire groups of packets get sent reliably from end to end and what happens when packets get lost, or "dropped." This layer is governed by two protocols, the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). UDP is a simple and lightweight protocol, emphasizing speed, whereas TCP is more complicated and has extra rules to prevent flooding the network with packets and ensure reliable delivery. This layer depends on IP for routing the packets.

Finally, we have the application layer (Layer 5). This layer is where programs like e-mail, instant messaging, and web browsers reside. Each program follows its own protocol and makes use of the transport layer, and consequently all of the layers beneath it, to send packets to other computers.

How the IoT is Changing Computer Networks

The Internet's layered protocol has served the Internet well for many years. However, the IoT raises several issues. First of all, the IoT requires energy efficient communication so that these devices can survive on battery power for long periods of time. Second, the IoT requires a large increase in the number of devices on the Internet, each with their own address. Third, IoT devices need to communicate in a way that is still compatible with the existing Internet protocols rather than being isolated on their own network.

Table 1. A comparison of the three protocol's ability to address IoT issues.

	Compatibility with IP	Number of Addresses	Energy Consumption
Wi-Fi	Yes	3.4×10^{38} (with IPv6)	High
ZigBee®	No	6.4×10^{4}	Low
6LoWPAN	Yes	3.4×10^{38}	Low

The following is a comparison of the three most common protocols used by IoT devices.

Wi-Fi

Wi-Fi, short for "Wireless Fidelity," is the most common physical and data link layer protocol for wireless transmission. Therefore, it is easy to make IoT devices that use Wi-Fi because they will be guaranteed to work with the existing infrastructure. Wi-Fi's widespread usage facilitates compatibility with the existing Internet, but it is too power-hungry to be used over long periods of time.

ZigBee®

ZigBee® is an increasingly popular protocol for home automation and industrial WSNs. ZigBee® re-defines the physical and data link layer protocols to minimize communication and save battery power. Iniewski (2013) states, "the target market for Zigbee® is general-purpose, inexpensive, self-organizing mesh networks for energy management, home automation, building automation, and industrial automation." However, Lu et al. (2011) notes that while ZigBee® is ideal for low-energy isolated WSNs, it is not compatible with the existing Internet Protocol, so it cannot directly communicate with the rest of the Internet on its own. Additionally, ZigBee® supports only 64,000 devices on a single network. As shown in Table 1, this supports a far fewer number of devices than Wi-Fi or 6LoWPAN can.

6LoWPAN

The IPv6 Low Power Personal Area Network (6LoWPAN) protocol is another protocol being used to address IoT concerns. According to Granjal et al. (2015), IPv6 specifically augments the IoT standard by inserting an extra translation layer between the data link layer and network layer while leaving the physical and data link layer protocols the same as ZigBee®. It also uses a low-power version of IP for routing and UDP for low-power transport. 6LoWPAN is the best solution of the three protocols for the IoT because it is low-power, provides an endless amount of addresses for devices, and is compatible with the existing Internet.

Conclusion

The IoT demands careful reconsideration of how devices use the Internet to support the needs of low-power communication, vastly increased number of devices, and compatibility. Table 1 summarizes the pros and cons of each protocol relative to these challenges.

Ultimately, 6LoWPAN is the most optimal choice of the three. The Red Team can integrate this information with its Networked Soil Monitoring project. Farmers need these devices to last an entire farming season, be compatible with the existing Internet, and scale up to as many devices as they need. By replacing Wi-Fi transmitters with 6LoWPAN transmitters, we can transmit soil condition data from each sensor to the customer's server more easily and efficiently.

As networking needs change, the Internet will continue to change with it. Rather than having to rewrite every protocol, the Internet's layered approach of communication facilitates modifying it to support these changes.

References

Granjal, J., Monteiro, E., & Silva, J. (2015). Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Communications Surveys & Tutorials IEEE Commun. Surv. Tutorials, 17*(3), 1294-1312. doi:10.1109/COMST.2015.2388550

Iniewski, K. (2013). Wireless Sensor Networks for Consumer Applications in the Smart Grid. In *Smart grid infrastructure & networking* (1st ed., Vol. 1). New York, New York: McGraw-Hill.

Lu, C., Li, S., & Wu, Q. (2011). Interconnecting ZigBee and 6LoWPAN wireless sensor networks for smart grid applications. *2011 Fifth International Conference on Sensing Technology,* 267-272. doi:10.1109/ICSensT.2011.6136979

National Instruments. (2012, May 5). *What is a Wireless Sensor Network* [White Paper]. Retrieved from http://www.ni.com/white-paper/7142/en/

Nguyen, K., Laurent, M., & Oualha, N. (September 2015). Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks, 32*, 17-31. doi: 10.1016/j.adhoc.2015.01.006