microwaves&rf

Making Connections in the IoT Cloud

Microwaves and RF

Jack Browne

Wed, 2015-12-16 13:42

Widespread use of the Internet for communicating with sensors and actuators will enable the programming and remote control of automobiles, homes, and businesses.

Internet-based communications may have started out slow, a few decades ago, but few would have foreseen that so many electronic devices would one day be using the Internet to send and receive information of some form. Various market predictions now project more than 50 billion electronic devices connected to the Internet by 2020 as part of the rapidly growing Internet of Things (IoT) phenomena.

Related

This Is Your Brain on IoT

IoT Wireless Convergence Sparks Testing Challenges

M&A Deals Jumpstart IoT

Not all of these devices will be like your father's PC, with a cable or wired connection. Most will rely on wireless technology and on RF/microwave components of some form, typically as integrated circuits (ICs) in smaller portable, mobile products. Others may rely on more discrete components in wireless IoT gateways, and as parts of the wireless Internet infrastructure that makes the interconnection of all those data-generating devices possible.

In addition to computers and mobile communications devices such as smartphones, the Internet and its ever-growing collection of networks known as the "cloud" is already flooded with a large and increasing number of sensors of different kinds. These include temperature, motion, and position sensors used for applications in monitoring room occupancy (for controlling lights and heating when a room is occupied); security; health and fitness monitoring; and even for control of robots and unmanned vehicles.

Some of these sensors will be interactive, requiring a response from someone receiving a message; some will operate as standalone units. Most of these sensors (except for hard-wired devices) will require wireless access to the Internet and generous bandwidth for communicating an enormous amount of data from all these sensors.

Already, a number of firms are offering medical alert devices, typically worn as pendants on a wrist by the

erly and others greatly in need of medical attention. A simple push of one button can alert medical and ergency services personnel by means of a wireless connection to the Internet. With the aid of a Global Positioning System (GPS) receiver, these same medical devices can provide location information. They are designed with devices and packaging that can withstand rough handling and high humidity, even in showers.

As the IoT expands, this basic concept of using wireless communications to monitor patient health can be applied by different types of sensors—even those embedded within a human body—allowing medical professionals to monitor patient heart-beat rate, blood pressure, and other key health parameters from a distance, and at any time. This significantly reduces the costs of doctor visits and health care in general.

In many ways, the evolution of RF/microwave components for IoT applications will parallel the development path taken by high-frequency manufacturers of devices and components for mobile communications products, such as cellular telephones. Essentially, two sets of devices and components will be needed: miniature, low-power electronic devices for use in wireless portable, mobile, and wearable IoT products; and larger, higher-power devices and components for IoT infrastructure equipment.

IoT gateways, which connect wireless IoT devices to the Internet using available wireless protocols such as cellular Long Term Evolution (LTE), Bluetooth, Wi-Fi, and ZigBee, will parallel the many cellular base stations that now provide the ease of use for mobile wireless handsets.

Wireless communications and IoT devices such as actuators and sensors are combining to make office buildings, warehouses, and homes “smarter” by allowing monitoring and control of security and environment functions by remote control from any communications device with Internet access *(Fig. 1)*. Home building supply stores are already selling IoT smoke detectors, thermostats, motion detectors (for monitoring room occupancy), and “smart plugs” that can be used to turn off lights from a distance.

A software application for remote control of a smart home may show a graphical representation of the home with the different IoT devices appearing on the screen of a monitoring device, such as a smartphone or tablet. As an example, a home owner may simply click on the on-screen image of a television set with a simple menu allowing the set to be turned on, switched to a low-power mode, or turned off as required. This can take place anytime and from anywhere with Internet access.

The IoT cloud is essentially one massive network consisting of possibly millions of “subnetworks”—such as cellular telephone networks and homeowner’s WLANs—linked together to provide data storage and applications. Basically, it turns the world into one giant computer hard drive. An IoT interconnected network will consist of the “things” that communicate to a local gateway either by wired connection, such as an Ethernet local area network (LAN) or wireless LAN (WLAN), Bluetooth, or Wi-Fi communications, with the gateway connected to the Internet.

The millions of wired and wireless gateways and their local subnetworks combine with the Internet to form the cloud. This connects back-end devices—such as servers, smartphones, and other data storage, software, and communications devices—to the wired and wireless “things” that are sending their data through this massive network.

Compared to hardwired devices, wireless technology offers a great deal of flexibility in mounting sensors throughout a location, and in making changes in sensor locations when necessary. These different sensors typically perform dedicated functions, such as detecting motion, temperature, or pressure; turning on or off lights; and communicating their data to a gateway by means of a particular wireless protocol, such as Wi-Fi, Bluetooth, ZigBee, or the IEEE 802.15.4 standard at 868, 915, and 2,400 MHz.

These sensors, or network nodes as they are known, are connected to the Internet through a gateway, which

ıslates each sensor's proprietary protocol to the Internet Protocol (IP) that allow interaction on the Internet. ıddition, some sensors are equipped with IP connectivity and can connect directly to an IP server where available. Rather than simple network nodes, these edge sensors are more like small computers, with their own memory and microprocessor.

Facing the Future

As wireless IoT technology spreads throughout multiple industries, including automotive, business, communications, industrial, healthcare, and transportation markets, a number of concerns arise concerning the large numbers of sensors and actuators and their eventual competition for bandwidth. The very capacity of the Internet will be a concern with the amount of data predicted from billions of worldwide sensors and the need to store and process that data.

In addition, the power requirements of the many IoT devices that will be mounted, worn, carried, or embedded within users is forcing circuit and device designers to rethink energy efficiency for their circuits, and novel approaches to providing energy for emerging IoT applications.

Numerous researchers have explored methods of harvesting energy from already-present power sources in a system. For example, a version of Wi-Fi WLAN technology known as power over Wi-Fi developed by engineers at the University of Washington gathers energy from a Wi-Fi router's signals for reuse to power sensors in a wireless sensor network.

In addition, recent research from the Eindhoven University of Technology in the Netherlands examined energy harvesting from 60-GHz line-of-sight millimeter-wave signals to power temperature sensors (see "World's Smallest Temperature Sensor Powered by MM-Waves").

EnOcean has developed patented energy-harvesting technology which it is already licensing to a number of wireless device developers. The technology employs 315 MHz in North America and 868 MHz in Europe to transfer power from an energy source to IoT devices in need of power. The firm has also developed a series of energy-harvesting wireless sensors and controls for building automation systems, for use at 315, 868, and 902 MHz *(Fig. 2)*.

Conservation of bandwidth may yet be another challenge for the growing IoT ecosystem, as more and more wireless devices compete for limited available frequencies. In some cases, millimeter-wave frequencies such as 60 GHz may be used while in other cases, the spectral spaces between existing wireless standards, known as "Weightless," may be recruited to linkIoT devices to IP gateways.

The design challenges are certainly intriguing—and with billions of IoT products forecasted for so many different markets, not without tremendous motivation for solutions.

Source URL: http://mwrf.com/systems/making-connections-iot-cloud