Communication Models in Internet of Things: A Survey

Santosh Kulkarni
Lecturer
Department of Electronics & Communication Engineering
KLS Shri Vasantrao Potdar Polytechnic, Belagavi, Karnataka

Prof. Sanjeev Kulkarni
Professor
Department of Electrical and Electronics Engineering
KLS Gogte Institute of Technology, Belagavi, Karnataka

Abstract

The term Internet of Things generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items and enable these devices to generate, exchange and consume data with minimal human intervention using various networking and communication models. The data generated or processed from those smart objects will ultimately pass through gateways with connectivity to IP-based networks or will otherwise be incorporated into products that are accessible through Internet.

Keywords: Internet of Things, Communication Models, SmartThings

I. INTRODUCTION

"Internet-of-Things" or IoT is a term which is used as a keyword to cover various aspects associated to the expansion of the Internet and the Web into the physical reality. The Internet of Things is an emerging topic of technical, social, and economic significance [1]. Consumer products, durable goods, cars and trucks, industrial and utility components, sensors, and other everyday objects are being combined with Internet connectivity and powerful data analytic capabilities by widely using spatially distributed devices with embedded identification, sensing and actuation capabilities. In future, IoT devices will be found everywhere and will enable ambient intelligence. It will bring huge changes to the future society, change our way of life and business models. In this document, an overview of the various communication models used in IOT is given.

II. IOT OVERVIEW AND BACKGROUND

A. What is the Internet of Things?

As shown in Fig. 1, the IoTs allow people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service [2]. They are “Material objects connected to material objects in the Internet”. For example, through RFID, laser scanners, global writing system, infrared sensors and other information sensing devices are connected to any object for communication services and data exchange.

Fig. 1: Definition of Internet of Things.
III. ARCHITECTURE AND PROTOCOL STACK OF IOTs

IoTs can be divided into three important layers viz; Perception, Network and Application. As shown in Fig.2, perception layer (also called as recognition layer) gathers data/information and identifies the physical world. Network layer is the middle layer which includes the processes such as, initial processing of data, broadcasting of data, and polymerization. The topmost application layer offers the services. Among these layers, the middle one network layer is the "Central Nervous System" that takes care of global services in the IoTs, because it is the key layer which interconnects the application layer and perception layer.

![Fig. 2: Architecture of Internet of things](image)

The IOT Protocol Stack, as shown in the Fig 3, from a PHY perspective, the current IEEE 802.15.4-2006 PHY layer(s) suffice in terms of energy efficiency. Given that a large amount of IoT applications however will require only a few bits to be send. It may be advisable to commence looking into a standardized PHY layer which allows ultra-low rate transmissions over very narrow frequency bands, with the obvious advantage of enormous link budgets and thus significantly enhanced ranges. IEEE802.15.4e standard is very suitable for a protocol stack for IoT because it is latest generation of highly reliable and low-power MAC protocol.

![Fig. 3: IOT Protocol Stack](image)

From networking perspective, the introduction of the IETF 6LoWPAN protocol family has been instrumental in connecting the low power radios to the Internet and the work of IETF ROLL allowed suitable routing protocols to achieve universal connectivity. From the transport layer and an application perspective, the introduction of the IETF CoAP protocol family has been instrumental in ensuring that application layers and applications themselves do not need to be re-engineered to run over low-power embedded networks.

IV. INTERNET OF THINGS COMMUNICATIONS MODELS

From an operational perspective, it is useful to think about how IoT devices connect and communicate in terms of their technical communication models. The discussion below presents this framework and explains key characteristics of each model in the framework. [3]
A. Device-to-Device Communications

The device-to-device communication model represents two or more devices that directly connect and communicate between one another, rather than through an intermediary application server. These devices communicate over many types of networks, including IP networks or the Internet. Often, however, these devices use protocols like Bluetooth, Z-Wave, or ZigBee to establish direct device-to-device communications, as shown in Figure below.

![Device-to-device communication model](image)

B. Device-to-Cloud Communications

In a device-to-cloud communication model, the IoT device connects directly to an Internet cloud service like an application service provider to exchange data and control message traffic. This approach frequently takes advantage of existing communications mechanisms like traditional wired Ethernet or Wi-Fi connections to establish a connection between the device and the IP network, which ultimately connects to the cloud service. This is shown in Figure 5 below.

![Device-to-Cloud communication model](image)

This communication model is employed by some popular consumer IoT devices like the Nest Labs Learning Thermostat and the Samsung Smart TV. Further, this cloud connection enables the user to obtain remote access to their thermostat via a smartphone or Web interface, and it also supports software updates to the thermostat. Similarly with the Samsung Smart TV technology, the television uses an Internet connection to transmit user viewing information to Samsung for analysis and to enable the interactive voice recognition features of the TV. In these cases, the device-to-cloud model adds value to the end user by extending the capabilities of the device beyond its native features.

However, interoperability challenges can arise while attempting to integrate devices made by different manufacturers. Frequently, the device and cloud service are from the same vendor. If proprietary data protocols are used between the device and the cloud service, the device owner or user may be tied to a specific cloud service, limiting or preventing the use of alternative service providers. This is commonly referred to as "vendor lock-in", a term that encompasses other facets of the relationship with the provider such as ownership of and access to the data. At the same time, users can generally have confidence that devices designed for the specific platform can be integrated.

C. Device-to-Gateway Model

In the device-to-gateway model, or more typically, the device-to-application-layer gateway (ALG) model, the IoT device connects through an ALG service as a conduit to reach a cloud service. In simpler terms, this means that there is application software operating on a local gateway device, which acts as an intermediary between the device and the cloud service and provides security and other functionality such as data or protocol translation. The model is shown in Figure 6.
Several forms of this model are found in consumer devices. In many cases, the local gateway device is a smartphone running an app to communicate with a device and relay data to a cloud service. This is often the model employed with popular consumer items like personal fitness trackers. These devices do not have the native ability to connect directly to a cloud service, so they frequently rely on smartphone app software to serve as an intermediary gateway to connect the fitness device to the cloud.

The other form of this device-to-gateway model is the emergence of “hub” devices in home automation applications. These are devices that serve as a local gateway between individual IoT devices and a cloud service, but they can also bridge the interoperability gap between devices themselves. For example, the SmartThings hub is a stand-alone gateway device that has Z-Wave and Zigbee transceivers installed to communicate with both families of devices. It then connects to the SmartThings cloud service, allowing the user to gain access to the devices using a smartphone app and an Internet connection.

**D. Back-End Data-Sharing Model**

The back-end data-sharing model refers to a communication architecture that enables users to export and analyze smart object data from a cloud service in combination with data from other sources. This architecture supports “the [user’s] desire for granting access to the uploaded sensor data to third parties”. This approach is an extension of the single device-to-cloud communication model, which can lead to data silos where “IoT devices upload data only to a single application service provider”. A back-end sharing architecture allows the data collected from single IoT device data streams to be aggregated and analyzed. For example, a corporate user in charge of an office complex would be interested in consolidating and analyzing the energy consumption and utilities data produced by all the IoT sensors and Internet-enabled utility systems on the premises. Often in the single device-to-cloud model, the data each IoT sensor or system produces sits in a stand-alone data silo. An effective back-end data sharing architecture would allow the company to easily access and analyze the data in the cloud produced by the whole spectrum of devices in the building. Also, this kind of architecture facilitates data portability needs. Effective back-end data sharing architectures allow users to move their data when they switch between IoT services, breaking down traditional data silo barriers. The back-end data-sharing model suggests a federated cloud services approach or cloud applications programmer interfaces (APIs) are needed to achieve interoperability of smart device data hosted in the cloud. A graphical representation of this design is shown in Figure 7.
V. CONCLUSION

While the concept of combining computers, sensors, and networks to monitor and control devices has been around for decades, the recent confluence of key technologies and market trends is emerging in a new reality for the “Internet of Things”. The main vision of IoT is to usher in a revolutionary, fully interconnected “smart” world, with relationships between objects and their environment and objects and people becoming more tightly intertwined.

If the system is more complex, a number of potential challenges may stand in the way of this vision – particularly in the areas of security; privacy; interoperability and standards; legal, regulatory, and rights issues; and the inclusion of emerging economies. The Internet of Things involves a complex and evolving set of technological, social, and policy considerations across a diverse set of stakeholders.

Since IoT devices connect and communicate in terms of their technical communication models, from a general user perspective, these communication models help illustrate the ability of networked devices to add value to the end user. By enabling the user to achieve better access to an IoT device and its data, the overall value of the device is amplified. However, these networked benefits come with trade-offs. Careful consideration needs to be paid to the incurred cost burdens placed on users to connect to cloud resources when considering an architecture, especially in regions where user connectivity costs are high.

While the end user benefits from effective communication models, it should be mentioned that effective IoT communication models also enhance technical innovation and open opportunity for commercial growth. New products and services can be designed to take advantage of IoT data streams that didn’t exist previously, acting as a catalyst for further innovation.

REFERENCES